Ministerie van Veiligheid en Justitie

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
708641

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 4 januari 2016
Onderwerp Kabinetsstandpunt encryptie

Kabinetsstandpunt Encryptie
Hierbij sturen wij u het kabinetsstandpunt toe over encryptie. Hiermee wordt tegemoet gekomen aan de gedane toezeggingen tijdens het AO Telecomraad van 10 juni 2015 (TK 2014-2015, 21501-33, nr. 552) en AO JBZ-Raad van 7 oktober 2015.

Inleiding
Encryptie, ook wel versleuteling, is in toenemende mate eenvoudig te verkrijgen en gebruiken en maakt daarmee steeds vaker onderdeel uit van het reguliere dataverkeer. Door de overheid, bedrijven en burgers wordt encryptie steeds meer toegepast om de vertrouwelijkheid en integriteit van hun communicatie en opgeslagen data te beschermen. Dat is belangrijk voor het vertrouwen van mensen in digitale producten en diensten en voor de Nederlandse economie in het licht van de zich snel ontwikkelende digitale maatschappij. Tegelijkertijd vormt encryptie een belemmering voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer kwaadwillenden (zoals criminelen en terroristen) hiervan gebruikmaken. De recente aanslagen in Parijs, waarbij mogelijk gebruik is gemaakt van versleuteling van de communicatie door de terroristen, leiden tot de gerechtvaardigde vraag wat er nodig is om opsporings-, inlichtingen- en veiligheidsdiensten goed zicht te bieden en laten houden op aanslagplanning.

De in de vorige alinea beschreven tweeledigheid was eveneens te horen in het publieke debat van de afgelopen maanden over de dilemma's rondom het gebruik van encryptie. Ook uw Kamer heeft over dit onderwerp gesproken. Tijdens het AO Telecomraad is gevraagd wat het Kabinet gaat doen aan het stimuleren van sterke encryptie. Daarnaast is vanuit de Tweede Kamer gevraagd om te komen met een kabinetsstandpunt rond encryptie.

Hierna wordt ingegaan op het belang van encryptie voor de systeem- en informatiebeveiliging van de overheid en bedrijven, en voor de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Daarnaast wordt het belang van opsporing van ernstige misdrijven en bescherming van de nationale veiligheid geschetst. Tot slot wordt na weging van de belangen gekomen tot een conclusie.

De Nederlandse situatie kan hierbij niet los worden gezien van de internationale context. Sterke encryptiesoftware is in toenemende mate wereldwijd beschikbaar of al geïntegreerd in producten of diensten. Gelet op de brede beschikbaarheid en toepassing van geavanceerde encryptietechnieken en het grensoverschrijdende karakter van het dataverkeer is het handelingsperspectief op nationaal niveau beperkt.

Belang van encryptie voor de overheid, bedrijven en burgers
Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Veel cybersecuritymaatregelen in organisaties leunen sterk op de toepassing van encryptie. De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups zijn moeilijker zonder het gebruik van encryptie. Het afschermen van gegevens die verstuurd worden via internet, bij internetbankieren bijvoorbeeld, is alleen mogelijk met behulp van encryptie. Door de verbondenheid van systemen, wereldwijde vertakkingen en verschillende routes die communicatie kan afleggen, is het risico op onderschepping, inbreuk, inzage of wijziging van informatie en communicatie altijd aanwezig.

De overheid communiceert in toenemende mate digitaal met de burgers en verleent diensten waarbij vertrouwelijke gegevens worden uitgewisseld, zoals het gebruik van DigiD of het doen van belastingaangifte. Zoals in het Regeerakkoord is geformuleerd moeten vanaf 2017 burgers en bedrijven hun overheidszaken volledig digitaal kunnen regelen. De overheid heeft hierbij de plicht om te zorgen dat deze gegevens tegen kennisneming door derden zijn beveiligd; encryptie is hiervoor onontbeerlijk. Ook de bescherming van de communicatie binnen de overheid is van encryptie afhankelijk zoals bij de beveiliging van diplomatiek berichtenverkeer en militaire communicatie.

Voor bedrijven is encryptie essentieel om bedrijfsinformatie veilig te kunnen bewaren en versturen. Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat voor onder andere startups, datacentra en cloudcomputing. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie, die vooral zit in de digitale economie.

Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers doordat het hen een middel biedt om de vertrouwelijkheid en integriteit van persoonsgegevens en communicatie te beschermen. Dit is ook belangrijk voor de uitoefening van de vrijheid van meningsuiting. Het stelt bijvoorbeeld burgers, maar ook beroepen met een belangrijke democratische functie zoals journalisten, in staat om vertrouwelijk te communiceren.

Encryptie stelt derhalve alle betrokkenen in staat de vertrouwelijkheid en integriteit van communicatie te waarborgen en zich beter te weren tegen bijvoorbeeld spionage en cybercriminaliteit. Hierbij zijn fundamentele rechten en vrijheden, veiligheids- en economische belangen gebaat.

Encryptie en de opsporings–, inlichtingen- en veiligheidsdiensten

De bevoegdheden en middelen die de diensten tot hun beschikking hebben, moeten toegerust zijn op de huidige en toekomstige digitale realiteit. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld. Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die gegevens. Zij ervaren deze belemmeringen bijvoorbeeld wanneer zij onderzoek doen naar de verspreiding en opslag van kinderporno, bij de ondersteuning van militaire missies in het buitenland, het tegengaan van cyberaanvallen of wanneer zij zicht willen krijgen en houden op het voorbereiden van aanslagen door terroristen. Criminelen, terroristen en tegenstanders in gewapende conflicten zijn zich er vaak van bewust dat zij op enig moment de aandacht van de diensten kunnen trekken en hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook zij gebruik kunnen maken. Dat bemoeilijkt, vertraagt, of maakt het onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten. Tevens kan het onderzoek ter zitting en de bewijsvoering voor een veroordeling ernstig worden gehinderd.

Het recht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers

Het toepassen van encryptie helpt burgers zoals eerder werd opgemerkt, bij het borgen van de persoonlijke levenssfeer en de vertrouwelijkheid van hun communicatie. De hierboven genoemde rechtmatige toegang tot gegevens en communicatie door opsporings-, inlichtingen- en veiligheidsdiensten vormt evenwel een inbreuk op de vertrouwelijke communicatie van burgers.

Vertrouwelijkheid van communicatie raakt aan de grondwettelijk geregelde eerbiediging van de persoonlijke levenssfeer en aan het recht op bescherming van het brief-, telefoon- en telegraafgeheim (hierna: 'het communicatiegeheim'). Deze grondrechten zijn verankerd in respectievelijk artikel 10 en artikel 13 Grondwet. Daarnaast zijn deze fundamentele rechten vastgelegd in artikel 8 EVRM en artikel 7 en artikel 8 EU-Handvest (voor zover Unierecht wordt geraakt).

De bescherming van grondrechten is van toepassing op de digitale wereld. De hiervoor genoemde grondrechtelijke- en internationaalrechtelijke bepalingen bieden samen het kader om onwettige inbreuken tegen te gaan. De genoemde rechten zijn niet absoluut, hetgeen inhoudt dat beperkingen zijn toegestaan voor zover deze voldoen aan de vereisten die de Grondwet en het EVRM (en voor zover het Unierecht betreft, het EU-Handvest) stellen. Een inbreuk is toelaatbaar wanneer deze een legitiem doel dient, bij wet is geregeld en de beperking voorzienbaar en kenbaar is. Daarnaast dient de beperking noodzakelijk te zijn in een democratische samenleving. Tot slot dient de inbreuk proportioneel te zijn, dat wil zeggen dat het door de overheid nagestreefde doel proportioneel dient te zijn in relatie tot de inbreuk op de persoonlijke levenssfeer en/of het communicatiegeheim.

Deze vereisten bieden het kader waarbinnen de afweging gemaakt kan worden tussen de bij encryptie in het geding zijnde belangen, zoals het recht op de persoonlijke levenssfeer en het communicatiegeheim, de openbare en nationale

veiligheid en het voorkomen van strafbare feiten. Voorgaand afwegingskader is voor zover het de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten betreft overigens ook neergelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (artikelen 18 en 31 van de Wiv 2002). De medewerkingsverplichtingen inzake decryptie die zijn opgenomen in de Wiv (artikelen 24, derde lid en 25, zevende lid van de Wiv 2002) en in het WvSv (artikel 126m, zesde lid, van het WvSv), kunnen worden ingeroepen indien de daaraan gekoppelde bijzondere bevoegdheden na een afweging in voormelde zin worden uitgeoefend.

Afweging en conclusie
Het breken van de versleuteling is tegenwoordig in steeds minder gevallen mogelijk. Daarnaast is de mogelijkheid om gegevens in onversleutelde vorm te vorderen bij een dienstverlener, minder vaak beschikbaar. In toenemende mate worden bij moderne toepassingen van encryptie de gegevens nog slechts in versleutelde vorm door dienstverleners verwerkt. Gelet op het belang van de opsporing en vervolging van strafbare feiten en de belangen die zijn gemoeid met de nationale veiligheid, nopen deze ontwikkelingen tot het zoeken naar nieuwe oplossingen.

Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Door bijvoorbeeld een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zou onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving.

Bij de uitvoering van hun wettelijke taken zijn de opsporings-, inlichtingen- en veiligheidsdiensten deels afhankelijk van samenwerking met aanbieders van ICT-producten en -diensten. Gegeven deze afhankelijkheid, is overleg nodig met aanbieders over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.

Gegeven de voorgaande afweging komen we tot de volgende conclusie:

Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven , en voor de Nederlandse economie.

Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan

ten grondslag liggen uitdragen. Ten aanzien van het stimuleren van sterke encryptie zal de minister van Economische Zaken opvolging geven aan de strekking van het amendement (TK 2015-2016, 34300 XIII, nr.10) op de begroting van het ministerie van Economische Zaken.

DSB

Datum
4 januari 2016

Ons kenmerk
708641

Minister van Veiligheid en Justitie,

G.A. Van der Steur

Minister van Economische Zaken,

H.G.J. Kamp

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 383

BRIEF VAN DE MINISTERS VAN VEILIGHEID EN JUSTITIE EN VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 januari 2016

Kabinetsstandpunt Encryptie

Hierbij sturen wij u het kabinetsstandpunt toe over encryptie. Hiermee wordt tegemoet gekomen aan de gedane toezeggingen tijdens het AO Telecomraad van 10 juni 2015 (Kamerstuk 21 501-33, nr. 552) en AO JBZ-Raad van 7 oktober 2015 (Kamerstuk 32 317, nr. 357).

Inleiding

Encryptie, ook wel versleuteling, is in toenemende mate eenvoudig te verkrijgen en gebruiken en maakt daarmee steeds vaker onderdeel uit van het reguliere dataverkeer. Door de overheid, bedrijven en burgers wordt encryptie steeds meer toegepast om de vertrouwelijkheid en integriteit van hun communicatie en opgeslagen data te beschermen. Dat is belangrijk voor het vertrouwen van mensen in digitale producten en diensten en voor de Nederlandse economie in het licht van de zich snel ontwikkelende digitale maatschappij. Tegelijkertijd vormt encryptie een belemmering voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer kwaadwillenden (zoals criminelen en terroristen) hiervan gebruikmaken. De recente aanslagen in Parijs, waarbij mogelijk gebruik is gemaakt van versleuteling van de communicatie door de terroristen, leiden tot de gerechtvaardigde vraag wat er nodig is om opsporings-, inlichtingen- en veiligheidsdiensten goed zicht te bieden en laten houden op aanslagplanning.

De in de vorige alinea beschreven tweeledigheid was eveneens te horen in het publieke debat van de afgelopen maanden over de dilemma's rondom het gebruik van encryptie. Ook uw Kamer heeft over dit onderwerp gesproken. Tijdens het AO Telecomraad is gevraagd wat het Kabinet gaat doen aan het stimuleren van sterke encryptie. Daarnaast is vanuit de Tweede Kamer gevraagd om te komen met een kabinetsstandpunt rond encryptie.

kst-26643-383
ISSN 0921 - 7371
's-Gravenhage 2016

Hierna wordt ingegaan op het belang van encryptie voor de systeem- en informatiebeveiliging van de overheid en bedrijven, en voor de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Daarnaast wordt het belang van opsporing van ernstige misdrijven en bescherming van de nationale veiligheid geschetst. Tot slot wordt na weging van de belangen gekomen tot een conclusie.

De Nederlandse situatie kan hierbij niet los worden gezien van de internationale context. Sterke encryptiesoftware is in toenemende mate wereldwijd beschikbaar of al geïntegreerd in producten of diensten. Gelet op de brede beschikbaarheid en toepassing van geavanceerde encryptietechnieken en het grensoverschrijdende karakter van het dataverkeer is het handelingsperspectief op nationaal niveau beperkt.

Belang van encryptie voor de overheid, bedrijven en burgers

Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Veel cybersecuritymaatregelen in organisaties leunen sterk op de toepassing van encryptie. De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups zijn moeilijker zonder het gebruik van encryptie. Het afschermen van gegevens die verstuurd worden via internet, bij internetbankieren bijvoorbeeld, is alleen mogelijk met behulp van encryptie. Door de verbondenheid van systemen, wereldwijde vertakkingen en verschillende routes die communicatie kan afleggen, is het risico op onderschepping, inbreuk, inzage of wijziging van informatie en communicatie altijd aanwezig.

De overheid communiceert in toenemende mate digitaal met de burgers en verleent diensten waarbij vertrouwelijke gegevens worden uitgewisseld, zoals het gebruik van DigiD of het doen van belastingaangifte. Zoals in het Regeerakkoord is geformuleerd moeten vanaf 2017 burgers en bedrijven hun overheidszaken volledig digitaal kunnen regelen. De overheid heeft hierbij de plicht om te zorgen dat deze gegevens tegen kennisneming door derden zijn beveiligd; encryptie is hiervoor onontbeerlijk. Ook de bescherming van de communicatie binnen de overheid is van encryptie afhankelijk zoals bij de beveiliging van diplomatiek berichtenverkeer en militaire communicatie.

Voor bedrijven is encryptie essentieel om bedrijfsinformatie veilig te kunnen bewaren en versturen. Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat voor onder andere startups, datacentra en cloudcomputing. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie, die vooral zit in de digitale economie.

Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers doordat het hen een middel biedt om de vertrouwelijkheid en integriteit van persoonsgegevens en communicatie te beschermen. Dit is ook belangrijk voor de uitoefening van de vrijheid van meningsuiting. Het stelt bijvoorbeeld burgers, maar ook beroepen met een belangrijke democratische functie zoals journalisten, in staat om vertrouwelijk te communiceren.

Encryptie stelt derhalve alle betrokkenen in staat de vertrouwelijkheid en integriteit van communicatie te waarborgen en zich beter te weren tegen bijvoorbeeld spionage en cybercriminaliteit. Hierbij zijn fundamentele rechten en vrijheden, veiligheids- en economische belangen gebaat.

Encryptie en de opsporings-, inlichtingen- en veiligheidsdiensten

De bevoegdheden en middelen die de diensten tot hun beschikking hebben, moeten toegerust zijn op de huidige en toekomstige digitale realiteit. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld. Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die gegevens. Zij ervaren deze belemmeringen bijvoorbeeld wanneer zij onderzoek doen naar de verspreiding en opslag van kinderporno, bij de ondersteuning van militaire missies in het buitenland, het tegengaan van cyberaanvallen of wanneer zij zicht willen krijgen en houden op het voorbereiden van aanslagen door terroristen. Criminelen, terroristen en tegenstanders in gewapende conflicten zijn zich er vaak van bewust dat zij op enig moment de aandacht van de diensten kunnen trekken en hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook zij gebruik kunnen maken. Dat bemoeilijkt, vertraagt, of maakt het onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten. Tevens kan het onderzoek ter zitting en de bewijsvoering voor een veroordeling ernstig worden gehinderd.

Het recht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers

Het toepassen van encryptie helpt burgers zoals eerder werd opgemerkt, bij het borgen van de persoonlijke levenssfeer en de vertrouwelijkheid van hun communicatie. De hierboven genoemde rechtmatige toegang tot gegevens en communicatie door opsporings-, inlichtingen- en veiligheidsdiensten vormt evenwel een inbreuk op de vertrouwelijke communicatie van burgers.

Vertrouwelijkheid van communicatie raakt aan de grondwettelijk geregelde eerbiediging van de persoonlijke levenssfeer en aan het recht op bescherming van het brief-, telefoon- en telegraafgeheim (hierna: «het communicatiegeheim»). Deze grondrechten zijn verankerd in respectievelijk artikel 10 en artikel 13 Grondwet. Daarnaast zijn deze fundamentele rechten vastgelegd in artikel 8 EVRM en artikel 7 en artikel 8 EU-Handvest (voor zover Unierecht wordt geraakt).

De bescherming van grondrechten is van toepassing op de digitale wereld. De hiervoor genoemde grondrechtelijke- en internationaalrechtelijke bepalingen bieden samen het kader om onwettige inbreuken tegen te gaan. De genoemde rechten zijn niet absoluut, hetgeen inhoudt dat beperkingen zijn toegestaan voor zover deze voldoen aan de vereisten die de Grondwet en het EVRM (en voor zover het Unierecht betreft, het EU-Handvest) stellen. Een inbreuk is toelaatbaar wanneer deze een legitiem doel dient, bij wet is geregeld en de beperking voorzienbaar en kenbaar is. Daarnaast dient de beperking noodzakelijk te zijn in een democratische samenleving. Tot slot dient de inbreuk proportioneel te zijn, dat wil zeggen dat het door de overheid nagestreefde doel proportioneel dient te zijn in relatie tot de inbreuk op de persoonlijke levenssfeer en/of het communicatiegeheim.

Deze vereisten bieden het kader waarbinnen de afweging gemaakt kan worden tussen de bij encryptie in het geding zijnde belangen, zoals het

recht op de persoonlijke levenssfeer en het communicatiegeheim, de openbare en nationale veiligheid en het voorkomen van strafbare feiten. Voorgaand afwegingskader is voor zover het de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten betreft overigens ook neergelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (artikelen 18 en 31 van de Wiv 2002). De medewerkingsverplichtingen inzake decryptie die zijn opgenomen in de Wiv (artikelen 24, derde lid en 25, zevende lid van de Wiv 2002) en in het WvSv (artikel 126m, zesde lid, van het WvSv), kunnen worden ingeroepen indien de daaraan gekoppelde bijzondere bevoegdheden na een afweging in voormelde zin worden uitgeoefend.

Afweging en conclusie

Het breken van de versleuteling is tegenwoordig in steeds minder gevallen mogelijk. Daarnaast is de mogelijkheid om gegevens in onversleutelde vorm te vorderen bij een dienstverlener, minder vaak beschikbaar. In toenemende mate worden bij moderne toepassingen van encryptie de gegevens nog slechts in versleutelde vorm door dienstverleners verwerkt. Gelet op het belang van de opsporing en vervolging van strafbare feiten en de belangen die zijn gemoeid met de nationale veiligheid, nopen deze ontwikkelingen tot het zoeken naar nieuwe oplossingen.

Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Door bijvoorbeeld een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zou onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving.

Bij de uitvoering van hun wettelijke taken zijn de opsporings-, inlichtingen- en veiligheidsdiensten deels afhankelijk van samenwerking met aanbieders van ICT-producten en -diensten. Gegeven deze afhankelijkheid, is overleg nodig met aanbieders over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.

Gegeven de voorgaande afweging komen we tot de volgende conclusie:

Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie.

Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en

de afwegingen die daaraan ten grondslag liggen uitdragen. Ten aanzien van het stimuleren van sterke encryptie zal de Minister van Economische Zaken opvolging geven aan de strekking van het amendement (Kamerstuk 34 300 XIII, nr.10) op de begroting van het Ministerie van Economische Zaken.

De Minister van Veiligheid en Justitie,
G.A. van der Steur

De Minister van Economische Zaken,
H.G.J. Kamp

Van: 10.2.e - BD/DGPOL/PBT/R&S 10.2.e @minvenj.nl>
Verzonden: dinsdag 5 januari 2016 20:17
Aan: Bestuursondersteuning
CC: 10.2.e DGPOL; 10.2.e 10.2.e 10.2.e BD/DGPOL/PMP/FMI
Onderwerp: Verzoek om input t.b.v Q&A's AO Politie 14 jauari a.s. n.a.v. Artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken'

Urgentie: Hoog

Beste collega's van Bestuursondersteuning (10.2.e en 10.2.e),

I.v.m. het AO Politie is het verzoek onderstaande vragen n.a.v. het Volkskrant-artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken' d.d. 2 januari 2016 z.s.m. te beantwoorden:

- De Volkskrant citeert in het artikel Inge Philips: 'Maar er moet wel een budget zijn. We kunnen deze agenten niet zonder fatsoenlijke spullen aan het werk zetten. Dan gaan ze gehandicapt van start.' **Welke 'spullen', met name op het gebied van ICT, worden bedoeld? En wanneer moeten deze 'spullen' gereed zijn?**
- De concept IV-portfolio 2016 omvat een project Wet computercriminaliteit III. **Voorziet dit project niet in de realisatie van de 'spullen'? Zo nee, waarom niet? Is de menscapaciteit of het geld de beperkende factor?**
- Er bestaat een project 'In werking brengen digitaal opsporen'. **Maakt dit project geen deel uit van de IV-portfolio 2016? Zo nee, waarom niet?**
- De realisatie van de 'spullen' neemt meerdere jaren in beslag. **Voorziet de meerjarige IV-portfolio 2016-2020 hierin?**
- **Als het geld de beperkende factor is, kan de bijzondere bijdrage van € 13,8 miljoen daarvoor niet worden ingezet?**

Alvast veel dank!

Groeten, 10.2.e

Met vriendelijke groet,

10.2.e

10.2.e
Senior beleidsmedewerker
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Regie en Strategie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
M 10.2.e
10.2.e @minvenj.nl
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 10.2.e) **Namens** 10.2.e
Verzonden: woensdag 6 januari 2016 08:47
Aan: 10.2.e @politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @knp.politie.nl>; Mailbox 10.2.e <10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: FW: Verzoek om input t.b.v Q&A's AO Politie 14 jauari a.s. n.a.v. Artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken'
Urgentie: Hoog

Hoi 10.2.e, 10.2.

DGPol heeft naar aanleiding van het artikel van de Volkskrant zaterdag jl. een aantal vragen tbv het AO Politie d.d. 14 januari (zie mail hieronder). Kunnen jullie dit oppakken ajb? Wanneer zou het jullie lukken om antwoord hierop te geven? Het gehele dossier voor de minister gaat vrijdag a.s. in zijn tas, maar als dit niet haalbaar is, horen we het uiteraard graag. Alvast dank voor je reactie!

Groet,

10.2.e
Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

From: 10.2.e
Sent: Wednesday, January 06, 2016 11:05 AM W. Europe Standard Time
To: Bestuursondersteuning; 10.2.e 10.2.e
Cc: Mailbox Bestuursondersteuning Landelijke Eenheid (LE);10.2.e @politie.nl'; 10.2.e 10.2.e 10.2.e
Subject: RE: Verzoek om input t.b.v Q&A's AO Politie 14 jauari a.s. n.a.v. Artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken'

10.2.e

Graag je actie 10.2.e is vrij vandaag) om onderstaande vragen te beantwoorden en kort te sluiten met 10.2.e voor afstemming met portefeuillehouder.

@10.2.e , graag je input naar 10.2.e mbt laatste bullet

@10.2.e , gepoogd wordt je antwoord te geven voor morgen (donderdag) einde dag.

10.2

Van: 10.2.e
Verzonden: donderdag 7 januari 2016 08:20
Aan: 10.2.e @politie.nl>; 10.2.e
10.2.e @knp.politie.nl>; 10.2.e
@politie.nl>
CC: Mailbox Bestuursondersteuning Landelijke Eenheid (LE)
10.2.e @klpd.politie.nl>; 10.2.e
@politie.nl>; 10.2.e @politie.nl>; 10.2.e
@politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Verzoek om input t.b.v Q&A's AO Politie 14 jauari a.s. n.a.v. Artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken'

Beste 10.2. ,10.2.e

Ik heb vandaag mijn eerste werkdag. Hebben jullie hierover ook al contact gezocht met de LE/ PFH?

Lijkt me goed om het antwoord gezamenlijk te maken. Ik zal in ieder geval de vraag voor de zekerheid daar ook gaan uitzetten.

Groet,

10.2.e

Van: 10.2.e
Verzonden: donderdag 7 januari 2016 09:15
Aan: 10.2.e
CC: 10.2.e
Onderwerp: RE: Verzoek om input t.b.v Q&A's AO Politie 14 jauari a.s. n.a.v. Artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken'
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hoi 10.2.e

Ik zag dat 10.2.e (net als wij bij bestuurszaken LE) de vragen gisteren in CC heeft ontvangen. Ik kan niet voor 10.2.e spreken, maar wij hebben er daarom niets mee gedaan. Inderdaad goed dus om 9 rechtstreeks te benaderen.

Groet, 10.2.e

10.2.e

Senior beleidsadviseur
Politie | Landelijke Eenheid | Staf i.o.
afdeling Bestuursondersteuning
Hoofdstraat 54, 3972 LB Driebergen
Bezoekadres: Lookant 2
Postbus 100, 3970 AC Driebergen

Van: 10.2.e
Verzonden: donderdag 7 januari 2016 12:29
Aan: 10.2.e
CC: 10.2.e 10.2.e
Onderwerp: beantwoording vragen.docx
Urgentie: Hoog

Hoi 10.2.e

Nav. je telefoontje vanochtend nav. mijn mail over de voorbereiding van het AO, heb ik een eerste opzet voor de beantwoording gemaakt.

Ik heb verder nog niemand te pakken kunnen krijgen om mee af te stemmen, ook niet van IV.
Het meest lastige in de beantwoording is dat we waarschijnlijk wel iets moeten zeggen over de stand van zaken van CCIII in het portfolio en of het zo is dat de politie de wet wel kan implementeren. Ik probeer dit nog verder af te stemmen met IV.

Misschien kun jij alvast kijken wat je vindt van deze beantwoordingslijn?

Groet,

10.2.e

From 10.2.e @politie.nl>
Subject **RE: beantwoording vragen.docx**
To 10.2.e @politie.nl>
Date 7 januari 2016 12:48:28 CET

Hoi 10.2.e KEURIG beantwoord! Dit is helemaal zoals ik het ook verwoord had naar de Volkskrant (maar dan in veel minder tekst). Mijn tekst was: als je effectief online wil opsporen in de volle breedte, zul je je personeel ook goed moeten outilleren. Hij schreef: we kunnen niet online opsporen. Klopt niet: we sporen natuurlijk allang onling op. HTC doet niet anders. Maar dat is een klein segment -zij het belangrijk- in het hele cybercrime palet.
De analogie is als het huis: de fundering (voorzieningen om aangifte via internet te doen, Hansken (digitaal beslag etc) en de fijnmazigheid van de voorzieningen tbv digitaal rechercheren) is karig en dat is van invloed op het robuuste dak (HTC). CCIII is de chique dakkapel die we nu op rammelende caravan met het mooie dak zetten.

De stavaza CCIII is dat we zeker op tijd in staat zullen zijn om op kleine schaal de werkzaamheden die nodig zijn te verrichten. Het hele idee van de implementatie is geleidelijkheid, klein beginnen.
MAAR..... 12-14

Heb je zo voldoende?

From: 10.2.e
Sent: Thursday, January 07, 2016 04:54 PM W. Europe Standard Time
To: 10.2.e
Cc: 10.2.e 10.2.e
Subject: beantwoording vragen nav interview.docx

Hallo 10.2.e

Hierbij de versie zoals ik hem wil insturen. Na afstemming met IV en informeel met adviseur DGPol zijn er nog een paar kleine aanpassingen geweest.

Graag je akkoord of eventuele opmerkingen op deze versie. Dan zorg ik voor verzending.

Groet,

10.2.e

From 10.2.e @politie.nl>
Subject **Re: beantwoording vragen nav interview.docx**
To 10.2.e @politie.nl>
Date 7 januari 2016 17:49:18 CET

Volgens mij helemaal goed zo. Mooi genuanceerd en helder dat de basis heel schraal is. Ben benieuwd of t ter sprake komt. Groe10.2.e

Groet,
10.2.e

9
Politie - Landelijke Recherche

Van: 10.2.e
Verzonden: vrijdag 8 januari 2016 09:07
Aan: 10.2.e @politie.nl>
Onderwerp: werving 7-12 CC III

Goede morgen 10.2.e,

Ik heb van 10.2.e de voornemens van de portefeuille Digitalisering & Cybercrime 2016-2018 ontvangen en zie hierin dat voor CCIII een werving 7-12 voor digitale expertise is opgenomen. Ik begrijp van 10.2.e dat jij hierbij bent aangehaakt.

Ik heb haar namelijk de volgende vraag gesteld en de volgende reactie gekregen:

Blz 45 CCIII: Werven en opleiden van medewerkers 7-12 Is dit een invulling van de huidige formatie of een surplus? Hoe verhoudt zich dit tot de voorziene instroom van 7-12 fte digitale expertise? Maakt dit er deel van uit of een surplus?

AS : In eerste instantie zal geprobeerd worden om mee te liften met de instroom van 7-12 fte digitale expertise. Mocht dit niet tot voldoende instroom gaan leiden dan komt de vraag inderdaad aan de orde of er extra geworven moet gaan worden. Dat is op dit moment nog niet te zeggen en ook allemaal sterk afhankelijk van de inrichting van de voorziening voor CCIII. Deze voorziening staat niet in het I&F plan en er zal een wijzigingsverzoek moeten worden gemaakt voordat we nieuwe FTE's kunnen gaan werven. We hebben hierover contact met HRM 10.2.e en zij helpt en begeleidt ons bij dit traject.

Wat is wat jou betreft hiervan de status? Gaat dit al een concrete actie worden of is het nog slechts een wens? Past dit binnen 7-12 fte zij-instroom OS, waarvan 7-12 digitale expertise, zoals in de SPP en de begroting voorzien, of wordt dit een surplus? Als dit een surplus wordt is dit dan wel binnen de formatie, of is het de bedoeling dat er een formatiewijziging plaats vindt (binnen de norm OS 49.802)?

Met vriendelijke groet,

10.2.e
Adviseur

Politie | Directie Financiën & Control | 9
Nieuwe Uitleg 1 | 2514 BP | Den Haag.
Postbus 17107 | 2502 CC | Den Haag
10.2.e @politie.nl
M 06 10.2.e

Van: 10.2.e
Verzonden: maandag 11 januari 2016 08:43
Aan: 10.2.e
Bijlagen: 20160105 - Wet Computercriminaliteit III.pdf

Hoi 10.2.e,

Ik denk dat deze voor jou interessant is?

Met vriendelijke groet,

10.2.e
9

Politie | Directie Operatiën | Werkprocessen en kwaliteit

Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag

M 06 10.2.e

Werkdagen: maandag t/m donderdag

12-14

12-14

12-14

From 10.2.e @politie.nl>
Subject **FW: werving 7-12 fte CC III**
To 10.2.e @politie.nl>
Date 11 januari 2016 15:56:35 CET

10.2.e
9

Politie | Staf Korpsleiding | Directie HRM | 9
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag
M 06 10.2.e

Van: 10.2.e
Verzonden: woensdag 20 januari 2016 16:41
Aan: 10.2.e @politie.nl>
CC: Bestuursondersteuning 10.2.e @knp.politie.nl>
Onderwerp: mogelijk rondetafelgesprek CIII

Hoi 10.2.e

Ter info, bijgaand verzoek wordt morgen bij de PV van VenJ besproken. Grote kans dat het wordt toegekend. Zodra meer bekend, laat ik het weten.

Groet,

10.2.e

Van: 10.2.e @politie.nl]
Verzonden: donderdag 21 januari 2016 13:02
Aan: 10.2.e - BD/DRC/CV; 10.2.e - BD/DGPOL/PBT/PT
CC: 10.2.e - BD/DRC/CV
Onderwerp: FW: mogelijk rondetafelgesprek CIII

Hoi 10.2 , 10.2.e ,

Zoals besproken in het cc-overleg is er inderdaad een verzoek voor een ronde tafel CCIII. Zie cc. We bespraken dat het goed zou zijn dan ook te kijken of (daarvoor) een werkbezoek georganiseerd kan worden.

Ik ga ervan uit dat dit wordt gesteund door Inge Philps/pfh, omdat we daar ook al eerder over hadden gesproken, maar heb die vraag voor de zekerheid uitstaan.

Laat dan svp. nog even weten of jullie de uitnodiging dan kunnen regelen.

Groet,

10.2.e

From: 10.2.e
Sent: Thursday, January 21, 2016 02:31 PM W. Europe Standard Time
To: 10.2.e
Cc: 10.2.e ; 10.2.e
Subject: CCIII

Hoi 10.2.e

Ter info. Gisteren was er een AO Cyber Security. Omdat dit AO nu eerder viel dan het AO politie (dat al een aantal keer is uitgesteld) hadden we voor de zekerheid de vragen over CCII nav. het interview aangeleverd die we eerder al hadden voorbereid.
Er werd inderdaad kort ingegaan op het interview door 9 , en er is dus in de lijn zoals afgestemd geantwoord dat het meer een algemeen signaal was over het belang van goede ICT voorzieningen.

Verder is het goed om te weten dat de TK waarschijnlijk een ronde tafel gesprek over CCIII wil organiseren. Zie ook de cc met het verzoek.
Zodra daar mee informatie over is hoor je het.
We hebben het er eerder over gehad om de vaste Kamercommissie, net als bij dataretentie, uit te nodigen voor een werkbezoek over CCIII. Het lijkt verstandig dit werkbezoek dan te houden voor de Ronde Tafel, aangezien er bij een ronde tafel altijd veel meer partijen aanwezig zijn en er ook minder tijd beschikbaar is per organisatie om je punt te maken.

Laat svp. weten of je je kunt vinden in het organiseren van een werkbezoek, dan pak ik dat op met V&J en in afstemming met jou.

Verder nog goed om te weten dat er een kabinetsstandpunt is gevraagd en toegezegd over het gebruik van 0-days. Ik begreep al van 10.2.e dat dat dan vooral met DLOS moet worden afgestemd, maar ook voor jou interessant.

Groet
10.2.e

10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën | 9
Nieuwe Uitleg 1, 2514 BP, Den Haag
M 06 10.2.e
E 10.2.e @politie.nl
Werkdagen: ma, di, do, vrij

From 10.2.e @politie.nl>
Subject **Re: CCIII**
To 10.2.e @politie.nl>
Date 21 januari 2016 14:44:12 CET

Dank voor je bericht 10.2.e Akkoord met bezoek voorafgaand aan ronde tafel. 0-day is vooral een CC3 aangelegenheid! Dus graag wel degelijk via ons.
Groet Inge

Groet,
Inge Philips

Plv Diensthoofd
Politie - Landelijke Recherche

Van: 10.2.e - BD/DWJZ/SSR
Verzonden: donderdag 21 januari 2016 16:40
Aan: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e . - BD/DRC/CV
CC: 10.2.e - BD/DWJZ/JZ
Onderwerp: Ronde tafel computercriminaliteit III

Hallo 10. , 10.2.e en 10.2.e , 10.2.e belden mij zojuist. De griffie van de Tweede Kamer heeft hem gebeld met de vraag om namen van deskundigen voor de ronde tafel bijeenkomst in de Kamer over het wetsvoorstel computercriminaliteit III. Graag namen van politie, OM en andere deskundigen (wetenschap, rechterlijke macht e.d.).

Ik dacht aan:
OM: 10.2.e en 10.2.e
Politie: twee nader aan te wijzen vertegenwoordigers
Rechterlijke macht: 10.2.e c.q. 10.2.e c.q. 10.2.e ?
IT-wereld: 10.2.e ?
Wetenschap: 10.2.e c.q. 10.2.e ?

Graag vandaag en morgen even contact, we moeten namelijk uiterlijk morgen de namen doorgeven.

Gr. 10.2

From: 10.2.e - BD/DRC/CV
Sent: donderdag 21 januari 2016 16:46:13
To: 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
Cc: 10.2.e . - BD/DWJZ/JZ; 10.2.e @politie.nl); 10.2.e - BD/DGPOL/PBT/PT; 10.2.e - BD/DGPOL/PBT/PT
Subject: RE: Ronde tafel computercriminaliteit III

Ben met je eens:
Voor politie (Inge Philipse en via haar iemand van THTC, denk ik (overleg met ondersteuning korpsleiding (9), via DGPOL

Voor OM inderdaad : 10.2.e en 10.2.e
Academici: 10.2.e

Europol: 10.2.e

Dit is uitkomst van de brainstorm van 10.2.e en mij.

10.2.e

9

.....
Law Enforcement Department
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag |
Postbus 20301 | 2500 EH | Den Haag
.....

Van: 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>
Verzonden: donderdag 21 januari 2016 16:59
Aan: 10.2.e
CC: 10.2.e . - BD/DGPOL/PBT/PT; 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: RE: mogelijk rondetafelgesprek CIII
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hoi 10.2.e

Is net via de politie assistent ook bevestigd. Ga aangegeven dat Inge Philips een goede is en een via jou aan ons te communiceren door haar aan te wijzen persoon.

Graag bevestigen.

10.2.e
9
.....
Law Enforcement Department
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag |
Postbus 20301 | 2500 EH | Den Haag
www.rijksoverheid.nl/venj
.....

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: donderdag 21 januari 2016 17:01
Aan: 10.2.e - BD/DRC/CV; 10.2.e . - BD/DWJZ/SSR; 10.2.e
- BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - DGPOL; 10.2.e
BD/DGPOL/PBT/PT
CC: 10.2.e - BD/DWJZ/JZ; 10.2.e 10.2.e
BD/DGPOL/PBT/PT; 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: RE: Ronde tafel computercriminaliteit III

Hoi, voor politie zal parlementair dgpol cluster dit laten lopen via bestuurszaken korpsleiding.
@ parlementair kunnen jullie dit oppakken?

Ik snap dat enige haast is geboden maar waarom moet dit al morgen? Eerdere verzoeken kregen we meer tijd.

Groet 10.2.e

Van: 10.2.e @minvenj.nl]
Verzonden: donderdag 21 januari 2016 17:20
Aan: 10.2.e @knp.politie.nl>
CC: 10.2.e minvenj.nl>
Onderwerp: Ronde tafel computercriminaliteit III

Beste collega's,

Zojuist kregen we het verzoek om namen van deskundigen door te geven voor de ronde tafel bijeenkomst in de Kamer over het wetsvoorstel computercriminaliteit III.
Het gaat om deskundigen die daarbij aanwezig kunnen zijn vanuit politie, OM en andere deskundigen (wetenschap, rechterlijke macht e.d.).

Hierbij werd al even een suggestie gedaan voor politie:
Inge Philipse en via haar iemand van THTC

Het verzoek lijkt enige haast te hebben, ze zouden graag morgen al twee namen van vertegenwoordigers willen krijgen.

Zouden jullie kunnen kijken wie er vanuit de politie kan aansluiten?

Ik hoor graag even van jullie.

Met vriendelijke groet,

10.2.e

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
DGPOL
Turfmarkt 147 | 2511 DP | Den Haag | 24ste etage
Postbus 20301 | 2500 EH | Den Haag

Van: 10.2.e
Verzonden: vrijdag 22 januari 2016 11:33
Aan: 10.2.e
CC: Bestuursondersteuning
Onderwerp: besluitenlijst VenJ - CIII
Bijlagen: Besluitenlijst_commissie_Veiligheid_en_Justitie_21_januari_2016[1].pdf

Hoi 10.2.e

Over je vraag over de datum van de hoorzitting, ik krijg de griffie van de cie venj even niet te pakken, maar in de besluitenlijst staat dat het rondetafelgesprek voor 18 februari georganiseerd zou moeten worden. De cie moet dan schriftelijke inbreng aanleveren, dus uit beleefdheid en om de beleidsmedewerkers tijd te geven om de schriftelijke inbreng te doen, zal waarschijnlijk het rondetafelgesprek (uiterlijk) ong. een week voor 18 februari plaatsvinden. Als ik meer te weten kom, laat ik het weten.

Gr.,
10.2.

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 21 januari 2016

HERZIENE BESLUITENLIJST (i.v.m. toevoeging agendapunt 75*)

Voortouwcommissie: **vaste commissie voor Veiligheid en Justitie**

Volgcommissie(s):

BiZa	i.v.m. agendapunt	26, 57, 58, 64, 65, 66, 67, 84
BuHa-OS	i.v.m. agendapunt	31, 73, 84
BuZa	i.v.m. agendapunt	33, 55, 63, 73, 84
DEF	i.v.m. agendapunt	55, 84
EU	i.v.m. agendapunt	2, 32, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 84
EZ	i.v.m. agendapunt	26, 30, 31, 46, 61, 62, 84
FIN	i.v.m. agendapunt	1, 16, 26, 84
I&M	i.v.m. agendapunt	64, 65, 84
IPC Art. 13	i.v.m. agendapunt	84
IPC Energie	i.v.m. agendapunt	84
IPC GBVB	i.v.m. agendapunt	84
IPC Mens	i.v.m. agendapunt	84
KR	i.v.m. agendapunt	84
OCW	i.v.m. agendapunt	26, 61, 84
SZW	i.v.m. agendapunt	26, 41, 84
VWS	i.v.m. agendapunt	26, 35, 40, 84
WR	i.v.m. agendapunt	26, 84

Document: **Besluitenlijst van de procedurevergadering van donderdag 21 januari 2016**

Wet- en regelgeving

1. Agendapunt: **Wijziging van de Wet op de kansspelen, de Wet op de kansspelbelasting en enkele andere wetten in verband met het organiseren van kansspelen op afstand**

Zaak: Wetgeving - staatssecretaris van Veiligheid en Justitie, F. Teeven - 21 juli 2014
Wijziging van de Wet op de kansspelen, de Wet op de kansspelbelasting en enkele andere wetten in verband met het organiseren van kansspelen op afstand - 33996
Besluit: Reeds aangemeld voor plenaire behandeling.
Volgcommissie(s): FIN

Zaak: Nota naar aanleiding van het (nader) verslag - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 15 december 2015
Nota naar aanleiding van het nader verslag - 33996-12
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.
Volgcommissie(s): FIN

Zaak: Nota van wijziging - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 15 december 2015
Tweede nota van wijziging - 33996-13
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.
Volgcommissie(s): FIN

2. Agendapunt: **Uitvoering van de op 28 juni 2006 te Wenen tot stand gekomen Overeenkomst tussen de Europese Unie en de Republiek IJsland en het Koninkrijk Noorwegen betreffende de procedures voor overlevering tussen de lidstaten van de Europese Unie en IJsland en Noorwegen (Pb EU L 292)**

Zaak: Wetgeving - minister van Veiligheid en Justitie, G.A. van der Steur - 16 december 2015
Uitvoering van de op 28 juni 2006 te Wenen tot stand gekomen Overeenkomst tussen de Europese Unie en de Republiek IJsland en het Koninkrijk Noorwegen betreffende de procedures voor overlevering tussen de lidstaten van de Europese Unie en IJsland en Noorwegen (Pb EU L 292) - 34365

Besluit: Inbrengdatum voor het verslag vastgesteld op 11 februari 2016.

Volgcommissie(s): EU

3. Agendapunt: **Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)**

Zaak: Wetgeving - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 21 december 2015
Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) - 34372

Besluit: Inbrengdatum voor het verslag vastgesteld op 18 februari 2016.

Zaak: Brief van lid/fractie/commissie - Tweede Kamerlid, K. Verhoeven (D66) - 20 januari 2016
Verzoek om rondetafelgesprek over Wet Computercriminaliteit III - 2016Z00960

Besluit: Voor 18 februari zal een rondetafelgesprek worden georganiseerd over het wetsvoorstel.

Besluit: Er zal worden geïnventariseerd welke personen/organisaties de commissie voor het rondetafelgesprek wenst uit te nodigen. Het voorstel met een opzet voor het rondetafelgesprek wordt per e-mail ter goedkeuring aan de commissie voorgelegd.

4. Agendapunt: **Wijziging van de Wet toezicht en geschillenbeslechting collectieve beheersorganisaties in verband met de implementatie van Richtlijn 2014/26/EU van het Europees Parlement en de Raad betreffende het collectieve beheer van auteursrechten en naburige rechten en de multiterritoriale licentieverlening van rechten inzake muziekwerken voor het online gebruik ervan op de interne markt (Implementatiewet richtlijn collectief beheer)**

Zaak: Wetgeving - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 30 juni 2015
Wijziging van de Wet toezicht en geschillenbeslechting collectieve beheersorganisaties in verband met de implementatie van Richtlijn 2014/26/EU van het Europees Parlement en de Raad betreffende het collectieve beheer van auteursrechten en naburige rechten en de multiterritoriale licentieverlening van rechten inzake muziekwerken voor het online gebruik ervan op de interne markt (Implementatiewet richtlijn collectief beheer) - 34243
Besluit: Aanmelden voor plenaire behandeling.

Zaak: Nota naar aanleiding van het (nader) verslag - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Nota naar aanleiding van het verslag - 34243-6
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.

Zaak: Nota van wijziging - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Nota van wijziging - 34243-7
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.

5. Agendapunt: **Implementatie van richtlijn 2012/29/EU van het Europees Parlement en de Raad van 25 oktober 2012 tot vaststelling van minimumnormen voor de rechten, de ondersteuning en de bescherming van slachtoffers van strafbare feiten, en ter vervanging van Kaderbesluit 2001/220/JBZ (PbEU 2012, L 315)**

Zaak: Wetgeving - minister van Veiligheid en Justitie, G.A. van der Steur - 24 juni 2015
Implementatie van richtlijn 2012/29/EU van het Europees Parlement en de Raad van 25 oktober 2012 tot vaststelling van minimumnormen voor de rechten, de ondersteuning en de bescherming van slachtoffers van strafbare feiten, en ter vervanging van Kaderbesluit 2001/220/JBZ (PbEU 2012, L 315) - 34236
Besluit: Aanmelden voor plenaire behandeling.
Noot: Implementatiedatum: 16 november 2015.

Zaak: Nota naar aanleiding van het (nader) verslag - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Nota naar aanleiding van het verslag - 34236-8
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.

Zaak: Nota van wijziging - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Nota van wijziging - 34236-9
Besluit: Betrekken bij de verdere behandeling van het wetsvoorstel.

6. Agendapunt: **Wijziging van Boek 2 van het Burgerlijk Wetboek ter uitvoering van Richtlijn 2014/95/EU van het Europees Parlement en de Raad van 22 oktober 2014 tot wijziging van richtlijn 2013/34/EU met betrekking tot de bekendmaking van niet-financiële informatie en informatie inzake diversiteit door bepaalde grote ondernemingen en groepen (PbEU 2014, L 330)**

Zaak: Wetgeving - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Wijziging van Boek 2 van het Burgerlijk Wetboek ter uitvoering van Richtlijn 2014/95/EU van het Europees Parlement en de Raad van 22 oktober 2014 tot wijziging van richtlijn 2013/34/EU met betrekking tot de bekendmaking van niet-financiële informatie en informatie inzake diversiteit door bepaalde grote ondernemingen en groepen (PbEU 2014, L 330) - 34383

Besluit: Inbrengdatum voor het verslag vaststellen op 18 februari 2016.

7. Agendapunt: **Tweede nota van wijziging**

Zaak: Nota van wijziging - minister van Veiligheid en Justitie, G.A. van der Steur - 13 januari 2016
Tweede nota van wijziging - 33799-12

Besluit: Betrokken bij de verdere behandeling van het wetsvoorstel.

8. Agendapunt: **Overzicht wetsvoorstellen, wetgevingsoverleggen en (dertigleden)debatten**

Zaak: Stafnotitie - 3 december 2015
Overzicht wetsvoorstellen, wetgevingsoverleggen en (dertigleden)debatten - 2015Z23420

Besluit: De Griffie Plenair zal worden verzocht de volgende wetsvoorstellen in onderstaande volgorde te agenderen:

1. Voorstel van wet van het lid Bosman houdende regulering van de vestiging van Nederlanders van Aruba, Curaçao en Sint Maarten in Nederland (Wet regulering vestiging van Nederlanders van Aruba, Curaçao en Sint Maarten in Nederland) (33325)*;
2. Voorstel van wet van het lid Voordewind tot strafbaarstelling van het in de openbaarheid ontkennen, op grove wijze bagatelliseren, goedkeuren of rechtvaardigen van volkerenmoord (strafbaarstelling negationisme) (30579)*;
3. Voorstel van wet van de leden Swinkels, Recourt en Van Oosten tot wijziging van Boek 1 van het Burgerlijk Wetboek en de Faillissementswet teneinde de omvang van de wettelijke gemeenschap van goederen te beperken (33987)*;
4. Implementatie van richtlijn 2012/29/EU van het Europees Parlement en de Raad van 25 oktober 2012 tot vaststelling van minimumnormen voor de rechten, de ondersteuning en de bescherming van slachtoffers van strafbare feiten, en ter vervanging van Kaderbesluit 2001/220/JBZ (PbEU 2012, L 315) (34236);
5. Implementatie van richtlijn nr. 2013/48/EU van het Europees Parlement en de Raad van 22 oktober 2013 betreffende het recht op toegang tot een advocaat in strafprocedures en in procedures ter uitvoering van een Europees aanhoudingsbevel en het recht om een derde op de hoogte te laten brengen vanaf de vrijheidsbeneming en om met derden en consulaire autoriteiten te communiceren tijdens de vrijheidsbeneming (PbEU L294) (34157);
6. Wijziging van het Wetboek van Strafvordering en enige andere wetten in verband met aanvulling van bepalingen over de verdachte, de raadsman en enkele dwangmiddelen (34159);

7. Voorstel van wet van de leden Segers, Volp en Kooiman tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafrecht BES, houdende de invoering van de strafbaarstelling van misbruik van prostitué(e)s die slachtoffer van mensenhandel zijn (Wet strafbaarstelling misbruik prostitué(e)s die slachtoffer zijn van mensenhandel) (34091);
8. 8. Wijziging van de Wet regulering prostitutie en bestrijding misstanden seksbranche (33885);
9. Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met een herziening van de wettelijke regeling van de tenuitvoerlegging van strafrechtelijke beslissingen (Wet herziening tenuitvoerlegging strafrechtelijke beslissingen) (34086);
10. Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie (Kamerstuk 33542);
11. Wijziging van de Wet rechtspositie rechterlijke ambtenaren en enige andere wetten in verband met de uitbreiding van de mogelijkheden om ten aanzien van voor het leven benoemde rechterlijke ambtenaren disciplinaire maatregelen op te leggen en tevens andere maatregelen te treffen (Kamerstuk 33861);
12. Wijziging van de Gerechtsdeurwaarderswet in verband met de evaluatie van het functioneren van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders, alsmede de regeling van enkele andere onderwerpen in die wet (34047);
13. Wijziging van de Advocatenwet, de Gerechtsdeurwaarderswet en de Wet op het notarisambt in verband met het doorberekenen van de kosten van toezicht en tuchtrechtspraak aan de beroepsgroepen (Wet doorberekening kosten toezicht en tuchtrecht juridische beroepen) (34145);
14. Wijziging van de Wet op de kansspelen, de Wet op de kansspelbelasting en enkele andere wetten in verband met het organiseren van kansspelen op afstand (33996);
15. Wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken (digitale processtukken Strafvordering) (34090);
16. Wijziging van het Wetboek van Strafvordering tot vastlegging van het recht op bronbescherming bij vrije nieuwsgaring (bronbescherming in strafzaken) (34032);
17. Wijziging van de Rijkswet op het Nederlanderschap ter verlenging van de termijnen voor verlening van het Nederlanderschap en enige andere wijzigingen (33852(R2023));
18. Aanpassing van Rijkswetten in verband met de invoering van de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht en van de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering in verband met vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie alsmede in verband met de uitbreiding van prejudiciële vragen aan de Hoge Raad (Invoeringsrijkswet vereenvoudiging en digitalisering procesrecht en uitbreiding prejudiciële vragen) (34237-(R2054));
19. Wijziging van de Wet toezicht en geschillenbeslechting collectieve beheersorganisaties in verband met de implementatie van Richtlijn 2014/26/EU van het Europees Parlement en de Raad betreffende het collectieve beheer van auteursrechten en naburige rechten en de multiterritoriale licentieverlening van rechten inzake muziekwerken voor het online gebruik ervan op de interne markt (Implementatiewet richtlijn collectief beheer) (34243).

Noot: * Wacht op initiatiefnemer(s).

Brieven minister van Veiligheid en Justitie

9. Agendapunt: **Spoedeisende wetsvoorstellen (Veiligheid en Justitie)**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 11 december 2015
Spoedeisende wetsvoorstellen (Veiligheid en Justitie) - 34300-67

Besluit: Voor kennisgeving aangenomen.

10. Agendapunt: **Uitstel toezending brief inzake toezicht en handhaving in de openbare ruimte**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 11 december 2015
Uitstel toezending brief inzake toezicht en handhaving in de openbare ruimte - 28684-457

Besluit: Voor kennisgeving aangenomen.

11. Agendapunt: **Beleidsreactie op het WODC-onderzoek over de privacy van slachtoffers**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Beleidsreactie op het WODC-onderzoek over de privacy van slachtoffers - 33552-17

Besluit: Agenderen voor een algemeen overleg over slachtofferbeleid; algemeen overleg plannen.

12. Agendapunt: **Voortgangsbrief over de uitvoering van de motie Dijksma tot invoering van een Nederlandse collectieve schadevergoedingsactie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Voortgangsbrief over de uitvoering van de motie Dijksma tot invoering van een Nederlandse collectieve schadevergoedingsactie - 31762-4

Besluit: Voor kennisgeving aangenomen; aangekondigde wetsvoorstel afwachten.

13. Agendapunt: **Uitstel beantwoording Kamervragen n.a.v. Rapport Cie. Oosting**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Uitstel beantwoording Kamervragen n.a.v. Rapport Commissie Oosting - 34362-3

Besluit: Voor kennisgeving aangenomen.

14. Agendapunt: **Reactie op het rapport 'Verkenning naar een landelijk klachtenloket voor sekswerkers'**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 15 december 2015
Reactie op het rapport 'Verkenning naar een landelijk klachtenloket voor sekswerkers' - 34193-2

Besluit: Agenderen voor algemeen het overleg over mensenhandel en prostitutie op 11 februari 2016.

15. Agendapunt: **Rapport Onderzoekscommissie ontnemingsschikking en Rapport Erfgoedinspectie door de commissie Oosting**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 9 december 2015
Rapport Onderzoekscommissie ontnemingsschikking en Rapport Erfgoedinspectie (commissie Oosting) - 34362-1

Besluit: Betrokken bij het debat over het rapport van de Commissie Oosting op 16 december 2015.

16. Agendapunt: **Beantwoording Kamervragen n.a.v. Rapport Cie. Oosting en de Erfgoedinspectie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 15 december 2015
Beantwoording vragen commissie over het rapport Onderzoekscommissie ontnemingsschikking en Rapport Erfgoedinspectie (commissie Oosting) - 34362-5

Besluit: Betrokken bij het debat over het rapport van de Commissie Oosting op 16 december 2015.

Volgcommissie(s): FIN

17. Agendapunt: **Toestemming voor deelname van de algemeen directeur Raad voor de Kinderbescherming aan het rondetafelgesprek over kindermisbruik**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Toestemming voor deelname van de algemeen directeur Raad voor de Kinderbescherming aan het rondetafelgesprek over kindermisbruik - 2015Z24774

Besluit: Voor kennisgeving aangenomen.

18. Agendapunt: **Wob-verzoek ontslagcijfers politieambtenaren**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Besluit van de politie op het Wob-verzoek van RTL Nieuws inzake ontslagcijfers politieambtenaren - 28844-90

Besluit: Betrekken bij het plenair debat over de screening bij de politie.

19. Agendapunt: **Verzamelbrief Veiligheidsregio's en IFV**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Verzamelbrief Veiligheidsregio's en Instituut Fysieke Veiligheid (IFV) - 29517-107

Besluit: Agenderen voor het algemeen overleg over nationale veiligheid, crisisbeheersing en brandweerzorg; algemeen overleg plannen.

Besluit: De minister van Veiligheid en Justitie zal worden verzocht te reageren op de uitzending van één vandaag van 18 januari 2015 inzake leegloop van vrijwillige brandweerkorpsen, alsmede een nader reactie te geven op beantwoording van de mondelinge vragen terzake van het lid Kooiman en deze vóór het algemeen overleg aan de Kamer te zenden.

20. Agendapunt: **Reactie op het artikel "Maastricht had geen eerlijke kans op rechtbank”**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Reactie op het artikel "Maastricht had geen eerlijke kans op rechtbank” - 32891-31

Besluit: Agenderen voor het te zijner tijd te houden algemeen overleg rechtspraak.

21. Agendapunt: **Tweede monitoringsrapportage arrondissementen Gelderland en Overijssel**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Aanbieding tweede monitoringsrapportage arrondissementen Gelderland en Overijssel - 29279-293

Besluit: Voor kennisgeving aangenomen.

22. Agendapunt: **Standpunt op het eerste rapport van de commissie Evaluatie Politiewet 2012**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Standpunt op het eerste rapport van de commissie Evaluatie Politiewet 2012 - 29628-598

Besluit: Geagendeerd voor het algemeen overleg over politie op 28 januari 2016.

23. Agendapunt: **Onderhandelingsresultaat Arbeidsvoorwaarden Sector Politie 2015-2017**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 18 december 2015
Onderhandelingsresultaat Arbeidsvoorwaarden Sector Politie 2015-2017 - 29628-599

Besluit: Geagendeerd voor het algemeen overleg over politie op 28 januari 2016.

24. Agendapunt: **Afronding en borging Programma Versterking Professionele Weerbaarheid Politie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 18 december 2015
Afronding en borging Programma Versterking Professionele Weerbaarheid Politie - 29628-600

Besluit: Geagendeerd voor het algemeen overleg over politie op 28 januari 2016.

25. Agendapunt: **Voortgang wetgevingsprogramma herijking faillissementsrecht**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 21 december 2015
Voortgang wetgevingsprogramma herijking faillissementsrecht - 33695-10

Besluit: Voor kennisgeving aangenomen.

26. Agendapunt: **Voortgang rijksbrede aanpak van fraude**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 21 december 2015
Voortgang rijksbrede aanpak van fraude - 17050-525

Besluit: Agenderen voor een algemeen overleg over fraude; algemeen overleg plannen.

Volgcommissie(s): SZW, EZ, VWS, BiZa, WR, OCW, FIN

27. Agendapunt: **Voortgang programma Versterking Prestaties Strafrechtketen**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 21 december 2015
Voortgang programma Versterking Prestaties Strafrechtketen - 29279-295

Besluit: Agenderen voor een te zijner tijd te voeren algemeen overleg over strafrechtelijke onderwerpen.

28. Agendapunt: **Privacy Voetbalvolgsysteem**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 4 januari 2016
Privacy Voetbalvolgsysteem (VVS) - 29628-601

Besluit: Voor kennisgeving aangenomen.

29. Agendapunt: **Heroriëntatie landelijke meldkamerorganisatie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 4 januari 2016
Heroriëntatie landelijke meldkamerorganisatie (LMO) - 29517-108

Besluit: Agenderen voor te zijner tijd te voeren algemeen overleg over nationale veiligheid, crisisbeheersing en brandweerzorg.

Besluit: Agenderen voor het algemeen overleg politie op 28 januari 2016.

30. Agendapunt: **Kabinetsstandpunt encryptie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 4 januari 2016
Kabinetsstandpunt encryptie - 26643-383

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EZ

31. Agendapunt: **Voortgangsbrief economische veiligheid**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 4 januari 2016
Voortgangsbrief economische veiligheid - 30821-27

Besluit: Agenderen voor te zijner tijd te voeren algemeen overleg over nationale veiligheid, crisisbeheersing en brandweerzorg.

Volgcommissie(s): EZ, BuHa-OS

32. Agendapunt: **EU-pakket bescherming persoonsgegevens**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
EU-pakket bescherming persoonsgegevens - 32761-91
Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.
Volgcommissie(s): EU

33. Agendapunt: **Goedkeuring van de Overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit (Trb. 2010, 321)**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Goedkeuring van de Overeenkomst tussen de Regering van het Koninkrijk der Nederlanden en de Regering van de Verenigde Staten van Amerika inzake verbetering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit (Trb. 2010, 321) - 33603-6
Besluit: Voor kennisgeving aannemen; nadere informatie afwachten.
Volgcommissie(s): BuZa

34. Agendapunt: **Nadere toelichting op het amendement van de leden Van der Staaij en Bisschop dat regelt dat het al dan niet aansluitend ten uitvoer leggen van straffen geen invloed heeft op de totale detentieduur (Kamerstuk 34 086, nr. 11)**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Nadere toelichting op het amendement van de leden Van der Staaij en Bisschop dat regelt dat het al dan niet aansluitend ten uitvoer leggen van straffen geen invloed heeft op de totale detentieduur (Kamerstuk 34 086, nr. 11) - 34086-21
Besluit: Betrekken bij de voortzetting van de plenaire behandeling van het wetsvoorstel Wet herziening tenuitvoerlegging strafrechtelijke beslissingen (34086).

35. Agendapunt: **Aanpak problematiek loverboys**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Aanpak problematiek loverboys - 31839-500
Besluit: De commissie Volksgezondheid, Welzijn en Sport zal worden verzocht de behandeling over te nemen in verband met het algemeen overleg over slachtoffers loverboys.
Volgcommissie(s): VWS

36. Agendapunt: **Reactie op ongevraagd advies Afdeling advisering Raad van State inzake sanctiestelsels (Stcrt. 2015, nr. 30280)**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 11 januari 2016
Reactie op ongevraagd advies Afdeling advisering Raad van State inzake sanctiestelsels (Stcrt. 2015, nr. 30280) - 34300-VI-72
Besluit: Agenderen voor een te zijner tijd te voeren algemeen overleg over bestuursrecht.

37. Agendapunt: **Landelijk Beeld Jaarwisseling 2015-2016**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Landelijk Beeld Jaarwisseling 2015-2016 - 28684-459

Besluit: Agenderen voor nog te plannen algemeen overleg Landelijk Beeld Jaarwisseling 2015-2016.

38. Agendapunt: **Beleidsregels Autoriteit persoonsgegevens**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Beleidsregels Autoriteit persoonsgegevens - 33662-26

Besluit: Agenderen voor te zijner tijd te voeren algemeen overleg over privacy.

39. Agendapunt: **Werkprogramma Inspectie Veiligheid en Justitie 2016**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 12 januari 2016
Aanbieding Werkprogramma Inspectie Veiligheid en Justitie 2016 - 34300-VI-73

Besluit: Voor kennisgeving aangenomen.

40. Agendapunt: **Reactie op het bericht dat het ziekenhuis Isala te Zwolle een vondelingenkamer opent**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 13 januari 2016
Reactie op het bericht dat het ziekenhuis Isala te Zwolle een vondelingenkamer opent - 31839-501

Besluit: Agenderen voor te zijner tijd te voeren algemeen overleg over vondelingenkamer.

Volgcommissie(s): VWS

41. Agendapunt: **Slachtofferbeleid en screening kinderopvang**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 13 januari 2016
Slachtofferbeleid en screening kinderopvang - 33552-18

Besluit: Agenderen voor het algemeen overleg over slachtofferbeleid. De vaste commissie voor Sociale Zaken en Werkgelegenheid zal als volgcommissie worden aangemerkt.

Volgcommissie(s): SZW

42. Agendapunt: **Reactie op het verzoek van het lid Omtzigt, gedaan tijdens de Regeling van werkzaamheden d.d. 12 januari 2016, over de kwestie rond professor Maat**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 januari 2016
Reactie op het verzoek van het lid Omtzigt, gedaan tijdens de Regeling van werkzaamheden d.d. 12 januari 2016, over de kwestie rond professor Maat - 33997-57

Besluit: Betrekken bij het plenair debat over de kwestie rond professor Maat.

43. Agendapunt: **Uitspraak Hoge Raad over verhoorbijstand**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 15 januari 2016
Uitspraak Hoge Raad over verhoorbijstand - 31753-111

Besluit: Voor kennisgeving aannemen; nadere informatie afwachten.

44. Agendapunt: **Voordracht kroonbenoeming van de heer E.S.M. (Erik) Akerboom als korpschef van politie**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 15 januari 2016
Voordracht kroonbenoeming van de heer E.S.M. (Erik) Akerboom als korpschef van politie - 29628-602

Besluit: Voor kennisgeving aangenomen.

Brieven staatssecretaris van Veiligheid en Justitie

45. Agendapunt: **Afzondering en visuele schouw in vreemdelingenbewaring**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 11 december 2015
Afzondering en visuele schouw in vreemdelingenbewaring - 19637-2108

Besluit: Betrekken bij de behandeling van de Wet terugkeer en vreemdelingenbewaring (Kamerstuk 34309).

Besluit: Geagendeerd voor het algemeen overleg over opvang, terugkeer en vreemdelingenbewaring op 19 januari 2016.

Besluit: Agenderen voor het algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016. Het algemeen overleg wordt met een uur verlengd.

46. Agendapunt: **Doorstroom startups in de zelfstandigenregeling**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 14 december 2015
Doorstroom startups in de zelfstandigenregeling - 30573-133

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

Volgcommissie(s): EZ

47. Agendapunt: **Onderzoek naar de beleidstheorie van de Modernisering van Kansspelen en het opstellen van een evaluatiekader**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 15 december 2015
Onderzoek naar de beleidstheorie van de Modernisering van Kansspelen en het opstellen van een evaluatiekader - 24557-137

Besluit: Agenderen voor het te zijner tijd te houden algemeen overleg over kansspelbeleid.

48. Agendapunt: **Continuering aanpak schijnhuwelijken**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 17 december 2015
Continuering aanpak schijnhuwelijken - 32175-59

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

49. Agendapunt: **Reactie op voorstellen vereniging EMDR Nederland**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 18 december 2015
Reactie op voorstellen vereniging EMDR Nederland - 19637-2110

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

50. Agendapunt: **Inventarisatie lijsten veilige landen van herkomst in andere lidstaten**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 5 januari 2016
Inventarisatie lijsten veilige landen van herkomst in andere lidstaten - 19637-2113

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

51. Agendapunt: **Reactie op de brief van het BelangenOverleg Niet Justitiegebonden Organisaties (BONJO) inzake de behandeling van de begroting van het ministerie van Veiligheid en Justitie voor het jaar 2016**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 5 januari 2016
Reactie op de brief van het BelangenOverleg Niet Justitiegebonden Organisaties (BONJO) inzake de behandeling van de begroting van het ministerie van Veiligheid en Justitie voor het jaar 2016 - 2016Z00040

Besluit: Voor kennisgeving aangenomen.

52. Agendapunt: **Toelichting op het aantal Dublinclaims in 2014 en 2015**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 5 januari 2016
Toelichting op het aantal Dublinclaims in 2014 en 2015 - 19637-2114

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

53. Agendapunt: **Wijziging toelatingsregeling buitenlandse investeerders**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 8 januari 2016
Wijziging toelatingsregeling buitenlandse investeerders - 30573-134

Besluit: Agenderen voor algemeen overleg over vreemdelingen- asielbeleid op 4 februari 2016.

54. Agendapunt: **Publicatie Rapportage Vreemdelingenketen**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 12 januari 2016
Informatie over de publicatie van de Rapportage Vreemdelingenketen (RVK) - 19637-2115

Besluit: Agenderen voor algemeen overleg over vreemdelingen- en asielbeleid op 4 februari 2016.

55. Agendapunt: **Nederlandse inzet in Frontex-operaties in 2016**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 12 januari 2016
Nederlandse inzet in Frontex-operaties in 2016 - 32317-379

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016 (JBZ-onderwerpen op het terrein van asiel- en vreemdelingenbeleid).

Volgcommissie(s): BuZa, DEF

56. Agendapunt: **Reactie op het rapport 'Als ik bezig ben, denk ik niet zoveel. Evaluatie van de pilot activeren bewoners gezinslocatie'**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 12 januari 2016
Aanbieding en reactie op het rapport 'Als ik bezig ben, denk ik niet zoveel. Evaluatie van de pilot activeren bewoners gezinslocatie' - 19637-2116

Besluit: Geagendeerd voor het algemeen overleg over opvang, terugkeer en vreemdelingenbewaring op 19 januari 2016.

57. Agendapunt: **Reactie op verzoek van het lid Van Klaveren, gedaan tijdens de Regeling van werkzaamheden van 15 december 2015, over verhoogde asielinstroom**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 15 januari 2016
Reactie op het verzoek van het lid Van Klaveren, gedaan tijdens de Regeling van Werkzaamheden van 15 december 2015, over verhoogde asielinstroom - 19637-2117

Besluit: Geagendeerd voor het algemeen overleg over opvang, terugkeer en vreemdelingenbewaring op 19 januari 2016.

Volgcommissie(s): BiZa

Brieven overige bewindspersonen

58. Agendapunt: **Bestuursakkoord Verhoogde Asielinstroom**

Zaak: Brief regering - minister van Binnenlandse Zaken en Koninkrijksrelaties, R.H.A. Plasterk - 27 november 2015
Aanbieding Bestuursakkoord Verhoogde Asielinstroom - 19637-2107

Besluit: Geagendeerd voor het algemeen overleg over opvang, terugkeer en vreemdelingenbewaring op 19 januari 2016.

Volgcommissie(s): BiZa

59. Agendapunt: **Verslag van het gesprek met de Onderzoekscommissie Ontnemingsschikking op 7 september 2015**

Zaak: Brief regering - minister-president, M. (Mark) Rutte - 16 december 2015
Verslag van het gesprek met de Onderzoekscommissie Ontnemingsschikking op 7 september 2015 - 34362-6

Besluit: Betrokken bij het debat over het rapport van de Commissie Oosting op 16 december 2015.

Europese aangelegenheden

60. Agendapunt: **Lijst met nieuwe EU-voorstellen op het terrein van V&J over de periode 5 - 25 december 2015 (week 49-51)**

Zaak: Lijst met EU-voorstellen - - 14 januari 2016
Lijst met nieuwe EU-voorstellen op het terrein van V&J over de periode 5 - 25 december 2015 (week 49-51) - 2016Z00565

Besluit: Ter informatie.

Besluit: De minister vragen of hij voornemens is te reageren op de openbare raadpleging 'Contractuele publiek-private partnerschappen voor cyberveiligheid en eventuele begeleidingsmaatregelen' en zo ja, de concept-reactie uiterlijk 30 dagen voor de sluitingsdatum aan de Kamer te zenden.

61. Agendapunt: **EU-voorstel: Mededeling modernisering auteursrecht COM (2015) 626 (Engelstalige versie)**

Zaak: EU-voorstel - Organisatie, Europese Commissie - 10 december 2015
EU-voorstel: Mededeling modernisering auteursrecht COM (2015) 626 (Engelstalige versie) - 2015Z24126

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EZ, OCW

Zaak: Stafnotitie - 14 januari 2016
EU-Stafnotitie behandelvoorstel EU-voorstel portabiliteit online-inhoudsdiensten en mededeling auteursrecht - 2016Z00587

Besluit: Ter informatie.

Besluit: Te ontvangen BNC-fiche agenderen voor algemeen overleg JBZ-raad 10-11 maart 2016.

62. Agendapunt: **EU-voorstel: Verordening grensoverschrijdende portabiliteit van online inhoudsdiensten COM (2015) 627 (Engelstalige versie)**

Zaak: EU-voorstel - Organisatie, Europese Commissie - 17 december 2015
EU-voorstel: Verordening grensoverschrijdende portabiliteit van online inhoudsdiensten COM (2015) 627 (Engelstalige versie) - 2015Z24800

Besluit: Geagendeerd voor het algemeen overleg op 21 januari 2016 over de informele JBZ Raad op 25 en 26 januari 2016.

Volgcommissie(s): EZ, EU

63. Agendapunt: **Stand van zaken JBZ-dossiers Nederlands voorzitterschap**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 17 december 2015
Stand van zaken JBZ-dossiers Nederlands voorzitterschap - 32317-378

Besluit: Geagendeerd voor algemeen overleg informele JBZ-raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU, BuZa

64. Agendapunt: **Voortgang van het besluitvormingsproces rond de EU PNR-richtlijn**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Voortgang van het besluitvormingsproces rond de EU PNR-richtlijn - 32317-375

Besluit: Geagendeerd voor het algemeen overleg op 21 januari 2016 over de informele JBZ Raad op 25 en 26 januari 2016.

Volgcommissie(s): BiZa, EU, I&M

65. Agendapunt: **Afschrift beantwoording vragen van de Eerste Kamer inzake de PNR Richtlijn**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Afschrift beantwoording vragen van de Eerste Kamer inzake de PNR Richtlijn - 32317-376

Besluit: Voor kennisgeving aangenomen.

Volgcommissie(s): BiZa, EU, I&M

66. Agendapunt: **Richtlijn procedurele waarborgen minderjarige verdachten**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 december 2015
Richtlijn procedurele waarborgen minderjarige verdachten - 22112-2036

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): BiZa, EU

67. Agendapunt: **Verslag van de extra Raad Justitie en Binnenlandse Zaken gehouden in Brussel op 3 en 4 december 2015**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 16 december 2015
Verslag van de extra Raad Justitie en Binnenlandse Zaken te Brussel op 3 en 4 december 2015 - 32317-377

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU, BiZa

68. Agendapunt: **Uitstel aanbieding BNC-fiche wijziging vuurwapenrichtlijn**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 18 december 2015
Uitstel aanbieding BNC-fiche wijziging vuurwapenrichtlijn - 22112-2039

Besluit: Voor kennisgeving aangenomen.

Volgcommissie(s): EU

69. Agendapunt: **Fiche inzake Doorgifte van persoonsgegevens uit de EU naar de VS na uitspraak HvJEU (Safe Harbour)**

Zaak: Brief regering - minister van Buitenlandse Zaken, A.G. Koenders - 18 december 2015
Fiche: Doorgifte van persoonsgegevens uit de EU naar de VS na uitspraak HvJEU (Safe Harbour) - 22112-2040
Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.
Volgcommissie(s): EU

70. Agendapunt: **Afschrift van de brief aan de Voorzitter van de Eerste kamer over EU-subsidiefraude en een Europees OM**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 18 december 2015
Aanbieding afschrift van de brief aan de Voorzitter van de Eerste Kamer over EU-subsidiefraude en een Europees OM - 2015Z25103
Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.
Volgcommissie(s): EU

71. Agendapunt: **Uitstel aanbieding Kabinetsappreciatie grenzenpakket**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Uitstel aanbieding Kabinetsappreciatie grenzenpakket - 22112-2047
Besluit: Voor kennisgeving aangenomen.
Volgcommissie(s): EU

72. Agendapunt: **Uitstelbericht aanbieding BNC-fiche modernisering auteursrecht COM (2015) 626**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 7 januari 2016
Uitstelbericht aanbieding BNC-fiche modernisering auteursrecht COM (2015) 626 - 22112-2046
Besluit: Voor kennisgeving aangenomen.
Volgcommissie(s): EU

73. Agendapunt: **Kabinetsappreciatie van de voorstellen van de Europese Commissie van 15 december 2015**

Zaak: Brief regering - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff - 8 januari 2016
Kabinetsappreciatie van de voorstellen van de Europese Commissie van 15 december 2015 - 2016Z00225
Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016 (JBZ-onderwerpen op het terrein van asiel- en vreemdelingenbeleid).
Volgcommissie(s): EU, BuZa, BuHa-OS

74. Agendapunt: **Europees Grensbeheer**

Zaak:	EU-voorstel - Organisatie, Europese Commissie - 18 december 2015 EU-voorstel: Verordening Europese grens- en kustwacht COM (2015) 671 (Engelstalige versie) - 2015Z25080
Besluit:	Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016 (JBZ-onderwerpen op het terrein van asiel- en vreemdelingenbeleid).
Besluit:	Inbrengdatum voor het stellen van vragen t.b.v. een schriftelijk overleg vaststellen op 4 februari 2016 te 14.00 uur.
Besluit:	Er zal een subsidiariteitstoets worden uitgevoerd op de verordening Europese grens- en kustwacht.
Besluit:	Per e-mail zal de deelname worden geïnventariseerd voor een gesprek met de heer Timmermans van de Europese Commissie. Naar aanleiding van deze inventarisatie zal worden bezien of het gesprek wordt georganiseerd.
Volgcommissie(s):	EU
Zaak:	Stafnotitie - 13 januari 2016 Behandelvoorstel EU-prioriteit Grensbeheer - 2016Z00447
Besluit:	Conform voorstel.
Volgcommissie(s):	EU

75. Agendapunt: **Europees Migratiebeheer**

Zaak:	EU-voorstel - Organisatie, Europese Commissie - 18 december 2015 EU-voorstel: Raadsbesluit tijdelijk uitstel verplichtingen Zweden inzake relocatie COM (2015) 677 (Engelstalige versie) - 2015Z25079
Besluit:	Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016 (JBZ-onderwerpen op het terrein van asiel- en vreemdelingenbeleid).
Besluit:	Inbrengdatum voor het stellen van vragen t.b.v. een schriftelijk overleg vaststellen op 4 februari 2016 te 14.00 uur.
Volgcommissie(s):	EU
Zaak:	EU-voorstel - Organisatie, Europese Commissie - 18 december 2015 EU-voorstel: Aanbeveling vrijwillige regeling met Turkije inzake toelating vluchtelingen op humanitaire gronden C (2015) 9490 - 2015Z25072
Besluit:	Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016 (JBZ-onderwerpen op het terrein van asiel- en vreemdelingenbeleid).
Besluit:	Inbrengdatum voor het stellen van vragen t.b.v. een schriftelijk overleg vaststellen op 4 februari 2016 te 14.00 uur.
Besluit:	Per e-mail zal de deelname worden geïnventariseerd voor een gesprek met de heer Timmermans van de Europese Commissie. Naar aanleiding van deze inventarisatie zal worden bezien of het gesprek wordt georganiseerd.
Volgcommissie(s):	EU
Zaak:	Stafnotitie - 13 januari 2016 Behandelvoorstel EU-prioriteit Migratiebeheer - 2016Z00458
Besluit:	Conform voorstel.
Volgcommissie(s):	EU

76. Agendapunt: **Voortgangsrapportage rapporteurschap Slimme Grenzen januari 2016**

Zaak:	Brief van lid/fractie/commissie - Tweede Kamerlid, A.H. Kuiken (PvdA) - 14 januari 2016 Voortgangsrapportage rapporteurschap Slimme Grenzen januari 2016 - 2016Z00510
Besluit:	Voor kennisgeving aangenomen.
Volgcommissie(s):	EU

77. Agendapunt: **Geannoteerde agenda informele JBZ-Raad 25 en 26 januari 2016 in Amsterdam**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 14 januari 2016
Geannoteerde agenda informele JBZ-Raad 25 en 26 januari 2016 in Amsterdam - 32317-380

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

78. Agendapunt: **Nauwere samenwerking inzake IPR huwelijksvermogensrecht en geregistreerd partnerschap**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 15 januari 2016
Nauwere samenwerking inzake IPR huwelijksvermogensrecht en geregistreerd partnerschap - 32317-381

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

79. Agendapunt: **Fiche: Richtlijn terrorismebestrijding**

Zaak: Brief regering - minister van Buitenlandse Zaken, A.G. Koenders - 15 januari 2016
Fiche: Richtlijn terrorismebestrijding - 22112-2053

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

80. Agendapunt: **Fiche: Verordening portabiliteit online content**

Zaak: Brief regering - minister van Buitenlandse Zaken, A.G. Koenders - 15 januari 2016
Fiche: Verordening portabiliteit online content - 22112-2054

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

81. Agendapunt: **Fiche: Mededeling EU Actieplan voor illegale handel in vuurwapens en explosieven**

Zaak: Brief regering - minister van Buitenlandse Zaken, A.G. Koenders - 15 januari 2016
Fiche: Mededeling EU Actieplan voor illegale handel in vuurwapens en explosieven - 22112-2055

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

82. Agendapunt: **Fiche: Richtlijn herziening van de vuurwapenrichtlijn (91/477/EEG)**

Zaak: Brief regering - minister van Buitenlandse Zaken, A.G. Koenders - 15 januari 2016
Fiche: Richtlijn herziening van de vuurwapenrichtlijn (91/477/EEG) - 22112-2056

Besluit: Geagendeerd voor het algemeen overleg over de informele JBZ Raad op 25 en 26 januari 2016 op 21 januari 2016.

Volgcommissie(s): EU

83. Agendapunt: **Uitnodiging voor de welkomstreceptie in het kader van de Informele JBZ Raad op zondagavond 24 januari 2016**

Zaak: Brief regering - minister van Veiligheid en Justitie, G.A. van der Steur - 18 januari 2016
Uitnodiging voor de welkomstreceptie in het kader van de Informele JBZ Raad op zondagavond 24 januari 2016 - 2016Z00752

Besluit: Overlaten aan individuele leden / fracties.

Overig (openbaar)

84. Agendapunt: **Aanbod van het lid Azmani om de commissie te informeren over een aantal bijzondere activiteiten in de planning van de parlementaire dimensie Nederlands EU-Voorzitterschap**

Zaak: Brief van lid/fractie/commissie - voorzitter van de vaste commissie voor Europese Zaken, M. Azmani (VVD) - 21 december 2015
Aanbod van het lid Azmani om de commissies te informeren over een aantal bijzondere activiteiten in de planning van de parlementaire dimensie Nederlands EU-Voorzitterschap - 2015Z25134

Besluit: De commissie gaat in op het aanbod van het lid Azmani de commissie te informeren over een aantal bijzondere activiteiten in het kader van het Nederlands EU-Voorzitterschap. Daartoe zal in een komende procedurevergadering worden ingepland.

Volgcommissie(s): BiZa, BuHa-OS, BuZa, DEF, EZ, EU, FIN, I&M, KR, OCW, SZW, VWS, WR, V&J, IPC Art. 13, IPC Energie, IPC GBVB, IPC Mens

85. Agendapunt: **Werkbezoek aan Griekenland en Macedonië van 25 t/m 29 februari 2016**

Zaak: Brief van lid/fractie/commissie - voorzitter van de vaste commissie voor Europese Zaken, M. Azmani (VVD) - 14 januari 2016
Werkbezoek aan Griekenland en Macedonië van 25 t/m 29 februari 2016 - 2016Z00563

Besluit: De commissie besluit met twee leden deel te nemen aan het werkbezoek van de commissie voor Europese zaken aan Griekenland en Macedonië van 25 tot 29 februari 2016. De reis- en verblijfkosten van de twee deelnemende leden zullen ten laste komen van het reisbudget van de commissie.

Volgcommissie(s): V&J

86. Agendapunt: **Beantwoording vragen commissie over het rapport Onderzoekscommissie Ontnemingsschikking**

Zaak: Brief Kamer - Voorzitter van de Tweede Kamer, A. van Miltenburg (VVD) - 12 december 2015
Beantwoording vragen commissie over het rapport Onderzoekscommissie Ontnemingsschikking - 34362-4

Besluit: Voor kennisgeving aangenomen.

87. Agendapunt: **Verzoek reactie aan de minister van Veiligheid en Justitie op het pleidooi van het CBP voor meer budget**

Zaak: Brief van lid/fractie/commissie - Tweede Kamerlid, J. van Wijngaarden (VVD) - 6 januari 2016
Verzoek reactie aan de minister van Veiligheid en Justitie op het pleidooi van het CBP voor meer budget - 2016Z00073

Besluit: De minister van Veiligheid en Justitie zal worden verzocht de Kamer een reactie te doen toekomen op het artikel "Privacywaakhond CBP kampt met onderbezetting"(NRC, 30 december 2015).

88. Agendapunt: **Verzoek om een reactie van de minister van Veiligheid en Justitie op het rapport over de zorgwekkende ontwikkeling dat er onvoldoende gemeld wordt bij Veilig Thuis als er minderjarigen betrokken zijnhttp://www.politieenwetenschap.nl/cache/files/56915bf15b980VK77.pdf**

Zaak: Brief van lid/fractie/commissie - Tweede Kamerlid, V.A. Bergkamp (D66) - 12 januari 2016
Verzoek om een reactie van de minister van Veiligheid en Justitie op het rapport over de zorgwekkende ontwikkeling dat er onvoldoende gemeld wordt bij Veilig Thuis als er minderjarigen betrokken zijn - 2016Z00388

Besluit: De minister van Veiligheid en Justitie zal worden verzocht de Kamer een reactie te doen toekomen op het TNO-rapport 'Huiselijk geweld gemeld en dan.....? en daarbij tevens aandacht te schenken aan de zorgwekkende ontwikkeling dat er onvoldoende gemeld wordt bij Veilig Thuis als er minderjarigen betrokken zijn.

89. Agendapunt: **Verzoek om spoedig mogelijk de 2de termijn van het algemeen overleg terrorismebestrijding te plannen**

Zaak: Brief van lid/fractie/commissie - Tweede Kamerlid, O.C. Tellegen (VVD) - 14 januari 2016
Verzoek om spoedig mogelijk de 2de termijn van het algemeen overleg terrorismebestrijding te plannen - 2016Z00582

Besluit: Er zal een tweede termijn algemeen overleg terrorisme worden gepland.

90. Agendapunt: **Verzoek van het Presidium aan de vaste commissie voor VWS en voor VenJ om de mogelijkheden te onderzoeken van een algemeen overleg van bijzondere aard waarbinnen moties kunnen worden ingediend**

Zaak: Overig - 17 december 2015 - 2015Z24805
Verzoek van het Presidium aan de vaste commissie voor VWS en voor VenJ om de mogelijkheden te onderzoeken van een algemeen overleg van bijzondere aard waarbinnen moties kunnen worden ingediend

Besluit: Het Presidium van de Tweede Kamer zal worden medegedeeld dat de commissie afziet van deelname aan het proefproject inzake moties in commissieverband (motie Segers c.s.)

Volgcommissie(s): V&J

Rondvraag

91. Agendapunt: **Technische briefing vanuit het ministerie van Veiligheid en Justitie over de gang van zaken rond het ICT-systeem RADAR**

Zaak: Rondvraagpunt procedurevergadering - 21 januari 2016
Technische briefing vanuit het ministerie van Veiligheid en Justitie over de gang van zaken rond het ICT-systeem RADAR - 2016Z01136

Besluit: Er zal per e-mail worden geïnventariseerd wie belangstelling heeft voor een technische briefing/werkbezoek aan het ministerie van Veiligheid en Justitie.

92. Agendapunt: **Kabinetsreactie op het onderzoek "Status vermist. Op zoek naar een oplossing".**

Zaak: Rondvraagpunt procedurevergadering - Tweede Kamerlid, L.M.J.S. Helder (PVV) - 21 januari 2016
Kabinetsreactie op het onderzoek "Status vermist. Op zoek naar een oplossing". - 2016Z01130

Besluit: De minister van Veiligheid en Justitie wordt gerappelleerd inzake gevraagde kabinetsreactie op het onderzoek "Status: vermist. Op zoek naar een oplossing" en hij zal worden verzocht binnen twee weken te reageren.

95. Agendapunt: **Verzoek om rapport "Leven bij Isis, de mythe ontrafeld" van de Algemene Inlichtingen- en Veiligheidsdienst te agenderen voor het algemeen overleg terrorismebestrijding (2e termijn).**

Zaak: Rondvraagpunt procedurevergadering - Tweede Kamerlid, O.C. Tellegen (VVD) - 21 januari 2016
Verzoek om rapport "Leven bij Isis, de mythe ontrafeld" van de Algemene Inlichtingen- en Veiligheidsdienst te agenderen voor het algemeen overleg terrorismebestrijding (2e termijn). - 2016Z01149

Besluit: De commissie besluit het rapport tijdens het algemeen overleg terrorismebestrijding te bespreken.

Brievenlijst

93. Agendapunt: **Brievenlijst (zie de zaken en de besluiten op de brievenlijst)**

Overig (besloten)

94. Agendapunt: **Voorstel opzet rondetafelgesprek over de Contourennota Modernisering Wetboek van Strafvordering (Kamerstuk 29279, nr. 284)**

Zaak: Stafnotitie - 23 december 2015
Voorstel opzet rondetafelgesprek over de Contourennota Modernisering Wetboek van Strafvordering (Kamerstuk 29279, nr. 284) - 2015Z25263

Besluit: De opzet van het rondetafelgesprek wordt vastgesteld.

Griffier: D.S. Nava

Activiteitnummer: 2016A00194

Van: 10.2.e BD/DGPOL/PBT/PT [mailto10.2.e @minvenj.nl]
Verzonden: dinsdag 26 januari 2016 14:01
Aan: 10.2.e
CC:10.2.e 10.2.e
Onderwerp: portfolio cc III
Hoi 10.2.e in de rapportage van het portfolio staat dit:

127 - 2014	2	Wet Computer Criminaliteit III (CCIII)	Zorko	loopt	2017

Wat mij opvalt zijn twee dingen: ‘vanwege eerdere onduidelijkheid wettelijk kader..”: volgens mij was dat niet de reden van IV organisatie om IV activiteiten te beperken. Maar goed, dat nog terzijde. Vindt nadere afstemming plaats over extra IV-activiteiten: afstemming met wie? En waar wordt op gedoeld? Dan staat er evt extra capaciteit kan in besluitvorming over bijstelling portfolio 2016 worden meegenomen: Kun je aangeven welke behoefte er bestaat en nodig is, zodat ik dat voor de bijstelling kan rapporteren?

Alvast dank!

Met vriendelijke groet,

10.2.e
9
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken
Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag
.....

Van: 10.2.e
Verzonden: dinsdag 26 januari 2016 14:36
Aan: 10.2.e - BD/DGPOL/PBT/PT'
CC: 10.2.e 10.2.e 10.2.e
Onderwerp: RE: portfolio cc III
Beste 10.2.e

in overleg met 10.2.e leggen wij deze vragen voor aan onze opdrachtgever in de operationele lijn.
Nader bericht hierover volgt nog.

Met vriendelijke groet,

10.2.e en 10.2

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 27 januari 2016

Nationale Politie
Aan mevrouw I. Philips
10.2.e @knp.politie.nl

Vaste commissie voor Veiligheid en Justitie
Postbus 20018
2500 EA Den Haag

T 9 / 9
E 10.2.e weedekamer.nl

Geachte mevrouw 10.2.e

De vaste commissie voor Veiligheid en Justitie organiseert een rondetafelgesprek over het wetsvoorstel computercriminaliteit III (Kamerstuk 34372). Het rondetafelgesprek zal plaatsvinden op donderdag 11 februari 2016 van 10.00 tot 13.00 uur en is opgedeeld in drie blokken.

Namens de commissie nodig ik u uit aan dit gesprek deel te nemen in het tweede blok dat duurt van 10.40 tot 11.50 uur. De minister van Veiligheid en Justitie is verzocht toestemming te verlenen voor uw deelname aan het rondetafelgesprek. Graag verneem ik uiterlijk donderdag 4 februari 2016 of u aan het rondetafelgesprek zult deelnemen. Gelet op de beperkte ruimte aan tafel en de beperkte spreektijd is er plaats voor één gespreksdeelnemer per organisatie. Uiteraard is de publieke tribune beschikbaar voor geïnteresseerden die het verloop van het gesprek willen volgen.

Om de beschikbare tijd tijdens het gesprek zo efficiënt mogelijk te kunnen gebruiken, stelt de commissie het op prijs als u voorafgaand aan het rondetafelgesprek een gespreksnotitie (uw standpunt in 1 à 2 A4'tjes) instuurt. Graag zie ik deze notitie uiterlijk donderdag 4 februari 2016 tegemoet, bij voorkeur per e-mail 9 @tweedekamer.nl). Graag maak ik u erop attent dat de gespreksnotitie via de website van de Tweede Kamer openbaar zal worden. Ik ga ervan uit dat u daartegen geen bezwaar heeft. Mocht dat wel het geval zijn dan verneem ik dat zo spoedig mogelijk van u.
Openbaarmaking geldt daarmee ook voor contactgegevens die standaard op briefpapier staan. Indien u hiertegen bezwaar heeft, wordt u verzocht de contactgegevens te verwijderen alvorens de gespreksnotitie in te sturen.

Het rondetafelgesprek, dat een openbaar karakter heeft, vindt plaats in het gebouw van de Tweede Kamer. U kunt zich vooraf melden bij de beveiliging aan de ingang op adres Plein 2. In verband met de veiligheidsmaatregelen verzoek ik u tijdig aanwezig te zijn en een geldig legitimatiebewijs mee te nemen. Mocht u nog vragen hebben over de gang van zaken met betrekking tot dit rondetafelgesprek, dan kunt u zich wenden tot het commissiesecretariaat.

Namens de commissie dank ik u bij voorbaat voor uw inzet.

Hoogachtend,
10.2.e
9 Veiligheid en Justitie

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 15:44
Aan: 10.2.e
CC: 10.2.e
Onderwerp: datum hoorzitting CIII - 11 februari 10.00-13.00 uur
Bijlagen: Convocatie_rondetafelgesprek_over_Computercriminaliteit_III_op_11_februari_2016[1].pdf

Inmiddels bekend

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 27 januari 2016

Voortouwcommissie:	**vaste commissie voor Veiligheid en Justitie**
Activiteit:	**Rondetafelgesprek**
Datum:	donderdag 11 februari 2016
Tijd:	10.00 - 13.00 uur
Openbaar/besloten:	openbaar
Onderwerp:	Computercriminaliteit III

Agendapunt:	**Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)**
Zaak:	Wetgeving - staatssecretaris van Veiligheid en Justitie, K.H.D.M. Dijkhoff – 21 december 2015 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) - 34372

Het schema volgt zo spoedig mogelijk.

Griffier:	10.2.e
Activiteitnummer:	2016A00399

From: 10.2.e
Sent: Wednesday, January 27, 2016 04:23 PM W. Europe Standard Time
To: 10.2.e @minvenj.nl>
Cc: 10.2.e ; 10.2.e
Subject: FW: Ronde tafel computercriminaliteit III

Beste collega's,

In verband met ziekte is dit verzoek blijven hangen. Bij deze, alsnog, de namen van de collega's die worden voorgedragen voor de hoorzitting op 11 februari (datum inmiddels bekend):
- Inge Philips, plv. Diensthoofd Nationale Recherche, Landelijke Eenheid
- Theo van der Plas, plv. Eenheidschef Landelijke Eenheid, Directeur Operatie

Wordt dit via jullie aan de griffie van de Tweede Kamer doorgegeven na akkoord? Alvast dank voor de reactie.
Hartelijke groet,

10.2.e

Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

Van: 10.2.e @politie.nl]
Verzonden: woensdag 27 januari 2016 16:24
Aan: 10.2.e
CC: Bestuursondersteuning; 10.2.e
Onderwerp: FW: Ronde tafel computercriminaliteit III

Beste collega's,

In verband met ziekte is dit verzoek blijven hangen. Bij deze, alsnog, de namen van de collega's die worden voorgedragen voor de hoorzitting op 11 februari (datum inmiddels bekend):
- 10.2.e plv. Diensthoofd Nationale Recherche, Landelijke Eenheid
- Theo van der Plas, plv. Eenheidschef Landelijke Eenheid, Directeur Operatie

Wordt dit via jullie aan de griffie van de Tweede Kamer doorgegeven na akkoord? Alvast dank voor de reactie.

Hartelijke groet,

10.2.e
Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 16:30
Aan: 10.2.e @politie.nl>
Onderwerp: Re: Ronde tafel computercriminaliteit III

Hoi 10.2.

Kun je svp nog een check doen wanneer de position paper af moet zijn? We zouden vooraf ook nog een werkbezoek proberen te regelen. Zal bij DGPol checken of dat nog realistisch is.

Met vriendelijke groet,

10.2.e

Staf Korpsleiding Politie
Directie Operatien

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 16:41
Aan: 10.2.e
CC: 10.2.e
Onderwerp: RE: Ronde tafel computercriminaliteit III

Net de griffie aan de lijn gehad. 4 februari moeten we het inleveren. We zitten bij blok 2, van 10.40 uur tot 11.50 uur. Andere sprekers mogen ze pas vertellen als ze bevestigd zijn. Ze willen maar één afgevaardigde. Uitnodiging richting Inge Philips/Theo van der Plas sturen ze via onze mailbox bestuursondersteuning. Ik zet het dan door richting beiden, als je het goed vindt. Dan mogen ze zelf beslissen wie van de twee gaat. Voor de voorbereiding, kijken wij uiteraard graag mee.

Werkbezoek wordt lastig als het via de commissie moet gaan, volgens mijn ervaring in de Kamer. Het makkelijkste is één op één richting de Kamerleden te doen, dan wel op een vrijdagochtend of een maandagmiddag, want ze zijn dan vrij van Kamerdebatten.

Groet,

10.2.

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 17:14
Aan: 10.2.e 10.2.e 10.2.e ; 10.2.e
CC: Plas, Theo van der (T.G.)
Onderwerp: FW: datum hoorzitting CIII - 11 februari 10.00-13.00 uur

Beste collega's,

De ronde tafel CCIII is gepland voor **11 februari 10.00-13.00 uur.**
Afgesproken is dat in principe Inge Philips en Theo vd. Plas deze ronde tafel doen. Willen jullie dit in de agenda's noteren? Mocht dit een probleem zijn dan hoor ik het graag zsm.

Verder moet de voorbereiding snel worden gestart.

Ter voorbereiding is het gebruikelijk dat we:
- een 'position paper' opleveren met ons standpunt (1 a 2 A4tjes) net als de andere partijen. Dit stuk is openbaar en wordt ook aan de Kamerleden gezonden
- een korte mondelinge toelichting voorbereiden die we aan het begin van de hoorzitting kunnen geven (tijd is afhankelijk van de voorzitter, maar meestal 2-5 minuten)
- Q&A's voor onszelf maken als dat helpt in de voorbereiding (maar volgens mij waren jullie daar al mee bezig?)

Ik wacht nog op nadere informatie, oa. wanneer die position paper aangeleverd moet worden.

Ik ga ervan uit dat we in dezelfde groep zitten als het OM. Ik zal even een check doen bij PaG en LP wie dit bij OM voorbereidt, zodat we in de voorbereiding kunnen afstemmen. Zodra bekend is welke rondes er zijn en wie er nog meer in onze groep zitten laat ik het weten.

Ik ga ervan uit dat jullie zelf vooral de inhoudelijk voorbereiding doen en ik met onze BZ meelees en help met de verdere afstemming en voorbereiding.
Om dat soepel te laten verlopen denk ik dat het handig is als wij 1 aanspreekpunt hebben voor de voorbereiding. Laat svp weten wie dit oppakt.

Ik heb nog afstemming gehad met DGPol over het werkbezoek van de vaste kamercommissie. Dat lijkt niet meer realistisch voor de ronde tafel. Advies DGPol iam. DGRR is dit na de ronde tafel te doen. De ronde tafel kan dan mogelijk gebruikt worden om de commissie uit te nodigen voor dat werkbezoek. Voordeel van een werkbezoek na de ronde tafel dat ik zelf nog zie is dat we dan nog kunnen teruggekomen op standpunten ingebracht door andere partijen, om die te nuanceren.

Met vriendelijke groet,

10.2.e

10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën | 9
Nieuwe Uitleg 1, 2514 BP, Den Haag
M 10.2.e

Van: 10.2.e j@tweedekamer.nl]
Verzonden: woensdag 27 januari 2016 17:18
Aan: 10.2.e @knp.politie.nl>
CC: 10.2.e @politie.nl>
Onderwerp: Uitnodiging voor het rondetafelgesprek over computercriminaliteit III op donderdag 11 februari van
10.00 tot 13.00 uur
Urgentie: Hoog

Geachte mevrouw Philips,

De vaste commissie voor Veiligheid en Justitie wil u graag uitnodigen voor het rondetafelgesprek over computercriminaliteit III (Kamerstuk 34 372) op donderdag 11 februari van 10.00 tot 13.00 uur.

De uitnodiging hiervoor treft u in de bijlage bij deze e-mail aan.
Zou u uw aanwezigheid bij dit rondetafelgesprek kunnen bevestigen?

Met vriendelijke groet,

10.2.e

9 commissie voor V&J
9 commissies Bestuur en Onderwijs
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 17:23
Aan: 10.2.e @politie.nl>
Onderwerp: RE: Ronde tafel computercriminaliteit III

Hoi,

Dank, maar ik denk dat het wel handig is even te weten wat onze lijn is als we maar 1 persoon sturen?
Inhoudsdeskundige of minimaal niveau eenheidsleiding? Heeft KL/BZ daar een lijn is?
Of mogen ze dat inderdada zelf beslissen?

Werkbezoek zal er nu wel na worden denk ik gezien de korte termijn….

Groet,

10.2.

From: 10.2.e
Sent: Wednesday, January 27, 2016 05:30 PM W. Europe Standard Time
To: 10.2.e
Subject: RE: Ronde tafel computercriminaliteit III

Mijn insteek (en ook de behoefte van 9) is om een deskundige te sturen, met wat politieke gevoeligheid, aangezien de vragen die Kamerleden stellen. De uitnodiging van 9 is nu binnen en is gericht op Inge Philips (zie bijlage). Ik ken de afwegingen van Woordvoering toen bij het interview bij de VK niet, maar als ze toen voor haar hebben gekozen, kunnen we consequent haar nog een keer als eerste vragen. Ik ken Theo en Inge echter niet, dus misschien kun je aangeven wie van beiden geschikter is. Het niveau lijkt ons hoog genoeg in beide gevallen. Met de juiste voorbereiding van Woordvoering en Bestuurszaken moet het goed komen.

From: 10.2.e
Sent: Wednesday, January 27, 2016 05:41 PM W. Europe Standard Time
To: 10.2.e 10.2.e Philips, Inge (I.C.); 10.2.e 10.2.e
Cc: Plas, Theo van der (T.G.)
Subject: Nadere informatie hoorzitting

Collega's,

We ontvingen net bijgaande uitnodiging met oa. het bericht dat:
- we in de tweede ronde aan de beurt zijn: 10.40-11.50 (maar het is natuurlijk verstandig er bij het begin al te zijn om de voorgaande genodigden te horen)
- er vanwege de beperkte ruimte nu maar 1 persoon afgevaardigd kan worden (vooralsnog is de uitnodiging aan 10.2.e gedaan, maar dit kan nog gewijzigd worden indien gewenst)
- we 4 februari onze position paper/gespreksnotitie moeten aanleveren.

Groet,

10.2.

10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën | 9
Nieuwe Uitleg 1, 2514 BP, Den Haag

Van: Philips, Inge (I.C.)
Verzonden: woensdag 27 januari 2016 18:28
Aan: 10.2.e 10.2.e 10.2.e ; 10.2.e
CC: Plas, Theo van der (T.G.)
Onderwerp: Re: Nadere informatie hoorzitting

Prima, genoteerd.

Groet,

Inge Philips

Plv Diensthoofd
Politie - Landelijke Recherche

Van: 10.2.e
Verzonden: woensdag 27 januari 2016 19:58
Aan: 10.2.e @politie.nl>
Onderwerp: RE: Ronde tafel computercriminaliteit III

Ok,dank, heb het doorgegeven en ga dan eerst maar uit van Inge.

Van: 10.2.e
Verzonden: donderdag 28 januari 2016 09:01
Aan: 10.2.e
Onderwerp: RE: Ronde tafel computercriminaliteit III

Hoi,

Vraagje en dubbel check. Aan wie heb je wat doorgegeven? Mag ik dan wel de uitnodiging doorzetten richting Inge?

Ik zet jou en 9 dan in de Cc. Wil je Theo van der Plas in de Cc of verder nog iemand die hiervan moet weten? Alvast dank voor je reactie.

Gr.,

10.2.

From: 10.2.e
Sent: Thursday, January 28, 2016 09:38 AM W. Europe Standard Time
To: Philips, Inge (I.C.); 10.2.e 10.2.e 10.2.e
Cc: Plas, Theo van der (T.G.)
Subject: RE: Nadere informatie hoorzitting

Goedemorgen allemaal,

we zullen vanuit het project voor 4 februari onze position paper aanleveren. Bij wie moet dit aangeleverd worden?

Groet,

10.2.e

From "Plas, Theo van der (T.G.)" 10.2.e @politie.nl>
Subject **RE: Nadere informatie hoorzitting**
To 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>
Date 28 januari 2016 10:37:01 CET

Hallo 10.2.e ik stel in elk geval voor dat ik met Inge bespreek wat de inhoud zal zijn. Kijk svp of we breder (het belang van) onze digitalisering en Cyber kunnen laten meelopen in het thema. Hoor graag nog even het voorstel. Inge, wij even overleggen? Vanavond of morgen ergens?
Groeten,Theo

drs. T.G. (Theo) van der Plas EMPM

Van: 10.2.e @minvenj.nl]
Verzonden: donderdag 28 januari 2016 12:12
Aan: 10.2.e @politie.nl>
CC: 10.2.e @knp.politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Ronde tafel computercriminaliteit III

Hoi 10.2.

Oké, dat is prima.

Dankjewel voor het doorgeven van de namen.
Ja, we geven het inderdaad door en dan wordt het aan 9 doorgegeven.

Met vriendelijke groet,

10.2.e
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
DGPOL
Turfmarkt 147 | 2511 DP | Den Haag | 24ste etage
Postbus 20301 | 2500 EH | Den Haag
.....

Van: 10.2.e)
Verzonden: donderdag 28 januari 2016 12:50
Aan: 10.2.e @minvenj.nl>
CC: 10.2.e @knp.politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Ronde tafel computercriminaliteit III

Inmiddels is de uitnodiging op naam van Inge Philips binnengekomen.

Van: 10.2.e @minvenj.nl>
Verzonden: donderdag 28 januari 2016 14:18
Aan: 10.2.e
Onderwerp: Jurisdiction conference registration information
Bijlagen: 28012016Draft programmeJurisdictioninCyberspace.pdf; Topics for discussion.pdf

Dear Sir/Madam,

We appreciate your interest in attending the expert meeting "Crossing Borders: Jurisdiction in cyberspace", which will take place 7-8 March 2016 in Amsterdam, the Netherlands. In this email you will find some practical information about the (mandatory) official registration process, hotel reservations and travel arrangements. Please read this information carefully to ensure your participation to the expert meeting is properly arranged. Attached you will also find a draft programme and short introduction into the purpose and content of the workshops.

Official registration
Registration via the official registration procedure is mandatory in order to gain access to the Europe Building. We will send an email containing a link for official registration to the email address you received this message on. We advise to register early. Registration requires uploading a copy of your ID and a passport photo and is followed by an accreditation process that may take up to three weeks. Registration is possible until **19 February 2016** at the latest.

The link to register for the conference will be sent to you from the e-mail address EU2016 – Support Desk (10.2.e @minbuza.nl). We understand that some participants have found the message about the registration portal in their spam-folder. If you have received the invitation, but do not receive the link to the registration portal within 3 days from now, please check your spam-folder. If it is not there either, please let us know so we can make sure it is sent again.

If you have questions about the registration portal, please contact the Registration Support Desk at the Ministry of Foreign Affairs: T: +31 10.2.e , E: 10.2.e @minbuza.nl.

Call for papers
During the conference three situations that remain especially challenging for combatting cybercrime will be discussed in three different workshops:

A 7-12

B
C

We invite the submission of papers on each of these three topics.

Various participants have already confirmed they will contribute to the discussion by submitting a paper. In case you are also willing to bring forward your views in advance, or otherwise would like to suggest to us which documents should be taken into account when formulating the basis for discussion during the conference, please feel free to contact us via 10.2.e @minvenj.nl.

Practical arrangements
Please be aware that Member States are expected to provide for travel and hotel costs of their respective delegations. Please make your own travel arrangements. Preferred hotel accommodation can be booked through this link. We advise to use the recommended hotel accommodation. It is easy to reach from the airport and the conference location and we will have our informal welcome reception there. As hotel accommodation is limited, we advise you to make a reservation as soon as possible.

If you have any questions please contact us via the conference email address 10.2.e @minvenj.nl).

We look forward to welcoming you to Amsterdam!
Kind regards,

10.2.e , 10.2.e , 10.2.e

Jurisdiction conference team
.....
Ministry of Security and Justice, The Netherlands
Turfmarkt 147 | The Hague
.....
10.2.e @minvenj.nl
http://english.eu2016.nl/
.....

Crossing Borders: Jurisdiction in cyberspace

Draft programme

6 March

20.00 – 21.30 Informal reception with drinks

7 March

PART I – Introduction (plenary session)

9.00 Registration and Welcome Coffee

9.30 Opening words of the Chair 10.2.e , *Senior Judge, Court of Appeal The Hague)*

9:40 Opening words of the European Commission (10.2.e , *Director, Directorate Internal Security, DG HOME, European Commission)*

9:50 E-evidence and access to data in the cloud 9 , *Council of Europe)*

10:20 Cybercrime Convention Article 32b (10.2.e , *Ministry of Justice, Romania)*

10:50 Questions from the audience

11:00 Coffee-break

11.30 Jurisdiction and principles of international law 10.2.e , *Bond University)*

12.00 Questions from the audience

12:15 Introduction Situation A: 7-12 10.2.e , *Eurojust)*

12.30 Introduction Situation B: 7-12 10.2.e , *Public Prosecutor Portugal)*

12:45 Introduction Situation C: 7-12 10.2.e , *Europol)*

13.00 Lunch

2016

Part II – Proposals for overcoming the obstacles to effective enforcement (parallel break-out sessions)

14:15 Workshops

Group A - 7-12

Group B – 7-12

Group C – 7-12

16.30 Coffee-break

17:00 Sharing the outcomes of each group (*workshop chairs*)

17.45 Closing remarks

18:00 Dinner
Dinner is served on board the Prins van Oranje luxury cruise ship. The ship will depart from the conference venue and will arrive at approx. 20.30 hrs at the recommended hotel in Zaandam.

8 March

Part III – The way forward (plenary session)

9.00 Welcome Coffee

9.30 Opening 9 , *Netherlands Ministry of Security and Justice*)

9.45 How to rob a bank in the digital age (10.2.e)

10.15 Presentation Group A and panel discussion

11:00 Coffee-break

11:15 Presentation Group B and panel discussion

12:15 Presentation Group C and panel discussion

13:15 Chair conclusions, future process and closing

13:30 Closing Lunch

Panel discussion leader:
10.2.e (*Queen Mary University of London*)

Panel members:

- 10.2.e *(Eurojust),*
- 10.2.e (*DG HOME, European Commission*),
- 10.2.e (*Bond University*),
- 10.2.e (*Facebook*),
- 10.2.e (*Microsoft*),
- 10.2.e *(Google)*

6 – 8 March, Amsterdam

Topics for discussion

Crossing Borders: Jurisdiction in cyberspace

Due to the digitalization of society, the protection of cyberspace from incidents, malicious activities and misuse has become crucial for the functioning of our societies and economies. The borderless nature of cyberspace poses special challenges and opportunities for law enforcement and judicial authorities.

The EU has recognized the challenge investigations in cyberspace pose and has acted accordingly. Unfortunately, some challenges remain unaddressed. For instance, 7-12

At the informal Ministerial JHA meeting of the 26th of January 2016 ministers supported the development of concrete elements for an EU common approach. On the basis of the conference outcomes possible courses of action will be developed and discussed in the appropriate council working groups and the formal JHA Council in June this year.

The expert conference serves to generate creative ideas for the development of such an EU common approach. The outcome of the conference will be discussed in the CATS meeting in May and the JHA Council in June 2016.

To structure the discussion, the conference is constructed around three workshops, each dealing with parts of the remaining challenges identified.

7-12

NL EU 2016

0085

2016

Van: 10.2.e namens Bestuursondersteuning
Verzonden: vrijdag 29 januari 2016 08:45
Aan: 10.2.e
CC: 10.2.e ; Bestuursondersteuning
Onderwerp: FW: Uitnodiging voor het rondetafelgesprek over computercriminaliteit III op donderdag 11 februari van 10.00 tot 13.00 uur
Bijlagen: Uitnodiging mevr. I. Philips.doc

Urgentie: Hoog

Hoi 10.2.e ,

Ter info, Inge Philips is uitgenodigd voor de hoorzitting computercriminaliteit III.10.2.e heeft de uitnodiging naar Inge doorgezet en haar erop attent gemaakt op de mogelijkheid om een gespreksnotitie vooraf te sturen (deze wordt wel openbaar).10.2.e gaat nog na wie van het OM en andere sectoren gaat, zodat het niveau een beetje vergelijkbaar blijft. De Kamer heeft echter liever experts aan het woord. De kennis heeft zij al en zij heeft eerder de pers te woord gestaan. Met aanvullende steun van Woordvoering en Bestuurszaken moet het goed komen. Eerste stap is meekijken met de gespreksnotitie, als deze zo ver is. Bevestiging van deelname en versturen van de notitie dient uiterlijk 4 februari te gebeuren.

Groet,
10.2.e

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 27 januari 2016

Dubbel - zie pag. 0061

Van: 10.2.e
Verzonden: vrijdag 29 januari 2016 14:13
Aan: 10.2.e Philips, Inge (I.C.); 10.2.e 10.2.e
CC: Plas, Theo van der (T.G.)
Onderwerp: RE: Nadere informatie hoorzitting

Hallo 10.2.e

Je mag hem naar mij sturen, dan zorg ik dat er vanuit de staf wordt meelezen door 9 en door BZ en mij meer politiek bestuurlijk. Het zou daarom handig zijn als jullie zo snel mogelijk een eerste conceptversie aanleveren, zodat we voldoende tijd hebben, ook voor akkoord PFH/KL.

Groet,

10.2.e

Van: 10.2.e
Verzonden: vrijdag 29 januari 2016 14:38
Aan: 10.2.e Philips, Inge (I.C.); 10.2.e 10.2.e
CC: Plas, Theo van der (T.G.)
Onderwerp: RE: Nadere informatie hoorzitting

Hoi 10.2.e,

ik ben druk bezig. Ik heb een allereerste ruwe versie vanochtend naar Inge en 10.2. gestuurd om commentaar op te leveren. Na verwerking van hun opmerkingen hoop ik vandaag, uiterlijk maandag vroeg in de middag een versie naar iedereen toe te sturen voor verdere becommentariëring.

Weet jij of Inge haar komst heeft bevestigd?

Groet,

10.2.e

-----Original Message-----
From: 10.2.e
Sent: Monday, February 01, 2016 01:51 PM W. Europe Standard Time
To: Plas, Theo van der (T.G.); Philips, Inge (I.C.); ;

Cc: 10.2.e
Subject: Gespreksnotitie CIE VenJ concept 0.2

Beste collega,

bijgaand treffen jullie aan een eerste opzet voor de gespreksnotitie als input voor het rondetafelgesprek op 11 februari.

k hoor graag of de gevolgde lijn in deze opzet een goede is en hoor graag jullie op- en aanmerkingen.

Ik heb deze mail bewust alleen naar jullie gestuurd, maar mocht ik iemand vergeten zijn, dan hoor ik dat graag.

Met vriendelijke groet,

10.2.e

From: 10.2.e
Sent: Monday, February 01, 2016 03:24 PM W. Europe Standard Time
To: Plas, Theo van der (T.G.); Philips, Inge (I.C.); 10.2.e 10.2.e 10.2.e
Cc: 10.2.e
Subject: RE: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.3)

Beste allemaa,

bijgaand een versie 0.3.

Groet,

10.2.e

Van: 10.2.e
Verzonden: dinsdag 2 februari 2016 08:02
Aan: 10.2.e @politie.nl>
Onderwerp: FW: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.3)

Lees je ook mee?

Van: 10.2.e
Verzonden: dinsdag 2 februari 2016 15:29
Aan: 10.2.e
CC: 10.2.e Bestuursondersteuning; 10.2.e
Onderwerp: FW: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.3)
Bijlagen: Gespreksnotitie CIE VenJ concept 0.3.doc; Opmerkingen_gespreksnotitie.docx; beantwoording vragen nav interview.docx

Hoi 10.2.e

Dank je wel voor het doorsturen! Heel fijn dat jij Bestuursondersteuning hierbij aangesloten houdt. Ik heb zelf ook 10.2.e (juridische zaken) in de Cc genomen, omdat hij eerder betrokken was bij de formele reactie op het wetsvoorstel.

De notitie ziet er goed uit. Ik heb een paar suggesties en opmerkingen in het document 'opmerkingen gespreksnotitie' meegenomen, want ik kon ze in het oorspronkelijke document niet zichtbaar maken. Wil jij deze namens mij aan de collega's doorgeven of zal ik het zelf doen? Ik weet niet wat jij met Theo, Inge, 10.2.e, 10.2.e en 10.2.e hebt afgesproken, daarom mail ik jou maar eerst.

De bevestiging en de notitie dienen uiterlijk 4 februari bij de griffie te zijn. Ik kan hiervoor zorgen, als jullie dan zo ver zijn. Is dit haalbaar?
Wordt verder nog een mogelijke Q&A voorbereid? De vragen die zijn voorbereid tbv het AO Politie stuur ik ook hierbij.
Ze kunnen misschien tijdens de hoorzitting aan bod komen.

Alvast dank voor je reactie!

Groet,

10.2.e

Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I 9
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag
M 06 10.2.e I 10.2.e @politie.nl
Werkdagen: maandag t/m vrijdagochtend

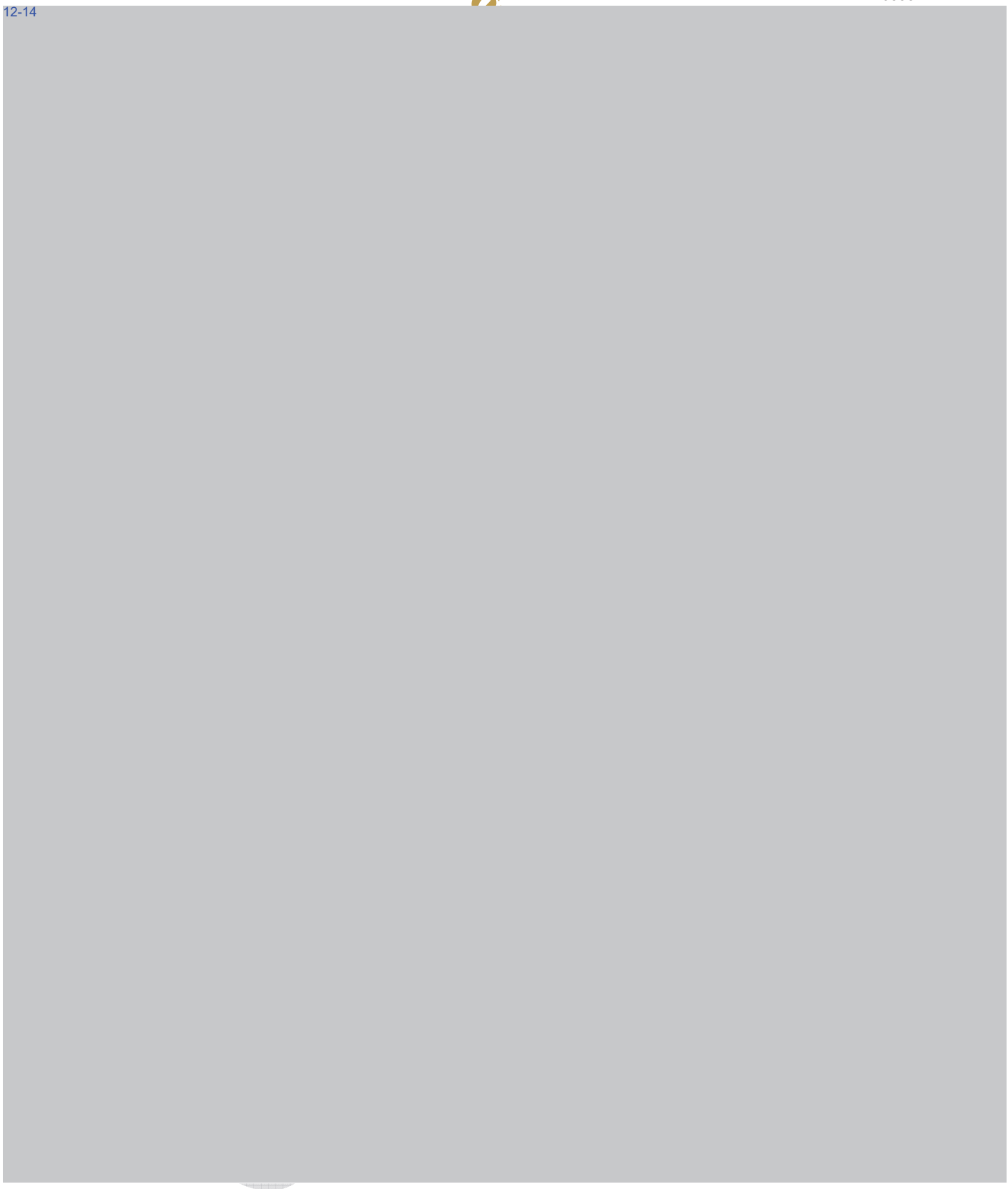
Organisatieonderdeel Eenheid/PDC
District/Dienst
Afdeling

POLITIE

12-14

[redacted]

12-14



12-14

12-14

Beste collega's van Bestuursondersteuning (cc. 10.2.e en 10.2.e),

I.v.m. het AO Politie is het verzoek onderstaande vragen n.a.v. het Volkskrant-artikel 'Politie krijgt hackbevoegheden, maar kan ze niet gebruiken' d.d. 2 januari 2016 z.s.m. te beantwoorden:

- De Volkskrant citeert in het artikel Inge Philips: 'Maar er moet wel een budget zijn. We kunnen deze agenten niet zonder fatsoenlijke spullen aan het werk zetten. Dan gaan ze gehandicapt van start.' **Welke 'spullen', met name op het gebied van ICT, worden bedoeld? En wanneer moeten deze 'spullen' gereed zijn?**

In het interview is in algemene zin gedoeld op het belang van goede voorzieningen voor digitaal rechercheren door de politie. De snelle digitalisering van de maatschappij maakt het noodzakelijk dat de politie deze ontwikkelingen bijhoudt om criminaliteit effectief te kunnen bestrijden. Daarvoor zijn investeringen nodig, onder andere in specifieke ICT middelen voor digitaal rechercheurs.

- De concept IV-portfolio 2016 omvat een project Wet computercriminaliteit III. **Voorziet dit project niet in de realisatie van de 'spullen'? Zo nee, waarom niet? Is de menscapaciteit of het geld de beperkende factor?**

In het project CCIII van politie ter implementatie van de wet is aandacht voor alle aspecten die van belang zijn om de nieuwe bevoegdheden van de politie uit te kunnen oefenen bij in werking treding van de wet, waaronder ook ICT voorzieningen.
In brede zin zijn de middelen, waaronder (extra inhuur van) capaciteit, van de IV organisatie voor het uitvoeren van operationele ICT vernieuwingen binnen de politie op dit moment beperkt. Dit is van invloed op de verdere ontwikkeling van middelen voor digitaal rechercheren. Bij de in werking treding van CCIII is de politie echter wel in staat de bijbehorende bevoegdheden uit te voeren.

- Er bestaat een project 'In werking brengen digitaal opsporen'. **Maakt dit project geen deel uit van de IV-portfolio 2016? Zo nee, waarom niet?**

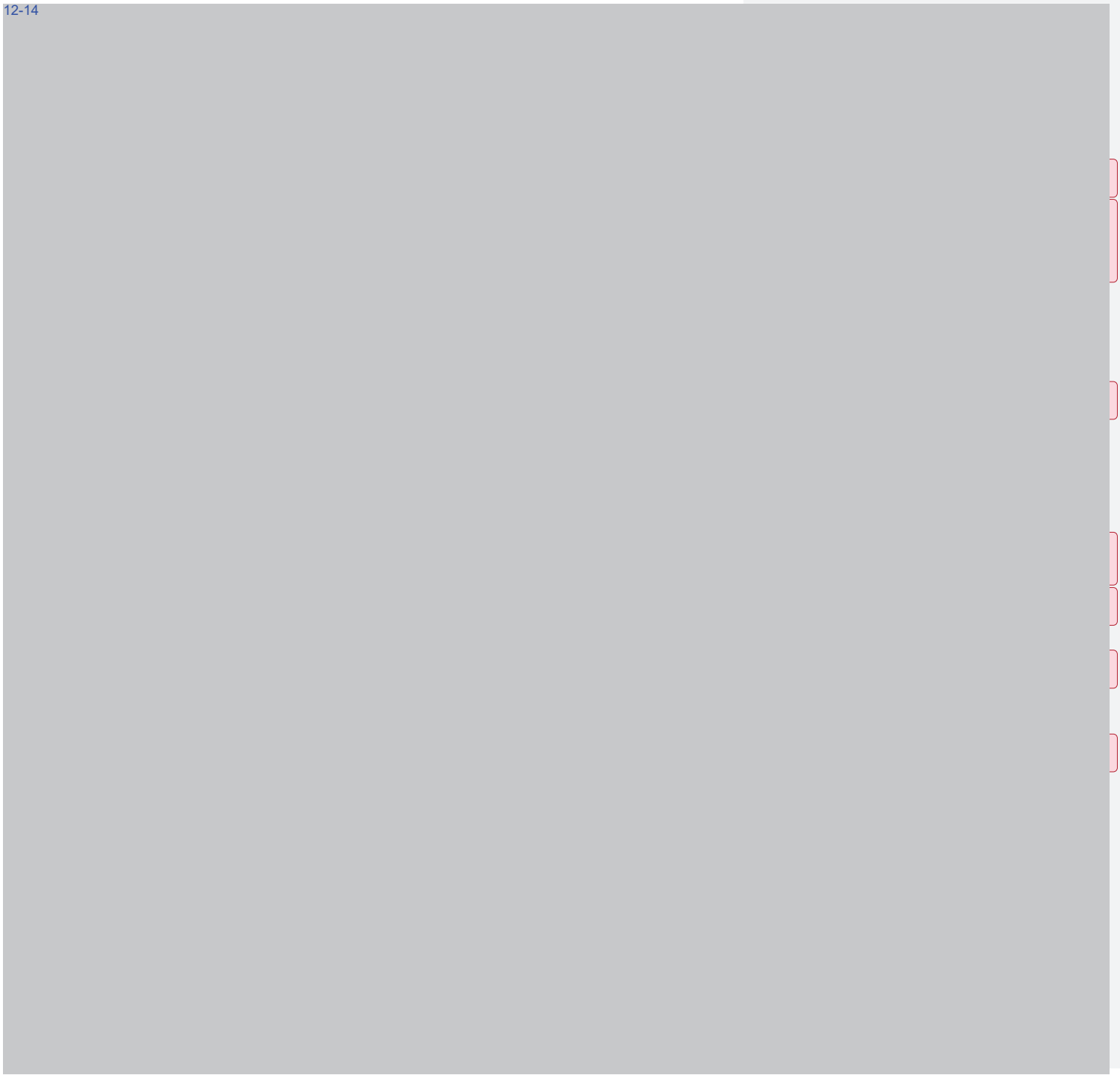
en

- De realisatie van de 'spullen' neemt meerdere jaren in beslag. **Voorziet de meerjarige IV-portfolio 2016-2020 hierin?**

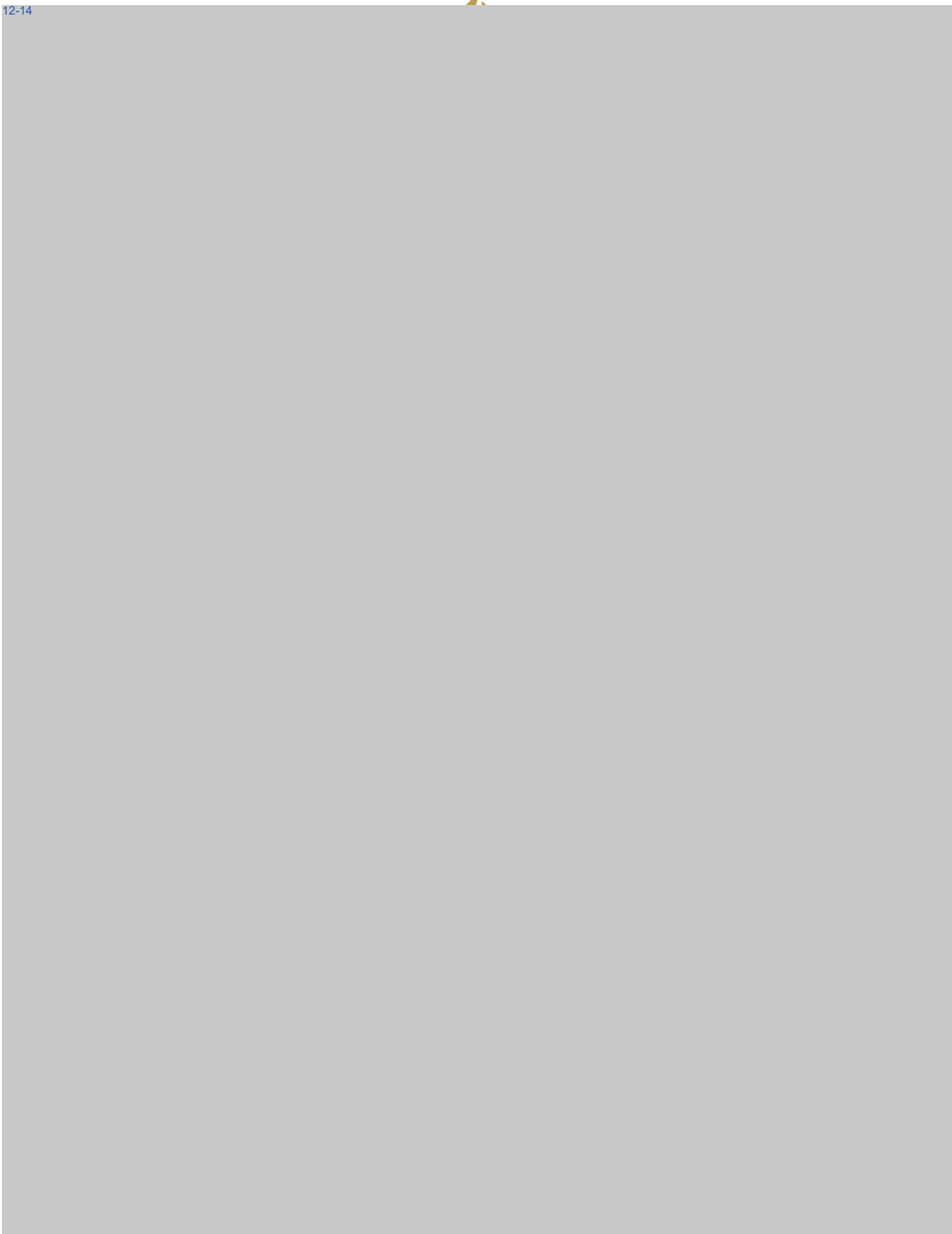
Het project ' in werking brengen digitaal opsporen' is een project dat zich bezig houdt met het in werking brengen van digitaal opsporen op het gebied van organisatie, mensen en middelen. ICT middelen die in het kader van dit project geïmplementeerd moeten worden, worden zodra deze zijn uitgewerkt opgenomen in het portfolio proces. In dit proces wordt, rekening houdend met de bestaande kaders, het portfolio vastgesteld. In het portfolio van 2016 zijn op dit moment enkele specifieke middelen opgenomen.
Het meerjaren IV-portfolio houdt rekening met de ontwikkeling van nieuwe IV voorzieningen op het gebied van digitale opsporing. Echter het financieel kader biedt op dit moment weinig ruimte om hier daadwerkelijk invulling aan te geven.

- **Als het geld de beperkende factor is, kan de bijzondere bijdrage van € 13,8 miljoen daarvoor niet worden ingezet?**

De bijzondere bijdrage van 13,8 mln. betreft een bijzondere bijdrage voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie.

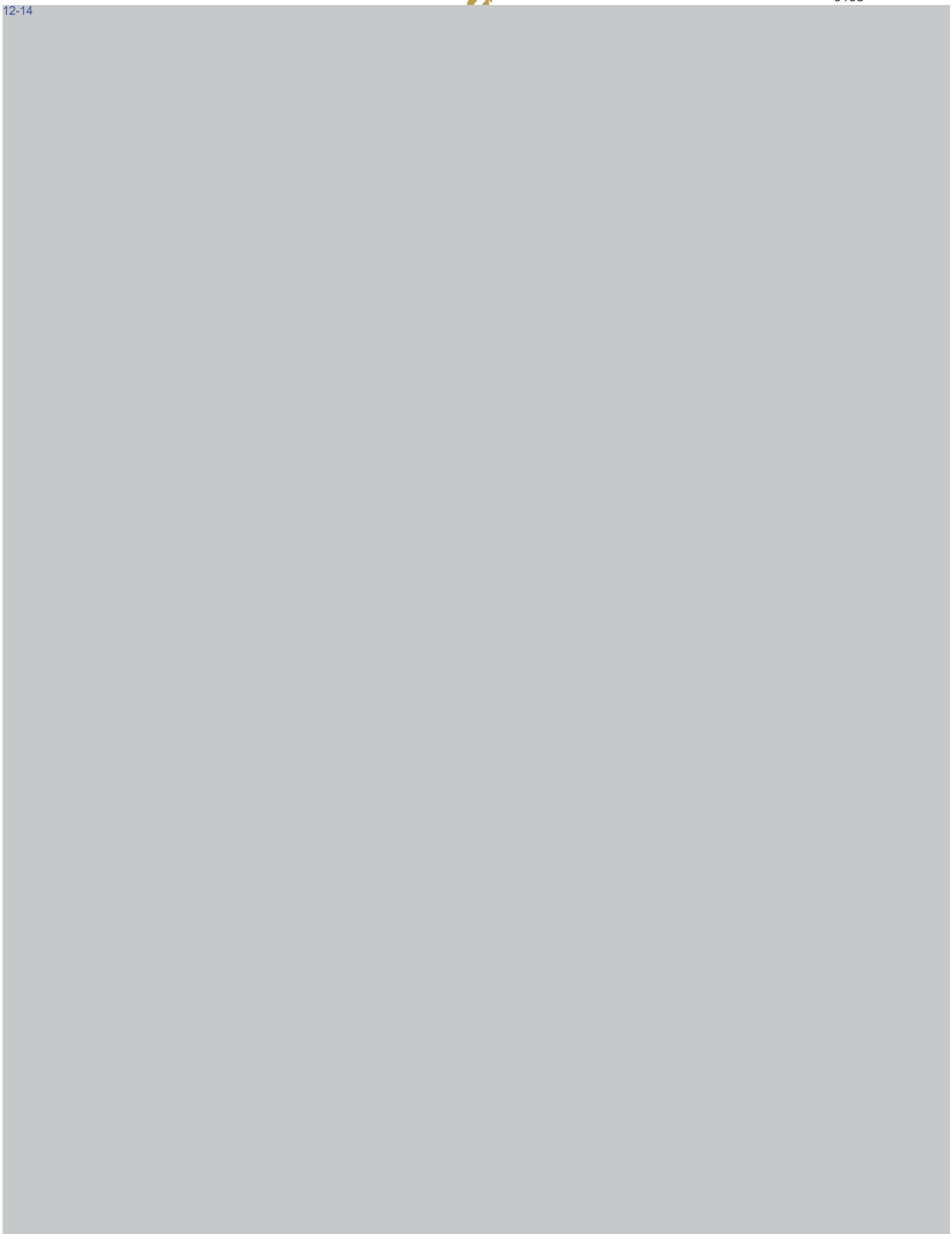

12-14

12-14



12-14

12-14



12-14

Hoofdlijnennotitie voorziening tot binnendringen

Hoofdlijnen voor de inrichting

9

Concept

Versie 0.4

Versie datum 20 april 2017

Rubricering Politie Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-02-17	Eerste versie	
0.2	06-03-17	Opmerkingen verwerkt 10.2.e , 10.2.e en Theo van der Plas	
0.3	13-03-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e	
0.4	20-04-17	Opmerkingen verwerkt Theo van der Plas 10.2.e , 10.2.e er 10.2.e	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	15-02-17	Theo van der Plas 10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, leiding DLOS, Leiding Project CCIII
0.2	06-03-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding project CCIII
0.3	13-03-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding project CCIII
0.4	20-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e , 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII

12-14

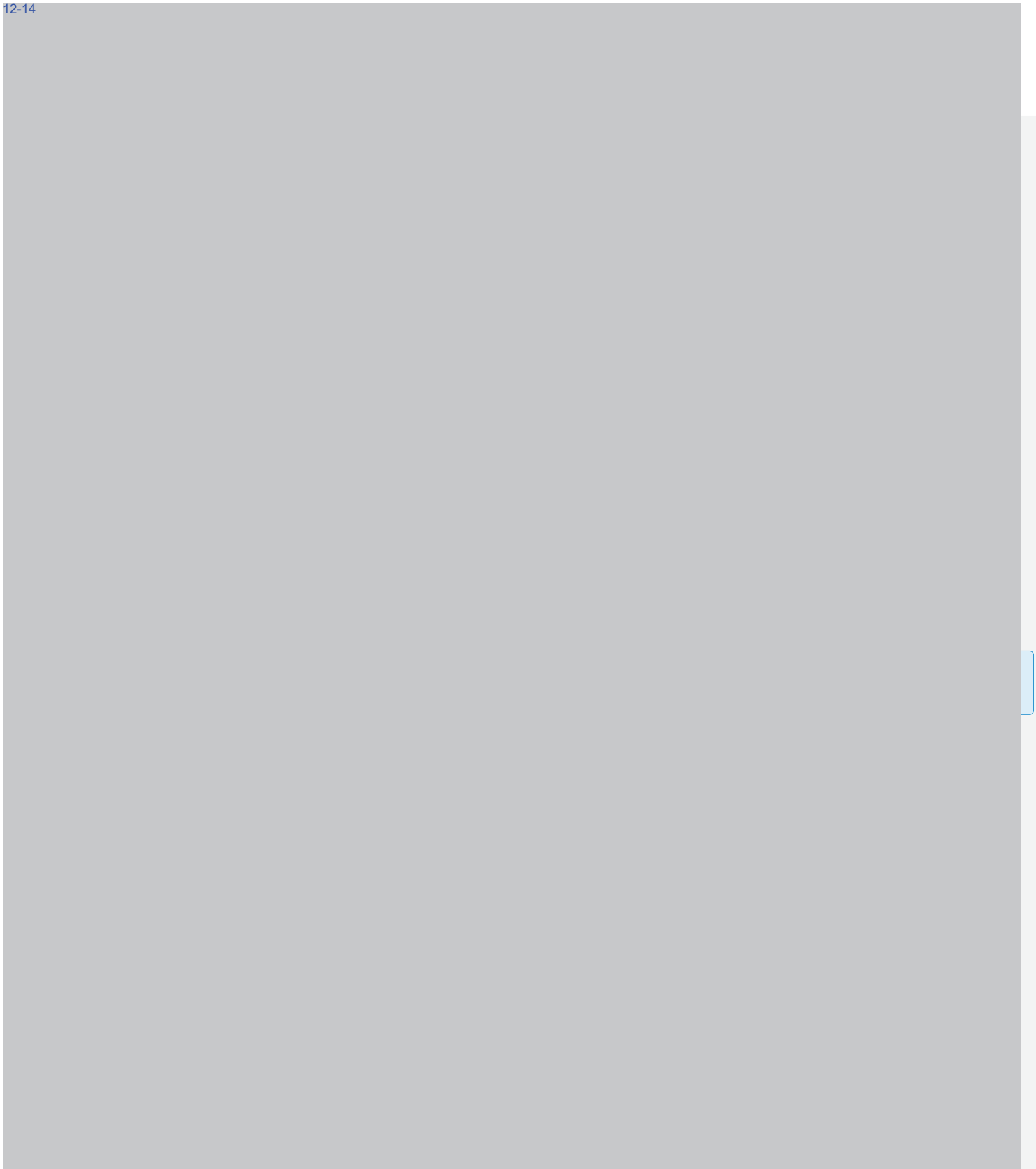
12-14

12-14

12-14

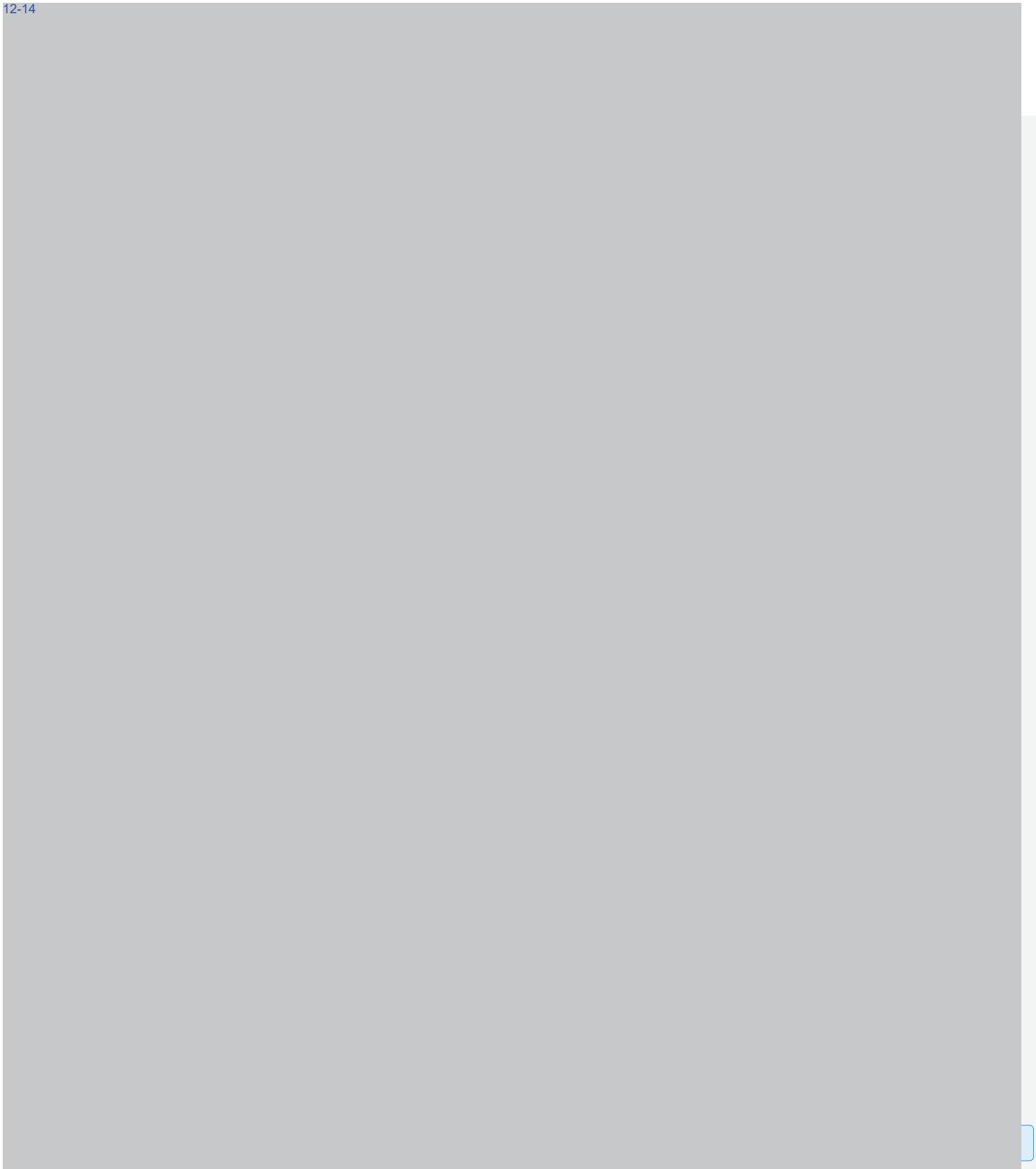
12-14

12-14

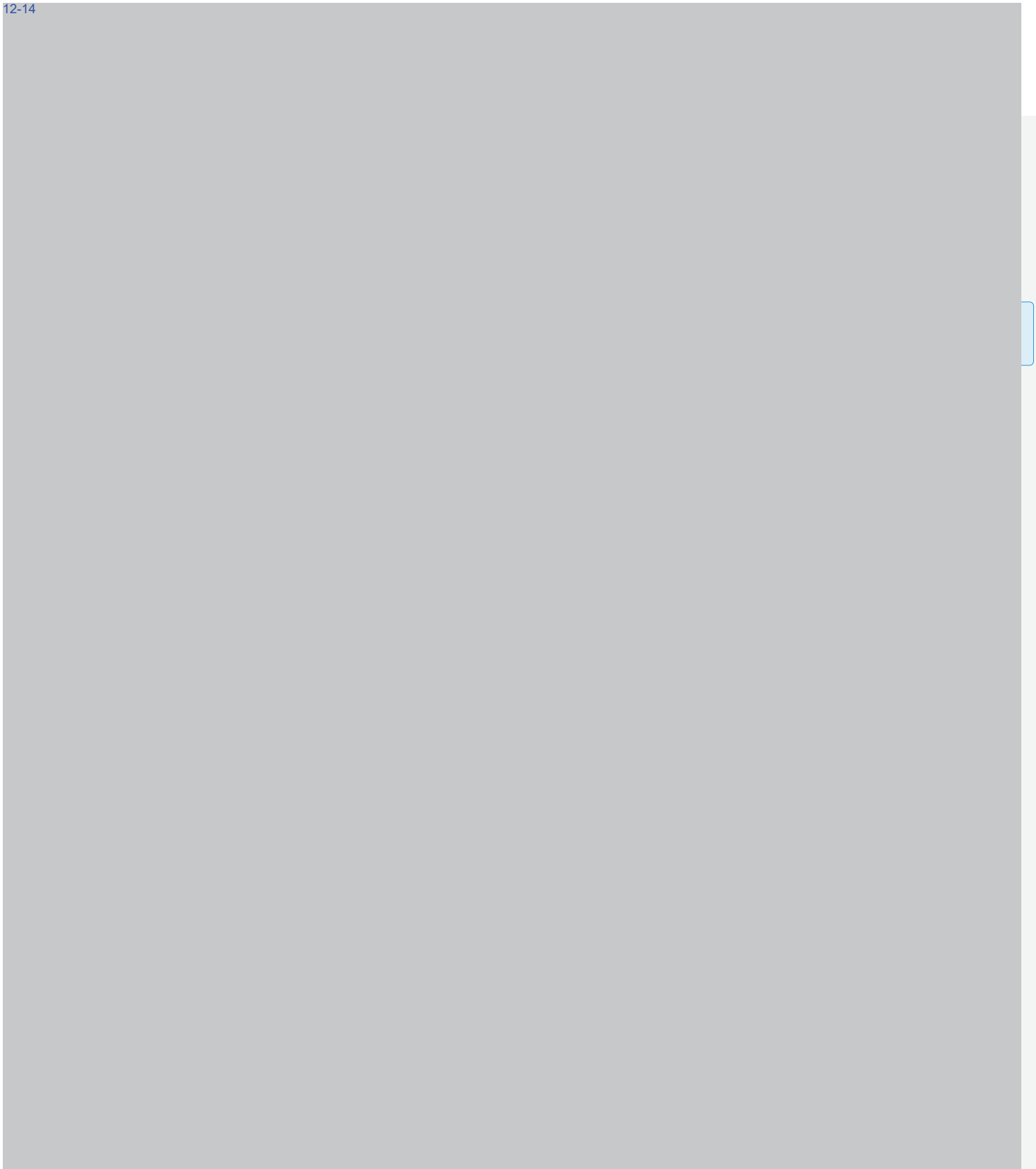


12-14

12-14



12-14



12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

Hoofdlijnennotitie voorziening tot binnendringen

Hoofdlijnen voor de inrichting

10.2.e

Concept

Versie 0.6

Versie datum 10 juli 2017

Rubricering Politie Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-02-17	Eerste versie	
0.2	06-03-17	Opmerkingen verwerkt 10.2.e ,10.2.e en Theo van der Plas	
0.3	13-03-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e	
0.4	20-04-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e en 10.2.e	
0.5	28-04-17	Opmerkingen verwerkt 10.2.e en 10.2.e en kleine redactionele wijzigingen	
0.6	10-07-17	Opmerkingen verwerkt vanuit BOO en aanpassing tijdspad.	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	15-02-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, leiding DLOS, Leiding Programma CCIII
0.2	06-03-17	Theo van der Plas, 10.2.e ,10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.3	13-03-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.4	20-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.5	28-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e ,10.2.e , 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII, Directie Operatien

0.5	02-05-17	Leden van het BOO	BOO
0.6	11-07-17	Leden van het KMTO	KMTO

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

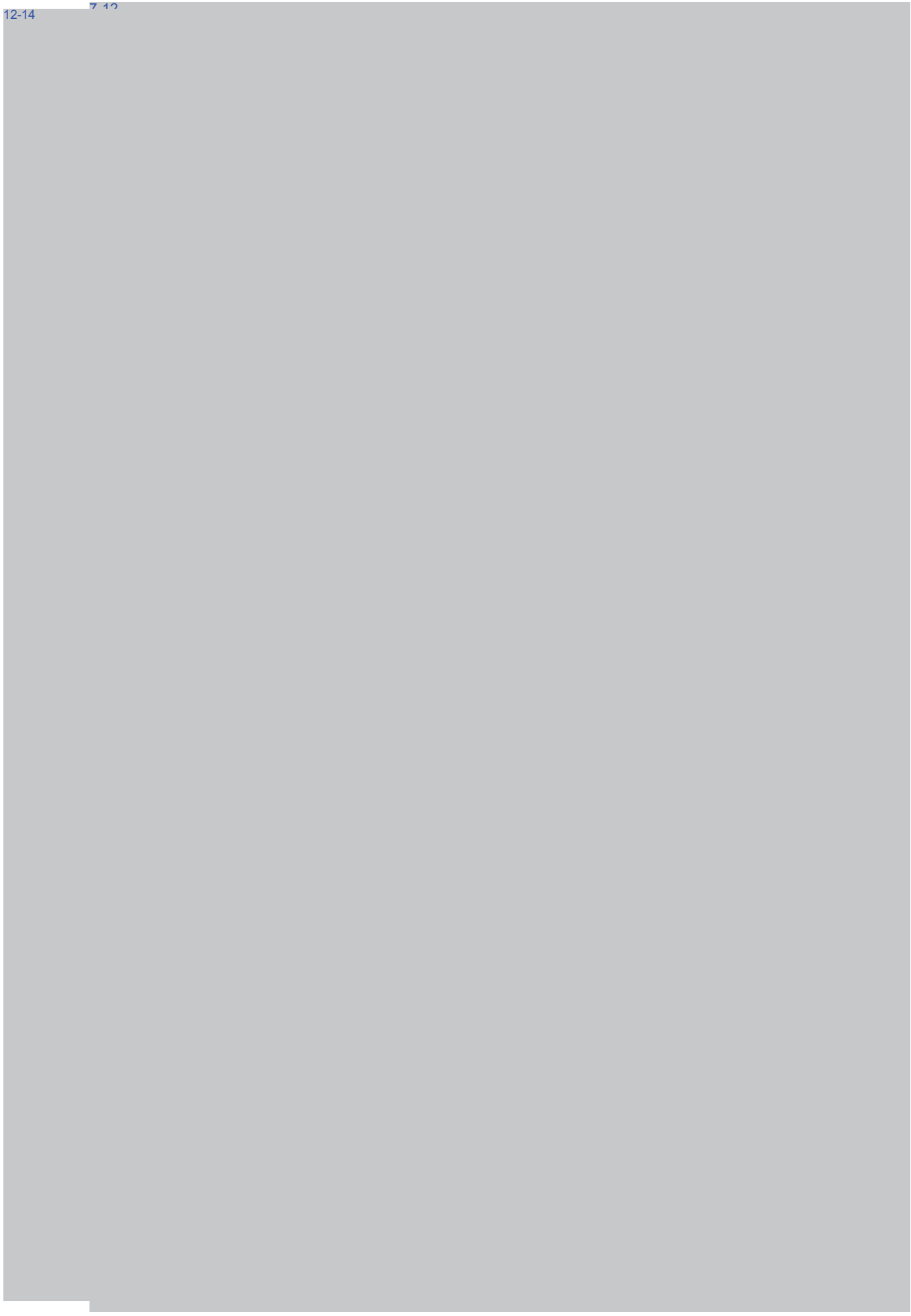
12-14

12-14

12-14

12-14

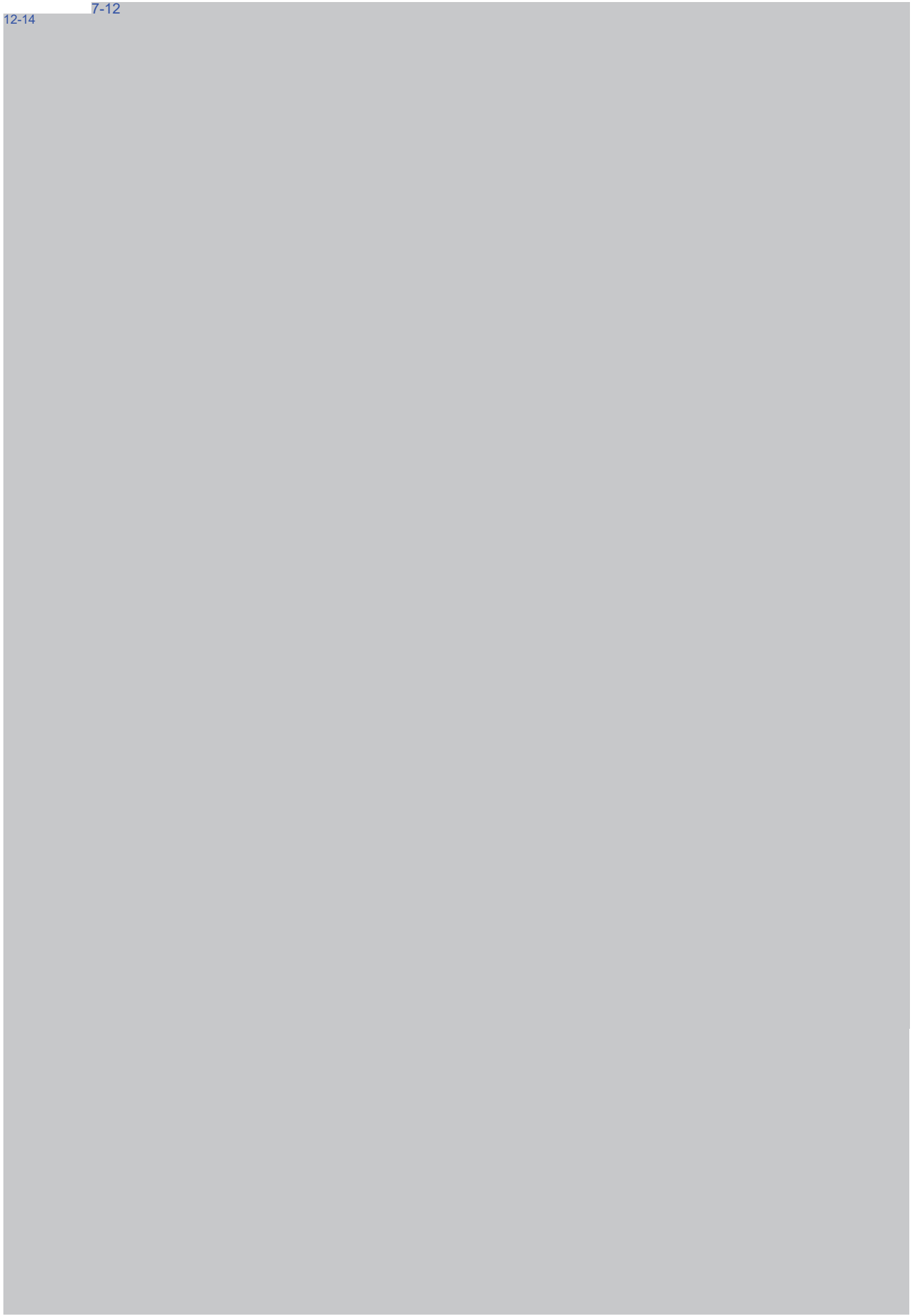
12-14


12-14

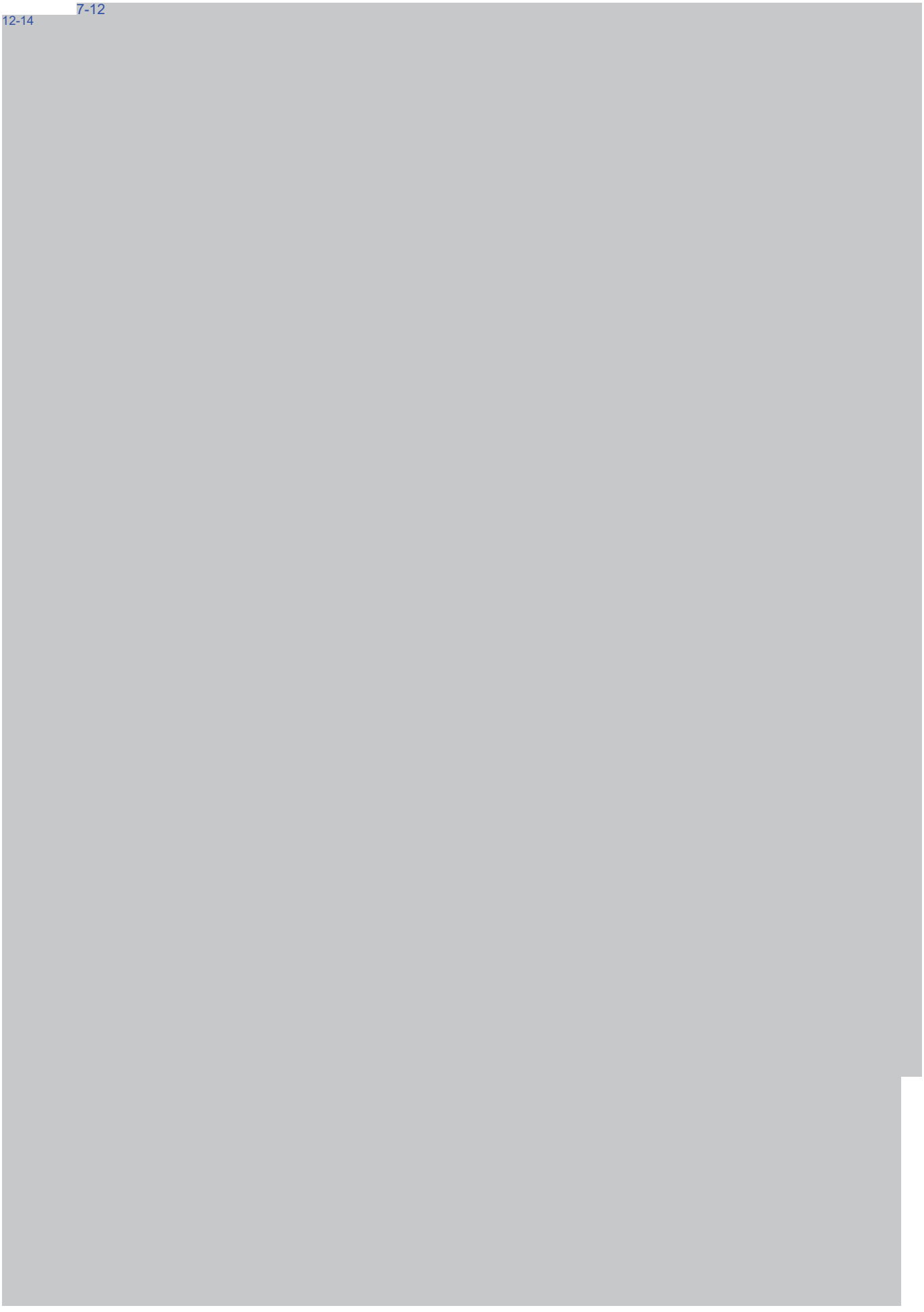
12-14

12-14


12-14
7-12


7-12
12-14

12-14


7-12
12-14

12-14

12-14

Hoofdlijnennotitie voorziening tot binnendringen

Hoofdlijnen voor de inrichting

10.2.e

Concept

Versie 0.6

Versie datum 10 juli 2017

Rubricering Politie Vertrouwelijk

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-02-17	Eerste versie	
0.2	06-03-17	Opmerkingen verwerkt 10.2.e , 10.2.e en Theo van der Plas	
0.3	13-03-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e	
0.4	20-04-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e en 10.2.e	
0.5	28-04-17	Opmerkingen verwerkt 10.2.e en10.2.e en kleine redactionele wijzigingen	
0.6	10-07-17	Opmerkingen verwerkt vanuit BOO en aanpassing tijdspad.	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	15-02-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e	Portefeuillehouder D&C, leiding DLOS, Leiding Programma CCIII
0.2	06-03-17	Theo van der Plas, 10.2.e , 10.2.e , 10.2.e 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.3	13-03-17	Theo van der Plas,10.2.e , 10.2.e , 10.2.e t, 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.4	20-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e , 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.5	28-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e 10.2.e , 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII, Directie Operatien

0.5	02-05-17	Leden van het BOO	BOO
0.6	11-07-17	Leden van het KMTO	KMTO

Inhoudsopgave

Vraagstelling

Op 21 december 2016 heeft de portefeuillehouder Digitalisering en Cybercrime (D&C) in de Nationale Briefing een presentatie gegeven over het wetsvoorstel CCIII en wat dit betekent voor de Nederlandse Politie. De Korpschef heeft verzocht om een hoofdlijnennotitie op te stellen waarin wordt beschreven hoe de politie over zal gaan tot implementatie van deze wet in de politieorganisatie.

Het KMT wordt gevraagd om:

Kennis te nemen van:

- De notitie over het programma CCIII en specifiek de implementatie van de bevoegdheid tot 'heimelijk op afstand binnendringen in een geautomatiseerd werk'.
- De fasering die in het programma is aangebracht in een fase 0 van experimenteren (tot 1 juli 2017), en fase 1 van preparen (tot 1 januari 2018) die leidt tot een nader onderbouwd realisatieplan voor fasen 1 en 2 (vanaf 1 juli 2017 tot en met 31 december 2018), waarin de PIOFACH aspecten concreet zijn uitgewerkt. Dit voorlopige realisatieplan wordt uiterlijk 1 september 2017 aan het KMT ter besluitvorming voorgelegd. Het realisatieplan voor de structurele inbedding wordt uiterlijk op 1 september 2018 aan het KMT aangeboden.
- De keuze om de voorziening voorlopig centraal in te richten en onder te brengen, gezamenlijk met de KMAR en de FIOD, bij de Landelijke Eenheid, vanwege de politiek-bestuurlijke gevoeligheden rond deze bevoegdheid en vanwege de technische en juridische complexiteit en potentieel hoge kosten van de implementatie.
- Het feit dat er op dit moment in fasen 1 en 2 onvoldoende capaciteit beschikbaar is in de voorziening om de benodigde experimenten uit te voeren die noodzakelijk zijn om tijdig een voldoende onderbouwd plan van aanpak voor de implementatie op te kunnen stellen.
- Het feit dat het lab CCIII in eerste instantie als een Eigen Beheerde Organisatie (EBO) is ingericht en dat de definitieve voorziening CCIII in de toekomst zal worden ingepast in de infrastructuur van de Nationale Politie.
- De noodzakelijke versterking van de programma-aanpak met participatie van de eenheden en partners om tot een effectieve voorlopige voorziening te komen, zoals weergegeven in de bijlage.

In te stemmen met de keuze van het BOO voor scenario 2 van de voorgestelde scenario's:

1. De Landelijke Eenheid werft 7-12 voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte van 7-12 afgeroomd ten behoeve van de Landelijk Eenheid. Hiermee wordt, gezamenlijk met de partners, een voorziening van 25 fte gecreëerd. Hierdoor komt de opgedane kennis en ervaring uiteindelijk niet terug naar de Eenheden, maar blijft centraal beschikbaar voor de politie.
2. De Landelijke Eenheid 7-12 voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in totaal 7-12 door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening van 7-12 gecreëerd. Na 2 jaar keren de medewerkers terug naar hun eenheid, waardoor de kennisontwikkeling van de eenheden een impuls krijgt. Het is dus lonend om te investeren voor de eenheden. Terugkeer zal gefaseerd plaatsvinden om een braindrain van de nieuwe eenheid te voorkomen.

Op basis van bovenstaande keuze te besluiten dat:

- Het sectorhoofd van de DLOS van de Landelijke Eenheid de opdracht krijgt om de voorziening op basis van deze notitie en de realisatieplannen in te richten en tot werking te brengen. Het betreft nu een tijdelijke

voorziening en in september 2018 wordt op basis van het definitieve realisatieplan een besluit over de structurele inbedding en financiering genomen.

- Er gestart wordt met de centrale werving en de eenheden (incl. DLOS) vacatureruimte ter beschikking stellen.- Daartoe een landelijke wervingscampagne wordt gestart, waarbij medewerkers van de eenheden mee kunnen solliciteren.
- Conform de afspraak met het BOO een visie moet worden ontwikkeld over de terugkeer van de geleverde mensen naar de eenheden, met een nadere duiding en koers hoe dit duurzaam tot stand kan worden gebracht.

1. Inleiding

Het wetsvoorstel CCIII gaat over de vergroting van de effectiviteit van het politieoptreden in het gehele opsporingsdomein. Met de nieuwe bevoegdheid om heimelijk op afstand geautomatiseerde werken binnen te dringen zullen we als politie onder andere weer in staat zijn om bij de communicatie tussen criminelen te komen. De traditionele interceptietechnieken leveren tegenwoordig steeds minder voldoende inhoudelijke informatie (door toenemend gebruik van encryptie) op. Met deze nieuwe bevoegdheid repareren we de achterstand, die de politie heeft op het terrein van de digitalisering van de maatschappij en de criminaliteit. Deze wet biedt de politie de mogelijkheid om op creatieve wijze de criminaliteit aan te pakken, door juist in de virtuele wereld gebruik te maken van mogelijkheden die in de fysieke wereld niet aanwezig zijn.

Als voorbereiding op de inwerkingtreding van de wet is in 2014 een impactanalyse opgesteld waarin een eerste impact op de operatiën en bedrijfsvoering is bepaald. Het programma CCIII is daaropvolgend op 1 januari 2015 van start gegaan. Op 14 augustus 2015 is het PID Binnendringen fase 1 opgeleverd en door de portefeuillehouder D&C goedgekeurd, waarmee de start werd gemaakt van de laboratorium omgeving van het programma CCIII bij de Landelijke Eenheid (DLOS). Vanaf 1 januari 2016 zijn de feitelijke werkzaamheden in de lab omgeving van start gegaan. Hieronder wordt kort weergeven op basis waarvan deze hoofdlijnennotitie is opgesteld. Het gaat dan vooral om de keuze voor het centrale model, de verbinding met de TDO's en de Eenheden en de verbindingen met de overige (digitale) ontwikkelingen binnen de Nationale Politie.

Tijdspad

De wet CCIII treedt op 1 januari 2018 in werking. De politie heeft om deze bevoegdheid gevraagd. De nieuwe bevoegdheid is noodzakelijk voor goed politiewerk en is een kans voor de opsporing. Invulling geven aan de nieuwe bevoegdheid komt neer op een innovatie die substantiële investeringen vereist.

Ten tijde van het opstellen van deze hoofdlijnennotitie is ervan uitgegaan dat het realisatieplan CCIII op 1 juli 2017 aan het KMT aangeboden zou worden. De aanvankelijke gedachte daarbij was dat met ingang van 1 januari 2018 een structurele CCIII voorziening geïmplementeerd zou worden. In de eerste helft 2017 heeft het programma CCIII analyses uitgevoerd naar zowel de risicofactoren als de succesfactoren bij realisatie van CCIII. Daarbij zijn de succesfactoren bij vergelijkbare vernieuwingen bij o.a. samenwerkingspartners, het buitenland en eerdere ervaringen in de politieorganisatie (realisatie van de OVC bevoegdheid en opzet van het THTC) onderzocht. Uit de analyses blijkt dat de bij de politie gebruikelijke blauwdruk- c.q. uitrolbenadering van veranderen zich niet verhoudt met effectieve en zorgvuldige realisatie van de nieuwe CCIII voorziening. De belangrijkste redenen daarvoor zijn de inhoudelijke complexiteit van CCIII; de grote dynamiek/ veranderlijkheid en onzekerheden in de omgeving waaronder politiek en wetgeving; en het feit dat het om een compleet nieuwe manier van werken gaat waarmee nog geen ervaring bestaat, zodat een referentiekader ontbreekt.

Deze inzichten zijn gedeeld met de begeleidingscommissie CCIII, waarin in- en externe experts en samenwerkingspartners zitting hebben. In overleg met de begeleidingscommissie, de programmadirecteur digitalisering en cybercrime, het sectorhoofd DLOS en de programmamanager CCIII is ervoor gekozen om het realisatieplan in twee fasen op te leveren. Op 1 september 2017 wordt het voorlopige realisatieplan voor periode van 1 januari 2018 t/m 31 december 2018 opgeleverd. In dit voorlopige realisatieplan worden de belangrijkste mijlpalen en op te leveren deelproducten uitgewerkt. Een samenvatting van de planning is in de bijlage opgenomen.

In 2018 zal de nieuwe bevoegdheid zorgvuldig en stapsgewijze worden toegepast, zodat ervaring wordt opgedaan die wordt benut bij het verder vormgeven en uitbouwen van de nieuwe werkwijze. Op 1 september 2018 wordt het definitieve realisatieplan opgeleverd, waarin een voorstel voor de structurele inrichting van de voorziening in alle relevante aspecten is uitgewerkt. De mijlpalenplanning voorziet in een structurele implementatie van de CCIII voorziening met ingang van 1 januari 2019, onder gelijktijdige afbouw van de programma-organisatie.

Er zijn vooralsnog geen structurele middelen beschikbaar om deze nieuwe bevoegdheid vorm te geven. Realisatie van de voorlopige voorziening tot binnendringen (in de periode tot en met 2018) geschiedt voor het overgrote deel door tijdelijke middelen vanuit de portefeuille Digitalisering en Cybercrime in te zetten en door tijdelijke herschikking van personele capaciteit. DLOS en de landelijke en regionale eenheden stellen ieder 7-12 ter beschikking, terwijl de samenwerkingspartners FIOD en KMAR samen met 7-12 participeren. Het definitieve realisatieplan dat op 1 september 2018 aan het KMT wordt aangeboden, omvat een volledige begroting en dekkingsvoorstel en een voorstel voor de formalisering van de samenwerking met de FIOD en de KMAR.

De gefaseerde oplevering biedt als voordeel dat besluitvorming beter doordacht en zorgvuldiger kan plaatsvinden, maar als mogelijk nadeel dat structurele middelen mogelijk niet op tijd gereserveerd kunnen worden zowel. Vanaf de tweede helft van dit jaar worden de samenwerking en verbinding met (vooral) tactische recherche en TDO's van de eenheden en externe partners versterkt door participatie in de vorm van 'samen bouwen' aan de nieuwe voorziening. Dit is verder uitgewerkt in de notitie versterking programma-aanpak CCIII.

Doelstelling van deze notitie is om tot een besluit te komen om over te kunnen gaan tot de werving van de minimaal benodigde capaciteit/expertise om op 1 januari 2018 het lab om te schakelen naar een werkende proefopstelling (fase 1). Dit besluit is op korte termijn noodzakelijk i.v.m. de noodzakelijke stappen in het personeelsproces (wervingscampagne, werving, selectie, screening, aanwijzing, opleiding e.d.). Zo kan, bij een positief verloop, eind 2017 een minimum aantal gekwalificeerde medewerkers aan het werk zijn voor de voorziening. Zo kunnen we voorkomen dat we wel de bevoegdheid hebben, maar de bevoegdheid niet in kunnen zetten.

Keuze voor het centrale model

In deze notitie wordt als uitgangspunt genomen dat de voorziening tot binnendringen op een centrale wijze wordt ingericht. Er is gekozen voor een (voorlopig) centrale aanpak. Deze keuze is gemaakt vanwege de politiek-bestuurlijke gevoeligheden, de keuze van de wetgever om deze bevoegdheid centraal te regelen en vanwege de complexiteit en hoge kosten die de implementatie met zich meebrengt. Het is daarom van groot belang dat er door de Eenheden geparticipeerd wordt in de bouw van deze voorziening voor alle opsporingsinstanties (politie, FIOD en KMAR). Hierdoor kan er kennis en expertise gedeeld en ontwikkeld worden voor de gehele politieorganisatie en de gehele opsporing in Nederland. Om deze reden dient deze centrale aanpak feitelijk gezien te worden als een gezamenlijke aanpak.

Om op dit moment een voorziening te bouwen voor alle opsporingsinstanties, welke in staat is om per 1 januari 2018 te bevoegdheid tot binnendringen uit te voeren is het noodzakelijk nu een team van 7-12 te creëren. Hiervoor zal de DLOS 7-12 vrijmaken binnen de huidige formatie. Daarnaast wordt uitgegaan van de levering van 7-12 door de KMAR, FIOD en overige partners. De partners KMAR en FIOD participeren reeds en gaan hun inzet verder uitbouwen. De eenheid Amsterdam doet ook al mee. De eenheid Zeeland West Brabant en Den Haag hebben 1 fte vacatureruimte ter beschikking gesteld. De overige eenheden participeren nog niet.

De voorziening wordt voorlopig opgezet met tijdelijke capaciteit vanuit de eenheden. Dat is reëel omdat er nog geen formatieruimte beschikbaar is en biedt meer flexibiliteit in de bouwfase. Deze capaciteit kan op twee manieren worden gerealiseerd. Deze twee manieren worden hieronder opgesomd. De eerste manier gaat uit van het afromen van

formatieruimte uit de eenheden ten behoeve van de voorziening. Deze formatieruimte blijft dan bij de Landelijke Eenheid. De tweede manier gaat uit van het vrijwillig tewerkstellen van gekwalificeerde medewerkers vanuit de eenheden voor 2 jaar om daarna met de opgebouwde kennis en ervaring terug te keren naar de eigen eenheid. Het is aan het KMT om hierin een keuze te maken.

Kort gezegd staat het KMT voor de keuze uit de onderstaande voorstellen:

1. De Landelijke Eenheid werft 7-12 voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte van 7-12 afgeroomd ten behoeve van de Landelijk Eenheid. Hiermee wordt, gezamenlijk met de partners, een voorziening van 7-12 gecreëerd. Hierdoor komt de opgedane kennis en ervaring uiteindelijk niet terug naar de Eenheden, maar blijft centraal beschikbaar voor de politie.
2. De Landelijke Eenheid werft 7-12 voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in totaal 7-12 door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening van 7-12 gecreëerd. Na 2 jaar keren de medewerkers terug naar hun eenheid, waardoor de kennisontwikkeling van de eenheden een impuls krijgt. Het is dus lonend om te investeren voor de eenheden. Terugkeer zal gefaseerd plaatsvinden om een braindrain van de nieuwe eenheid te voorkomen.

De werving van nieuwe medewerkers wordt centraal en gelijktijdig in – en extern opengesteld. Invulling van de vacatures kan zowel via externe inhuur (ICT, wetenschap, etc.) als via personeel vanuit de eenheden plaatsvinden. Hiermee kan externe deskundigheid die nog niet beschikbaar is binnen de politie tijdelijk worden binnengehaald. De vereiste expertise is zeer schaars, zowel in de politieorganisatie als in de arbeidsmarkt. Forse inspanningen zijn nodig om de expertise te werven en te behouden. Ook daarom kan werving niet langer uitgesteld worden.

Verbinding met TDO's

In elke eenheid is een TDO ingericht. Deze TDO's zullen straks een belangrijke schakel vormen tussen het tactische team in de eenheid (de vragende partij) en het technisch team bij de Landelijke Eenheid (de uitvoerende partij). De gedachte is 7-12

De TDO's zullen zo, samen met het CCIII team, een gelinkt netwerk vormen, waardoor de informatie-uitwisseling tussen techniek en tactiek zo efficiënt mogelijk verloopt. Dit netwerk is noodzakelijk om zo de input vanuit het CCIII team via het TDO naar het tactische team door te geleiden als bruikbare informatie voor het opsporingsonderzoek. Deze werkwijze staat borg voor efficiënte en korte lijnen tussen opsporing en technisch team, met inachtneming van de wettelijke eis van functiescheiding.

Verbinding met de Eenheden

Zoals hierboven aangeven wordt er nu uitgegaan van de inrichting van een centrale gezamenlijke voorziening voor alle opsporingsinstanties in Nederland. Dit betekent uiteraard niet dat de Eenheden hiermee geen invloed hebben op de werkzaamheden die in het CCIII team uitgevoerd worden. De tactische teams in de eenheden zijn de vragende partij en alleen op basis van verzoeken zal het CCIII team zijn werkzaamheden uitvoeren. Het is daarom van groot belang dat de Eenheden vanaf het begin betrokken zijn bij de inrichting van het lab CCIII en de voorziening, zodat de wensen vanuit de Eenheden mee worden genomen bij de bouw van het lab CIII en het team.

Verbinding met het buitenland

Nederland heeft de hoogste 'digital density[1]' ter wereld. Digitale technologie is in ons land sterk doorgedrongen tot bedrijven en economie. Continue innoveren en investeren in nieuwe ontwikkelingen als CCIII is ook daarom noodzakelijk. Vanuit onze koppositie is internationale samenwerking een gegeven. Nederland is het niet het enige land waar deze bevoegdheid uitgevoerd wordt. Er zijn door het programma CCIII verkennende gesprekken gevoerd met 7-12 . De mogelijkheden voor verdere samenwerking met deze landen wordt op dit moment onderzocht.

Verbinding met overige (digitale) ontwikkelingen

De portefeuille D&C investeert in de oprichting van 7-12 , die ingezet gaan worden voor projecten en programma's binnen deze portefeuille. Het programma CCIII participeert hierin om de implementatie van de nieuwe bevoegdheid vorm te geven. Binnen de lab omgeving van het programma wordt ook volgens 7-12 gewerkt en deze innovatieve aanpak past uitstekend binnen de portefeuille D&C. Door aansluiting te zoeken bij deze nieuwe methodiek kan sneller worden ingespeeld op nieuwe concepten en daardoor kunnen deze nieuwe concepten sneller worden geïmplementeerd binnen de politie organisatie.

Daarnaast is door het programma CCIII aansluiting gevonden bij het Programma Herijking Opsporing. CCIII kan namelijk als katalysator dienen voor de digitale ontwikkeling van de Nationale Politie. De aanpak vanuit CCIII draagt bij aan een innovatieve en vernieuwende aanpak van de digitale ontwikkeling van de opsporing. Ook is de verbinding gezocht binnen de portefeuille Digitalisering en Cybercrime met de projecten Digitaal Opsporen en Cybercrime en met de portefeuilles Zeden en CTER. Bovendien is het programma CCIII onderwerp van onderzoek voor het onderzoeksprogramma Technologie en Informatiegebruik van de Politieacademie (in opdracht van de KL).

Vanuit de KL wordt binnen het project Bijzondere Bedrijfsvoering gewerkt aan de inrichting van een Serviceteam Afgeschermde Operatie & Bedrijfsvoering (STA-OB). Het programma sluit hierbij aan om de afgeschermde inkoop van technische middelen te kunnen stroomlijnen.

Governance

Vanaf 1 april 2017 fungeert de programmadirecteur Digitalisering en Cybercrime als opdrachtgever van het programma CCIII. Het sectorhoofd DLOS treedt als opdrachtnemer op voor het inwerking brengen van deze voorziening. Het programma CCIII is belast met de dagelijkse uitvoering van de werkzaamheden en zal regelmatig over de voortgang rapporteren aan de opdrachtnemer. De opdrachtnemer heeft een begeleidingsgroep tot haar beschikking waarin alle relevante partijen (OM, IM/IV, TAO, TEXPO, HDE, FIOD, KMAR, etc.) zitting hebben.

2. Fase 1 (experimenteerfase) naar fase 2 (implementatiefase)

Er is in 2016 door 7-12 medewerkers van verschillende afdelingen van de DLOS (ATOE, AO en I&S) een infrastructuur gebouwd, waarmee bij inwerkingtreding van de wet de eerste zaken gedraaid kunnen worden. Op basis van experimenten worden de eerste voorbereidingen getroffen voor de uitvoering van de nieuwe bevoegdheid. Hierbij valt te denken aan het bepalen van de juiste architectuur voor een veilige infrastructuur van waaruit de politie kan gaan werken, het experimenteren met demo software op geautomatiseerde werken in een gesloten omgeving of deze

[1] Zie b.v. Digital Density Index, Accenture Oxford Economics 2016.

software bruikbaar kan zijn, het draaien van oefeningen om te zien of de werkprocessen toepasbaar zijn, het bepalen van de juiste functieprofielen en het evalueren van opsporingsonderzoeken waarin het mogelijk zou zijn geweest om deze bevoegdheid in te zetten. Al deze voorbereidende werkzaamheden leiden er toe dat het bij inwerkingtreding van de wet duidelijk is op welke manier het “echte” werk uitgevoerd wordt. Verdere doorontwikkeling naar de implementatie is nu noodzakelijk.

Fase 1 (experimenteerfase tot 1 januari 2018)

Op basis van het gekozen scenario zal de werving voor de verdere uitbouw van het lab CCIII worden uitgevoerd. Hieronder wordt voor fase 1 aangegeven welke rollen er noodzakelijk zijn om tot een werkende voorziening te komen. Er wordt gesproken over rollen aangezien het werken met specifieke functies niet past op het flexibel organiseren van de opgaven van het CCIII team. Daarom is de opzet uitgewerkt in rollen en zo goed mogelijk passend gemaakt op de bestaande LFNP functieprofielen. Daarna wordt aangegeven welke rollen er noodzakelijk zijn vanaf 1 januari 2018 om de tijdelijke voorziening operationeel te krijgen. De rollen in fase 1 en 2 zijn in sommige gevallen overlappend, er zijn niet altijd nieuwe fte’s nodig om de werkzaamheden uit te kunnen voeren. Voor alle functies voor het lab CCIII, het CCIII inzetteam en de ondersteuning van het inzetteam is een uitgebreide functiebeschrijving opgenomen in bijlage 1.

Behoefte lab CCIII

Op korte termijn is er de behoefte aan de volgende rollen/functies met de gedachte dat de voorziening voor binnendringen vanaf 1 januari 2018 uit 7-12 zal bestaan. Om de processen binnen het lab goed uit te kunnen voeren, moeten er taken worden uitgevoerd die te bundelen zijn in verschillende rollen. Afhankelijk van de grootte van het team en de competenties van de medewerkers zullen medewerkers een of meerdere rollen binnen hun functie uitoefenen. Een nadere uitwerking zal in de realisatieplannen plaatsvinden. Deze behoefte is mede tot stand gekomen door gesprekken met een van onze partners in het veiligheidsdomein. Deze partner heeft al geruime tijd de mogelijkheid tot het heimelijk op afstand binnen te dringen in geautomatiseerde werken. De kennis en ervaring (zowel op personeel als op technisch vlak) die hier is opgedaan is van wezenlijk belang voor inrichting van de voorziening bij de politie. Hieronder is een lijst met rollen opgenomen waar op dit moment behoefte aan is:

1. **Coördinator/teamleider: 1 fte.**
2. 7-12
3.
4.
5.

3. Fase 2 (implementatiefase vanaf 1 januari 2018)

Per 1 januari 2018 zal op basis van de input van het voorlopig realisatieplan gestart worden met de voorlopige voorziening tot binnendringen. In dit voorlopig realisatieplan zullen alle bedrijfsvoering aspecten aan de orde worden gesteld om te komen tot een werkende voorziening. Dit houdt in dat er een duidelijk beeld zal worden geschetst van onder andere de benodigde huisvesting, personeel, financiën, techniek en opleidingen. Op basis van dit voorlopig realisatieplan zal gestart worden met de inrichting van de voorziening tot binnendringen. Een definitief ingerichte voorziening zal per 1 januari 2019 gereed zijn.

Per 1 januari 2018 zal de voorziening tot binnendringen uit 7-12 moeten bestaan om de eerste zaken te kunnen draaien. Op basis van ervaringen is duidelijk geworden dat voor een goede uitvoering van een CCIII actie het noodzakelijk is om 7-12 in het inzetteam CCIII te hebben en om voor 1 inzetteam 7-12 aan ondersteuning te hebben.

Het is van belang om op te merken dat sommige rollen zowel in het CCIII inzetteam benodigd zijn als in de periferie rondom het inzetteam. Deze scheiding is noodzakelijk om te zorgen voor functiescheiding tussen het inzetteam en de overige leden van de voorziening. Op deze wijze wordt voorkomen dat manipulatie van gegevens van binnenuit mogelijk is: Zoals hierboven is aangegeven is er op dit moment onvoldoende capaciteit om de implementatie van de nieuwe bevoegdheid goed vorm te geven. Het gaat hier niet alleen om technische ondersteuning, maar ook om bijvoorbeeld juridische ondersteuning. Deze inzet is niet alleen in fase 1, maar ook in de implementatiefase (fase 2) noodzakelijk. In fase 2 zal de voorziening operationeel werkend moeten zijn.

CCIII inzetteam 7-12

Een inzet team is verantwoordelijk voor het uitvoeren van een of meerdere inzetten (tegelijkertijd). Zij zouden als zelfstandig en zelfsturend team moeten functioneren en slechts een heel beperkte afhankelijkheid moeten hebben met de rest van het unit / afdeling. Op basis van ervaringen van o.a. veiligheidspartners is bepaald dat een inzet team uit 10 fte bestaat. Indien er behoefte is aan het opschalen zodat meer zaken tegelijkertijd, dan wel per tijdseenheid uitgevoerd kunnen worden, zullen extra inzet teams toegevoegd moeten worden. Het vergroten van een enkel inzet team is waarschijnlijk contraproductief. Om het inzet team zelfstandig te kunnen laten functioneren, zullen er een redelijk aantal rollen zoals hier gedefinieerd moeten worden ingevuld. Elke medewerker zal binnen het inzet team twee of meerdere rollen moeten kunnen vervullen.

1. **Leider Operaties**
2. 7-12
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

Schematisch betekent dit het volgende voor de samenstelling van het inzetteam (1 fte kan meerdere rollen vervullen):

Rol	LFNP Functie	Aantal
Teamleider	Teamchef C	1
7-12	OS-D	7-12
	OS-C/D	
	OS-C/D/E	
	OS-B/C/D	
	OS-A/B/C	
	OS-C/D	
	OS-B/C/D	
	OS-B/C	
	OS-D	

7-12

OS-A/B

OS-B/C/D

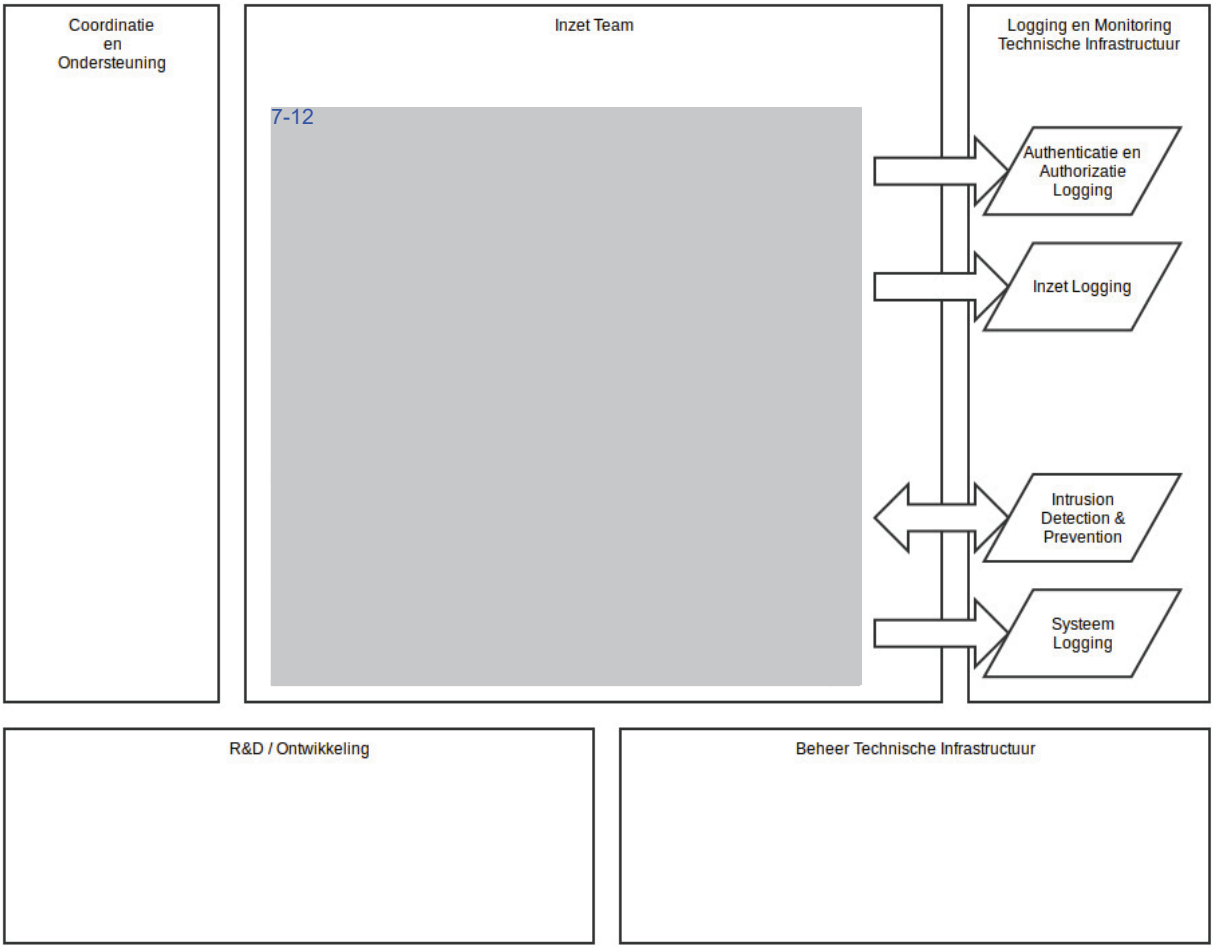
7-12

Coördinatie en Ondersteuning CCIII team 7-12

Om het CCIII inzetteam te laten functioneren zijn de volgende ondersteunende rollen/functies nodig binnen de voorziening:

1. **Teamleider**
2. 7-12
3.
4.
5.

De precieze invulling van deze 7-12 is nog niet uitgewerkt in rollen en functies. Dit wordt nader uitgewerkt in het voorlopig realisatieplan. Een groot aantal van deze rollen zijn al benoemd ten behoeve van het inzetteam. De werkzaamheden binnen de coördinatie en ondersteuning zullen verschillen van de werkzaamheden binnen het inzetteam. Op dit moment is de behoefte aan deze medewerkers minder urgent dan de medewerkers voor het CCIII inzetteam, met uitzondering van de teamleider rol. Deze zal door de DLOS worden meegenomen in de openstelling van de 7-12 . Schematisch ziet de rolverdeling er ongeveer uit als in onderstaand schema..



4. Randvoorwaarden

Investeren in de Keuringsdienst

Een belangrijk aandachtspunt is de keuring van het technische hulpmiddel. De keuringsdienst van de Landelijke Eenheid wordt hiervoor, naast haar huidige keuringswerkzaamheden, verantwoordelijk. De keuringsdienst is analoog ingesteld en zal op basis van de huidige bezetting niet in staat zijn om tijdig middelen te kunnen keuren die ingezet zullen worden voor de bevoegdheid tot het heimelijk op afstand binnendringen in een geautomatiseerd werk. De keuringsdienst zal moeten worden uitgebreid met digitaal specialisten die in staat zijn om de eisen die het besluit gaat stellen aan de keuring van het technisch hulpmiddel op een snelle en zorgvuldige manier uit te voeren.

Vooruitlopend op fase 2 is het noodzakelijk dat in fase 1 de keuringsdienst wordt uitgebreid met 7-12 testengineers) om in staat te zijn de digitale middelen voor de voorziening te keuren. Deze vraag staat los van de uitvraag aan de eenheden voor het CCIII team, echter de eenheden worden ook uitgenodigd om hiervoor de expertise te leveren. Een uitgebreide functiebeschrijving is te vinden in bijlage 2.

Investeren in security

Op het moment dat er binnengedrongen gaat worden, is het zeer waarschijnlijk dat de ICT infrastructuur van de politie zelf ook meer aangevallen zal gaan worden. Het gaat om twee dingen: aanvallen op de algemene infrastructuur van de politie en specifieke aanvallen op de CCIII voorziening. Het is absoluut noodzakelijk dat de security van de digitale infrastructuur van de Nederlandse Politie op een zeer hoog niveau ligt. 7-12 , kan hier een belangrijke rol in spelen. Zij zijn in staat om aan te geven waar de zwakheden in de systemen liggen als zij het juiste mandaat hebben om onafhankelijk onderzoek te doen. Een intensieve samenwerking tussen 7-12 en de voorziening is van groot belang. Ook uitbreiding van 7-12 maakt onderdeel uit van het cyber security fiche.

Investeren in opleidingen, huisvesting en financiën

Op basis van bovenstaande is duidelijk dat er geïnvesteerd moet worden in mensen. In de praktijk blijkt dit een grote uitdaging te zijn. Daarnaast liggen er ook nog grote uitdagen op de terreinen van opleidingen, huisvesting en middelen. Dit wordt hieronder kort toegelicht.

Opleidingen

Hoog gekwalificeerd personeel is nodig om met de meest geavanceerde middelen aan de slag te gaan. Samen met de Directie HRM wordt een strategie bepaald om te komen tot een innovatieve manier van werving. Daarnaast zal er samen met de Politieacademie in 2017 gewerkt worden aan het opstellen van een opleidingsplan, om politiemedewerkers op te leiden en te certificeren om te mogen binnendringen. Tot op heden is de Politieacademie niet in staat geweest om te voldoen aan deze vraag.

Huisvesting

In 2018 zal verder worden gebouwd aan de voorziening tot binnendringen. De precieze invulling hiervan zal nader worden uitgewerkt in het voorlopig realisatieplan. Op dit moment is het lab CCIII 7-12 gehuisvest en deze ruimte is nu al ontoereikend. Zonder voldoende huisvesting is verder doorontwikkeling niet mogelijk en zullen de gevraagde fte's niet geplaatst kunnen worden. Er zal door de Landelijke Eenheid gezocht moeten worden naar een huisvestingslocatie om de voorziening tijdig en adequaat te kunnen huisvesten.

Financiële consequenties

Techniek, mensen, huisvesting en middelen vergen grote investeringen, terwijl het structurele budget van de politie hierin niet voorziet. De precieze invulling hiervan zal nader worden uitgewerkt in de realisatieplannen. Vanuit de portefeuille D&C zijn er gelden beschikbaar gesteld voor de opstartkosten van het laboratorium CCIII, waarmee op het

moment van inwerkingtreding van de wet de eerste zaken gedraaid zullen kunnen worden. Vanuit deze middelen kunnen echter geen structurele kosten worden betaald. Duidelijk is wel dat de invoering van deze nieuwe bevoegdheid niet alleen kosten met zich meebrengt. Deze manier van werken betekent bijvoorbeeld dat het bij een actie op het terrein van Kinderporno niet meer noodzakelijk zal zijn om de verdachte op heterdaad te betrappen. Hierdoor zal de inzet van bijvoorbeeld, 7-12 veel minder intensief kunnen zijn in bepaalde zaken. Er kan in de toekomst op een andere (goedkopere) manier in een groot tactisch onderzoek inzicht worden gekregen in de criminele structuren. De precieze opbrengsten zijn op dit moment nog niet in kaart gebracht, maar zullen worden meegenomen in de realisatieplannen. De structurele kosten zijn meegenomen in de cyber security fiche voor de onderhandelingen van het nieuwe kabinet.

5. Risico's

Een van de grootste risico's is dat de Eerste Kamer niet akkoord gaat met het wetsvoorstel en dat het terug wordt gezonden aan de Tweede Kamer.

Overige risico's zijn daarnaast onderschatting van de complexiteit van de materie, onvoldoende draagvlak binnen de politie om deze bevoegdheid op de voorgestelde manier in te regelen, doorlooptijden van de aanvraag van middelen en techniek (inclusief heimelijke inkoop) en de tijdige keuring van de te gebruiken middelen.

Tot slot wordt er vaak gezegd dat de inrichting van deze voorziening een ICT traject is. ICT is een belangrijke component van het binnendringen, echter de menselijke component, zoals altijd bij politiewerk is van veel groter belang. Zonder goed gekwalificeerde (en uitgeruste) mensen is deze bevoegdheid niet uit te voeren. De operationele werkprocessen (opsporing) zijn bepalend.

Kort gezegd zijn dit de risico's voor dit programma. Door nu akkoord te gaan met deze hoofdlijnennotitie kunnen een groot aantal van deze risico's nu worden ondervangen:

- Eerste Kamer gaat niet akkoord gaat met het wetsvoorstel.
- Onderschatting van complexiteit van de materie
- Onvoldoende draagvlak binnen de politie om deze bevoegdheid centraal in te regelen
- Doorlooptijden van de aanvraag van middelen en techniek (inclusief heimelijke inkoop
- Tijdige keuring van de te gebruiken middelen
- Onvoldoende gekwalificeerd (en uitgerust) personeel
- Implementatie zien als een ICT-project

Er is door het programma CCIII een uitgebreide risico analyse opgesteld op de hoofdgebieden omgeving, organisatie, mens, management, juridisch, techniek en middelen. Deze analyse wordt als basis gebruikt voor de verdere programma aanpak, om zodoende zo veel als mogelijk aan de voorkant rekening te houden met mogelijke risico's.

6. Het wetsvoorstel CCIII

Het wetsvoorstel CCIII is na een lange doorlooptijd op 20 december 2016 door een ruime meerderheid in de Tweede Kamer met twee amendementen goedgekeurd. De lange voorbereidingstijd voordat de wet uiteindelijk is goedgekeurd, gecombineerd met het politieke klimaat, de grote afbreukrisico's als de politie dit onderwerp niet goed ter hand neemt en het vergrootglas waaronder de gehele politie organisatie op dit moment ligt, maakt dat dit onderwerp met de grootste zorgvuldigheid opgepakt moet worden. De politieke discussie spitst zich toe op het heimelijk binnendringen, echter de wet gaat ook over:

- de verbeterde strafbaarstelling van online handelsfraude en heling van gegevens (het wordt makkelijker om aangifte te doen en de bewijslast voor het slachtoffer wordt vereenvoudigd).
- de strafbaarstelling van grooming en corrumperen[2] , waardoor de inzet van bijvoorbeeld 7-12 mogelijk wordt. Met corrumperen wordt de strafbepaling van 248 Sr uitgebreid door het kind beter te beschermen tegen schadelijke invloeden op de persoonlijke en seksuele ontwikkeling.
- het ontoegankelijk maken van gegevens wordt mogelijk gemaakt langs de digitale weg 7-12 .

Heimelijk op afstand binnendringen

De uitoefening van deze bevoegdheid zal met zware waarborgen omkleed zijn. De belangrijkste hiervan zijn:

- Strafmaat (in principe) > 8 jaar of meer [3]
- Toetsing vooraf door OvJ/RC/CTC
- Keuringseisen software analoog aan de inzet van heimelijke middelen
- Meldingsplicht gebruikte onbekende kwetsbaarheden
- Onafhankelijk toezicht door de Inspectie I&V
- Expliciete functiescheiding technisch team en tactisch team
- Alleen inzet van gekwalificeerde aangewezen ambtenaren

Er zal voldoende transparantie in moeten worden gebouwd om de buitenwereld te overtuigen van de juiste inzet van deze bevoegdheid (voldoende logging en monitoring). Er zal sprake moeten zijn van een functiescheiding tussen techniek en tactiek omwille van de onafhankelijkheid[4]. Dit betekent dat de technische voorziening gescheiden van de tactische opsporing zal worden georganiseerd.

---

[2] Met het Landelijk Programma Zeden zijn afspraken gemaakt over de onderwerpen grooming en corrumperen. In 2017 zal er nog een impactanalyse worden opgesteld over de strafbaarstelling van heling van gegevens.

[3] Met betrekking tot de strafmaat is het volgende van belang voor wat betreft de onderzoekshandelingen:
a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
c. de ontoegankelijkmaking van gegevens;
d. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie (richtmicrofoon);
e. de uitvoering van een bevel tot stelselmatige observatie.
Voor de bevoegdheden, genoemd in de punten a., d. en e. geldt het vereiste van een feit waarvoor voorlopige hechtenis mogelijk is. Voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens (punten b en c) geldt het vereiste van een feit waarvoor gevangenisstraf van acht jaar of meer kan worden opgelegd of dat bij AMvB is aangewezen. Deze AMvB is nog in de maak.

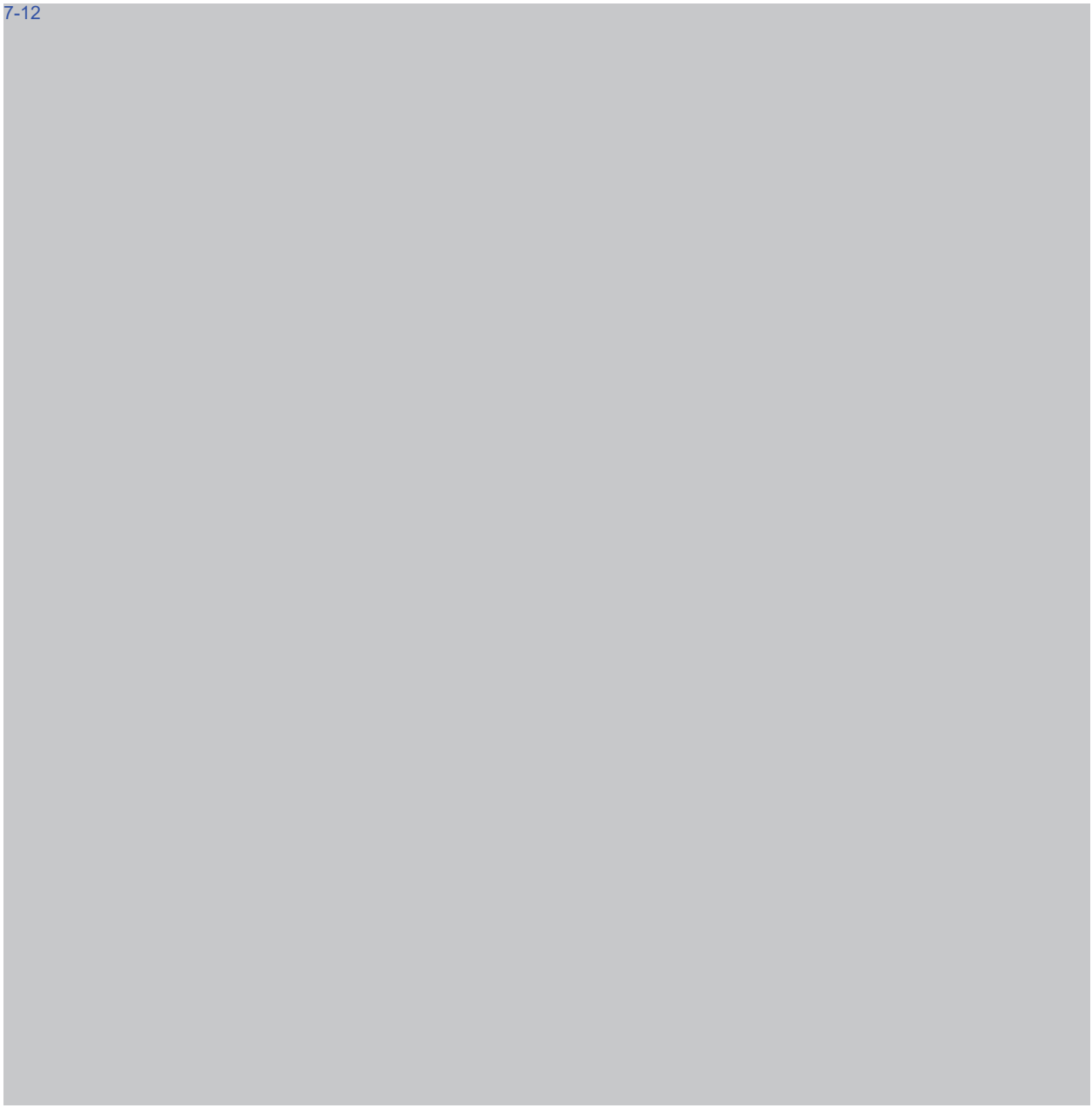
[4] De wettelijke regeling moet ook waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. In het voorgestelde artikel 126nba Sv zijn deze waarborgen nader uitgewerkt. De bevoegdheid kan slechts worden toegepast als sprake is van een verdenking van ernstige strafbare feiten die een ernstige inbreuk op de rechtsorde opleveren. Daarnaast moet sprake zijn van een dringend onderzoeksbelang. Voorts kan bij de inzet van de bevoegdheid slechts gebruik worden gemaakt van een technisch hulpmiddel dat voldoet aan bepaalde eisen, die zijn neergelegd in het Besluit

De eerste behandeling in de Eerste Kamer heeft op 7 maart 2017 plaatsgevonden. Het voorlopig verslag van de Eerste Kamer is op 3 april aan de Staatssecretaris van Veiligheid en Justitie verzonden. De verwachting is dat het wetsvoorstel uiterlijk 1 januari 2018 in werking zal treden. Daarnaast wordt er op dit moment door de Staatssecretaris van Veiligheid en Justitie, met medewerking van het programma CCIII, gewerkt aan het opstellen van een apart besluit “onderzoek in een geautomatiseerd werk”. In dit besluit wordt onder ander nader uitgewerkt aan welke eisen een technisch hulpmiddel moet voldoen, op welke wijze de keuring van dit technisch hulpmiddel moet plaatsvinden, wie toegang heeft tot een technisch hulpmiddel, wie mag plaatsen en wie mag inzetten. Hierop is door de Korpsleiding op 6 juli 2017 formeel gereageerd naar aanleiding van een consultatieverzoek door het Ministerie van Veiligheid en Justitie.

technische hulpmiddelen strafvordering. Met deze voorwaarden wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik alsmede voor het verzekeren van de authenticiteit en integriteit van door middel van het technische hulpmiddel vastgelegde gegevens. Daarbij is voorzien in functiescheiding tussen opsporingsambtenaren die betrokken zijn bij het onderzoek in een geautomatiseerd werk (het technische team) en de opsporingsambtenaren die betrokken zijn bij het operationele opsporingsonderzoek (het tactische team). Ook is voorzien in logging van de gegevens over de handelingen die in het kader van de inzet van het technische hulpmiddel worden verricht. (Memorie van Toelichting, Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3 pagina 54.)

Bijlage 1

Lab CIII
Behoefte lab CCIII tot 1 januari 2018:

1. **Coördinator/teamleider:**
   a. **Taken en verantwoordelijkheden**
      De coördinator/teamleider is in deze fase verantwoordelijk voor de coördinatie binnen de voorziening.
      Hij gaat over:
      - de inzet van mensen en middelen binnen het team.
      - de sturing op de kwaliteit van processen, mensen en middelen.
   b. **Functie eis**
      Het functieniveau is Teamchef-C.
   c. **Vraag**
      In verband met de groei van het lab CCIII is de behoefte aanwezig om hier een teamleider verantwoordelijk voor te maken.
2. 7-12
3. 

7-12

4.

5.

7-12

CCIII inzetteam 7-12

Behoefte CCIII inzetteam vanaf 1 januari 2018

1. **Leider Operaties**
   a. **Taken en verantwoordelijkheden**

      De Leider Operaties is verantwoordelijk voor het uitvoeren van haalbaarheidsonderzoek, de voorbereiding en de uitvoering van de inzet. Hierbij heeft de LO een duidelijke coördinerende verantwoordelijkheid. De LO draait meerdere zaken tegelijkertijd. De eindverantwoordelijkheid van de inzet ligt bij de teamleider.

   b. **Functie eisen**

      De LO is operationeel ingesteld en zal zeer bekend moeten zijn met het werk van de binnentreder en uitvoerder uit eigen ervaring. Het functieniveau is minimaal OS-C.

   c. **Opmerkingen**

      Deze rol kan separaat worden ingevuld, maar kan binnen het CCIII team ook door de Teamleider worden uitgevoerd, onder de voorwaarde dat de teamleider beschikt over de functie eisen; met name met betrekking tot de ervaring.
2. 7-12
3.

7-12

4.

5.

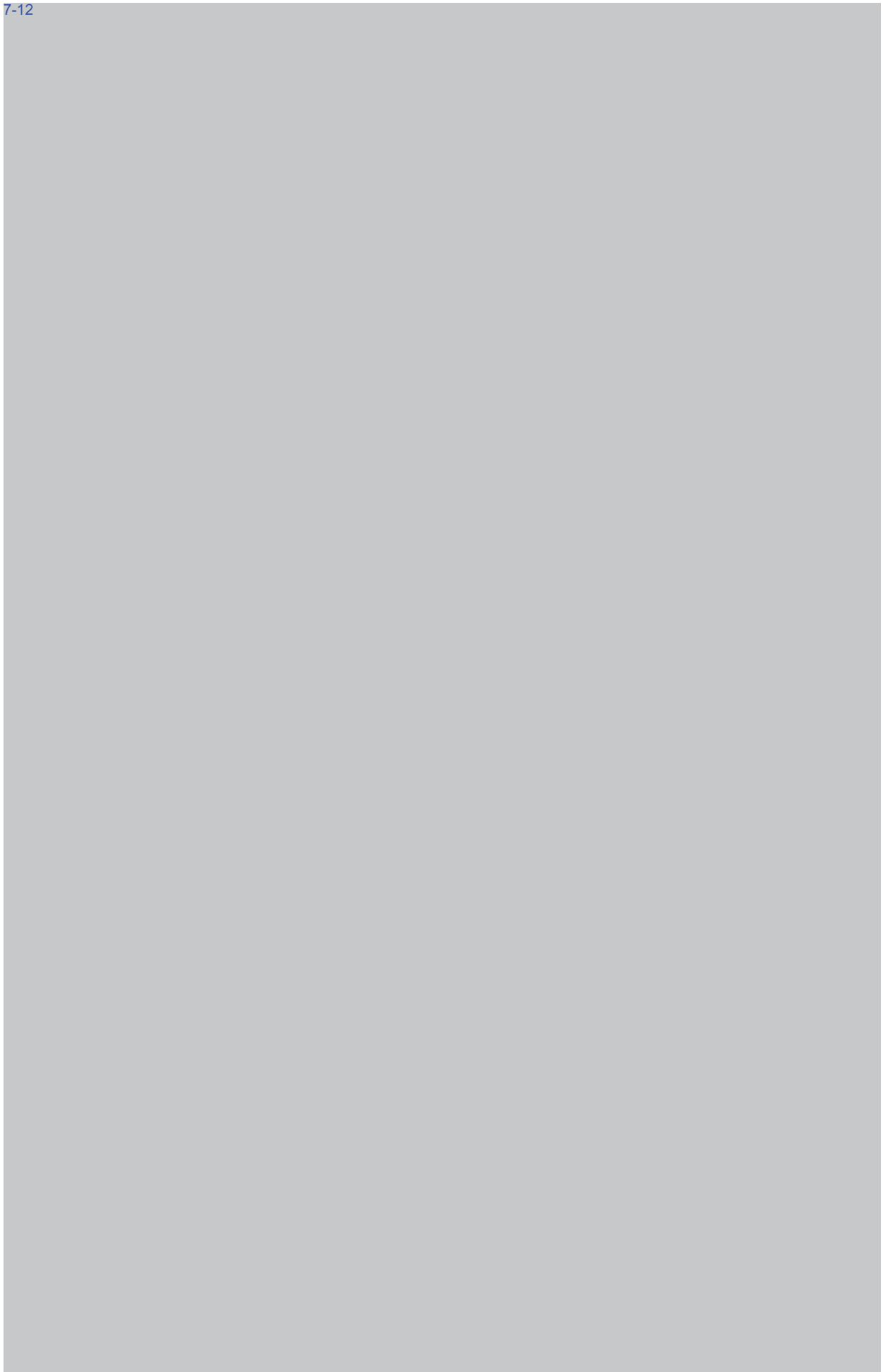
6.

7-12

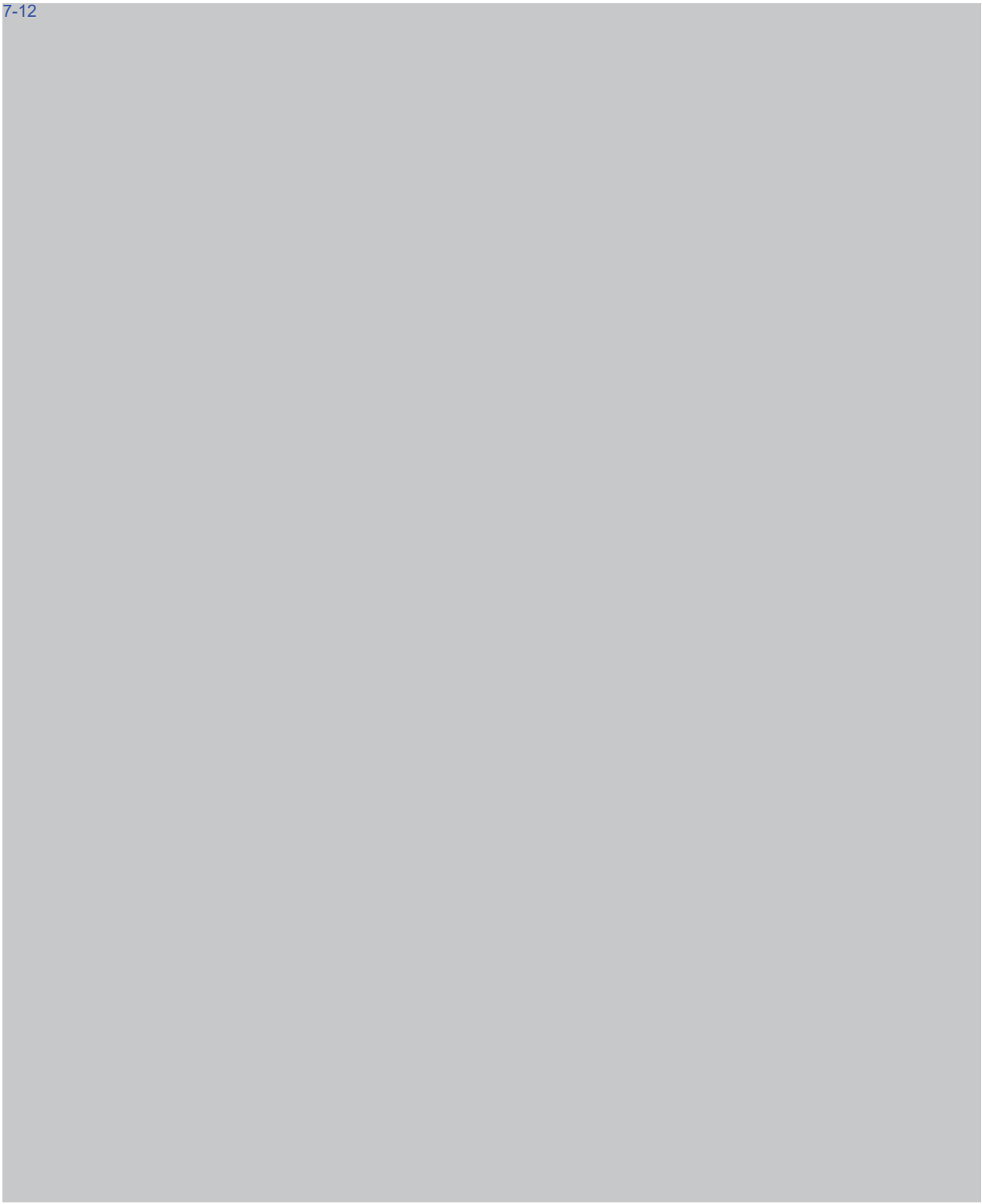
7.

8.

9.



7-12



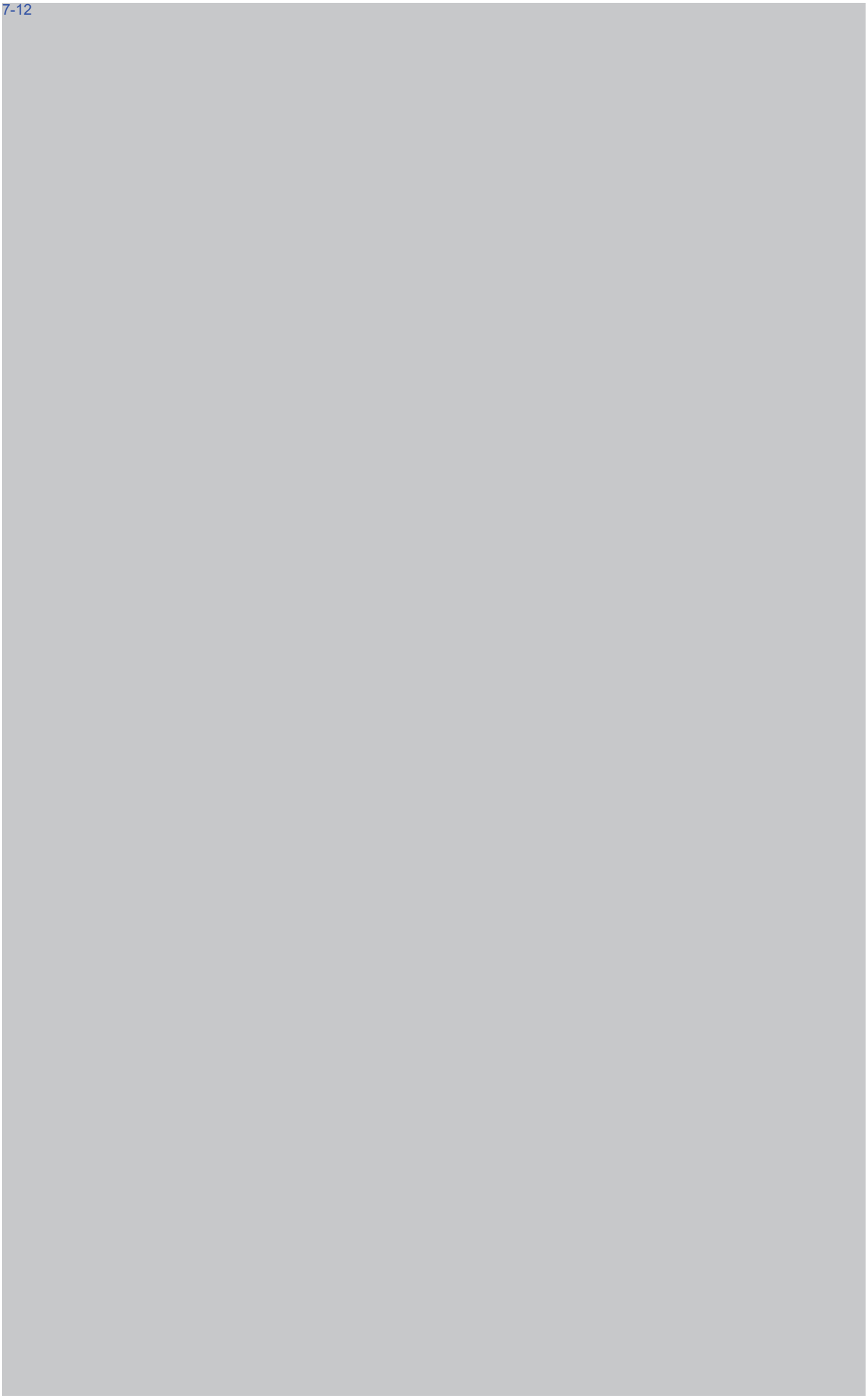
Coördinatie en Ondersteuning CCIII team 7-12

Om het CCIII inzetteam te laten functioneren zijn de volgende ondersteunende rollen/functies nodig binnen de voorziening:

1. **Teamleider:**
    a. **Taken en verantwoordelijkheden**
    De teamleider is het afdelingshoofd van de voorziening. Verantwoordelijk voor de PIOFACH-taken van de voorziening.
    b. **Functie eis**
    Het functieniveau is Teamchef C.

7-12

2.

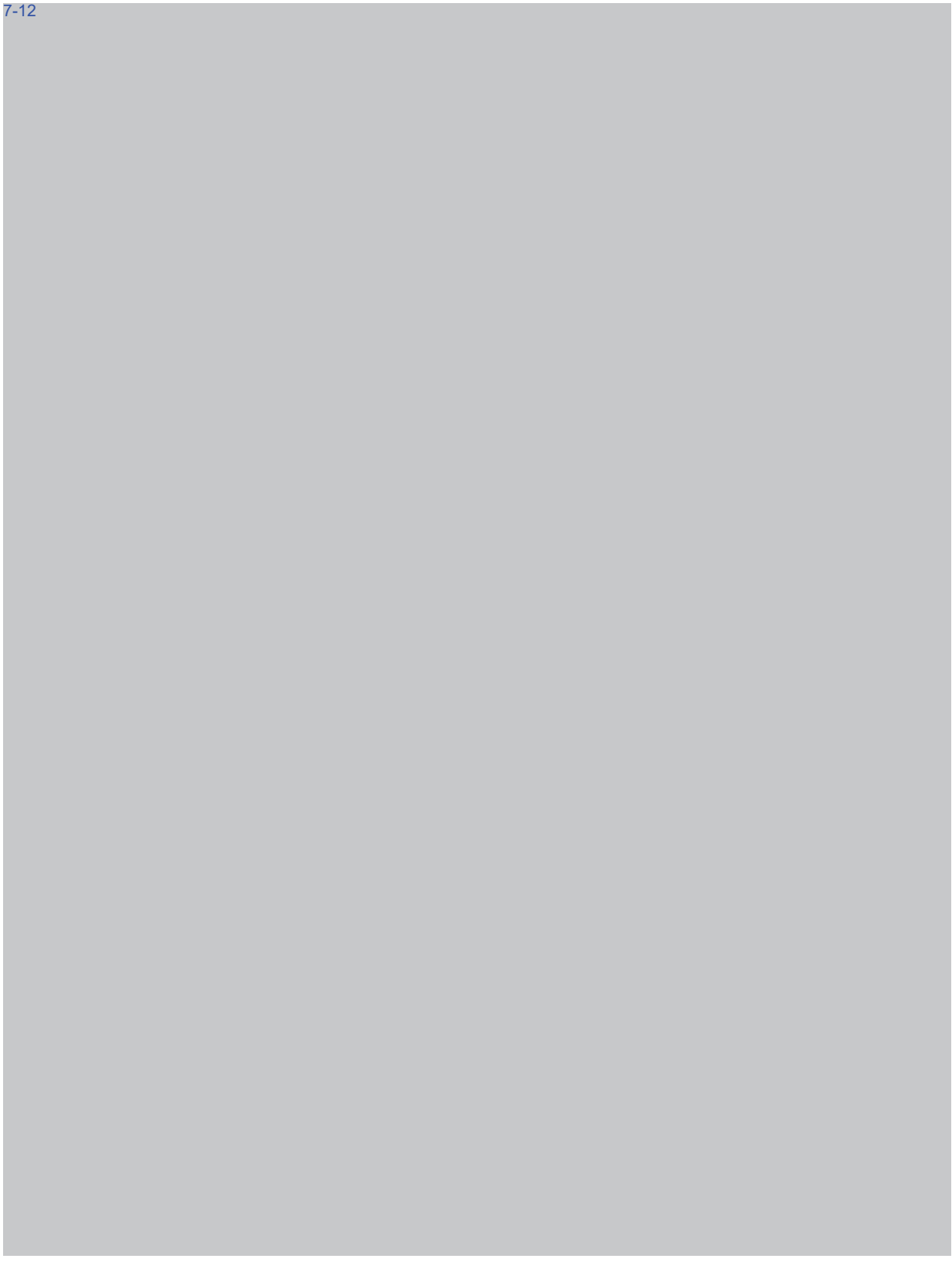


3.

7-12

4.

5.



Bijlage 2

Voor de uitbreiding van de Keuringsdienst bestaat de behoefte aan onderstaande functie.

1. **Test engineer:**
    a. **Taken en verantwoordelijkheden**

    verantwoordelijk voor het keuren van de technische hulpmiddelen van de voorziening.

    b. **Functie eisen**

    - Moet in staat zijn om testen te automatiseren
    - Moet in staat zijn om regressietesting uit te kunnen voeren.
    - Kennis van de wetgeving rondom het binnendringen is gewenst.
    - Het functieniveau is OS-C/D.

    c. **Vraag**

    Om de keuring van de technische hulpmiddelen uit te kunnen voeren is uitbreiding van de Keuringsdienst met 7-12 noodzakelijk.

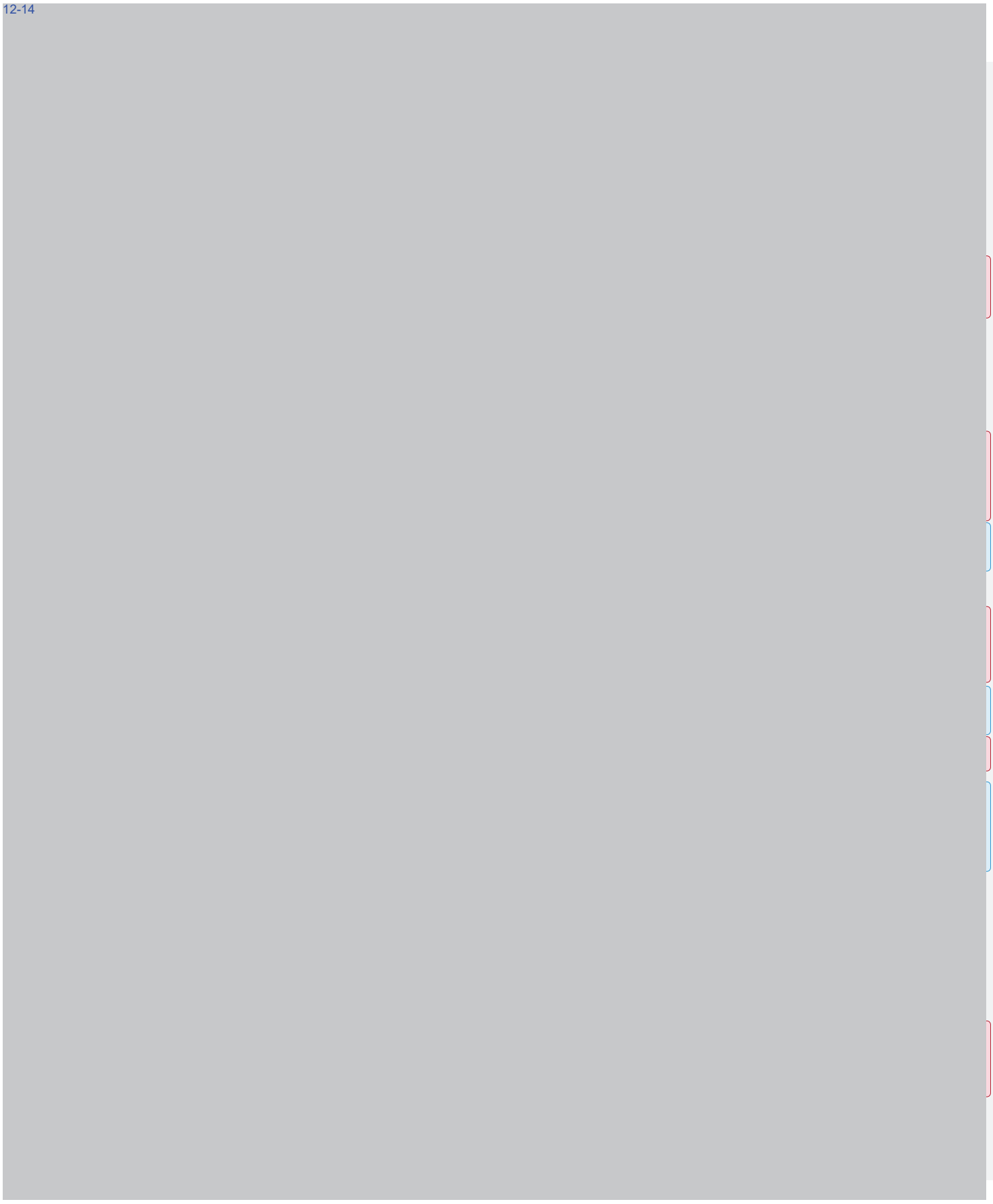
Bijlage 3

Het tijdschema voor de implantatie ziet er als volgt uit:

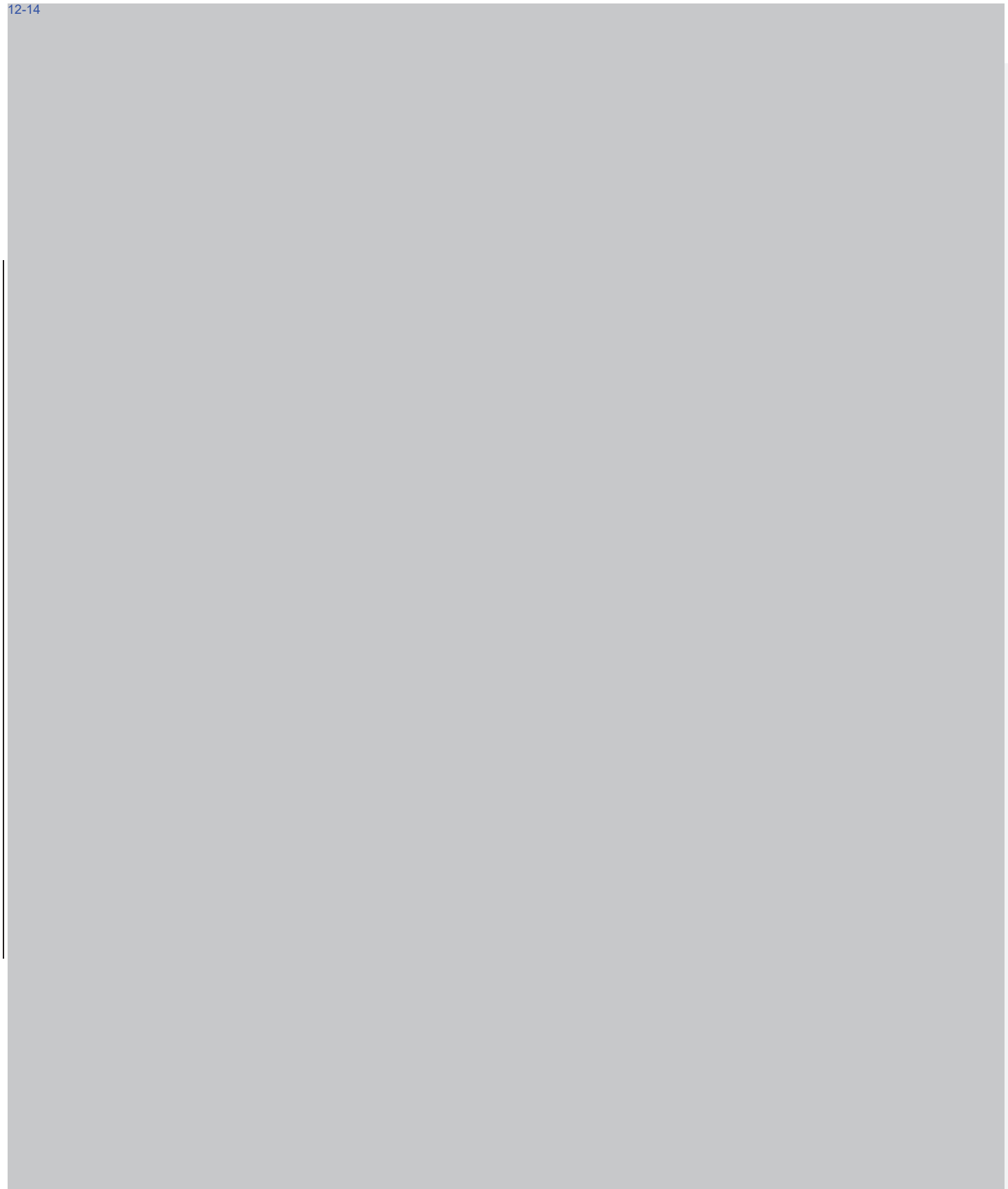
Inrichting voorziening CCIII:
1 april 2017: Risicoanalyse en outline realisatieplan gereed.
1 september 2017: Voorlopige realisatieplan gereed.
1 januari 2018: Start inrichting voorlopige voorziening CCIII.
1 september 2018: Definitief realisatieplan gereed.
1 januari 2019: Start definitieve voorziening CCIII.

Wetgevingstraject:
Besluit onderzoek in geautomatiseerd werk
april 2017: Start formele consultatieronde (incl. toezending TK/EK).
juli 2017: Formele consultatieronde afgerond.
juli 2017: Ministerraad.
juli – september 2017: Notificatie Europese Commissie (standstill periode).
juli – september 2017: Adviesaanvraag Afdeling advisering Raad van State.
september 2017: Advies Afdeling Advisering.
oktober 2017: Nader rapport.
1 januari 2018: Inwerkingtreding

Wet CCIII
7 maart 2017: eerste bespreking in Eerste Kamer.
3 april 2017: Inbreng voorlopig verslag Eerste Kamer.
15 mei 2017: reactie Staatssecretaris Veiligheid en Justitie op inbreng Eerste Kamer.
20 juni 2017: Hoorzitting Eerste Kamer
september 2017: Plenair debat Eerste Kamer (incl. stemming)
1 januari 2018: Inwerkingtreding

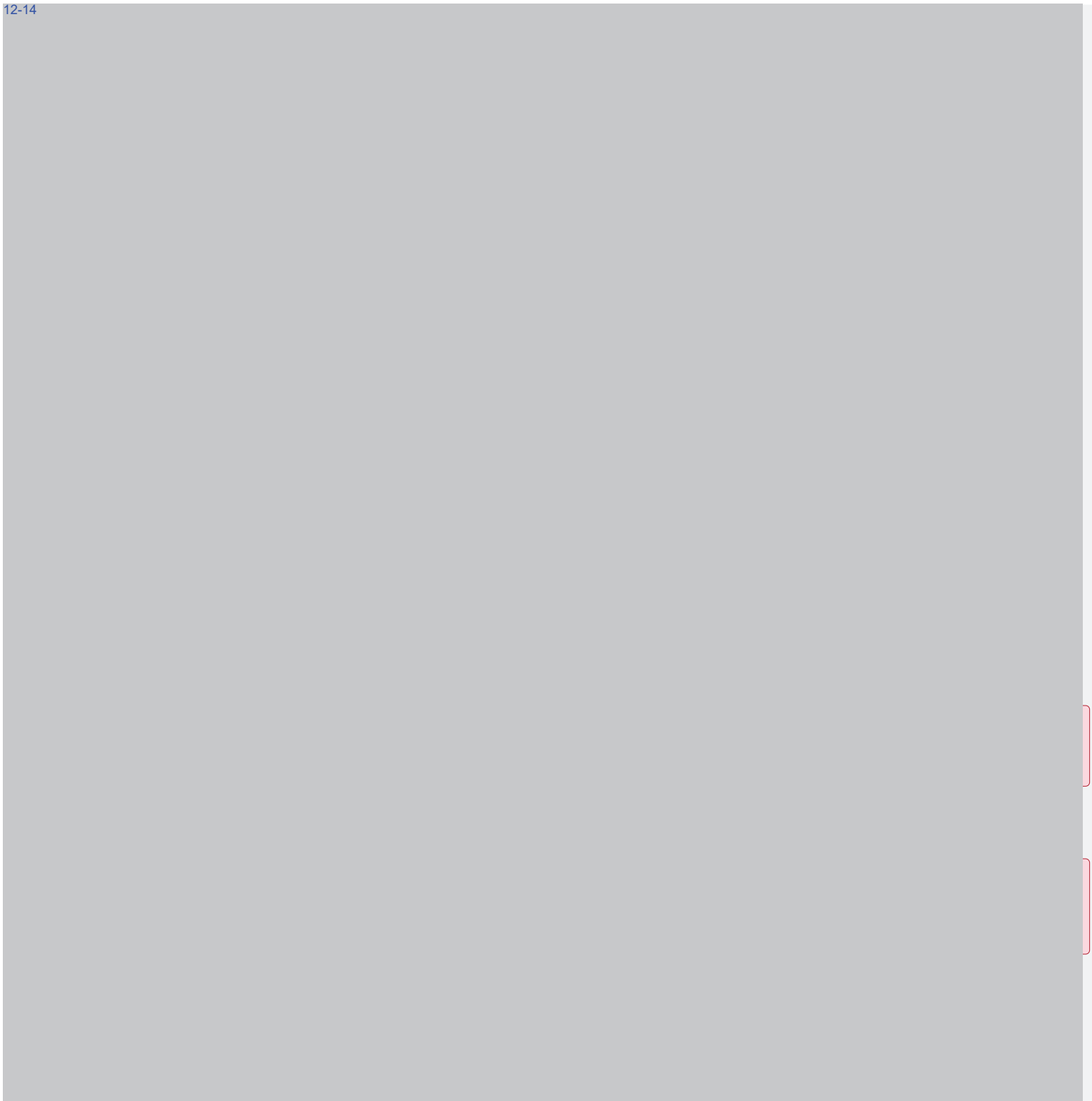

12-14

12-14



Nationale politie.

12-14


12-14

12-14

12-14

Van: 10.2.e
Verzonden: woensdag 3 februari 2016 9:39
Aan: Plas, Theo van der (T.G.); 10.2.e
CC: 10.2.e
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2

Beste 10.2.e ea, Ik heb de notitie gelezen en met 10.2.e besproken in diverse versies. Goed werk. Ik vind 12-14

12-14

?

Ik bereid alvast een opzetje voor voor de twee minuten spreektijd. In ieder geval korte intro aard vd wet (aanpassing Sv en Sr.), irt online handelsfraude en heling benadrukken noodzaak brede ontwikkeling politie, en vervolgens uitleggen wat 'het precisie instrument ' inhoudt en hoe het proces (mn de controle) er ongeveer uit zou kunnen zien.

Groet,10.2.e

-----Original Message-----
From: 10.2.e
Sent: Wednesday, February 03, 2016 10:52 AM W. Europe Standard Time
To: ; ; Plas, Theo van der (T.G.);

Cc: 10.2.e
Subject: RE: Gespreksnotitie CIE VenJ concept 0.2

Hallo 10.2. ,

Ter informatie: 12-14
Wordt vervolgd.

Ik neem aan dat jij de afstemming ook van belang vind. Misschien is het goed als jij bv. 10.2.e dan ook zelf eens benaderd om te kijken hoe hij hierin zit?

Als aanvulling op te verwachten vragen:
- In welke zaken heeft de politie deze bevoegdheid eerder al toegepast en op basis van welke bevoegdheid? (laatste zou overigens vooral aan OM zijn) (SP-Gesthuizen)
- Het kabinet heeft recent een kabinetsstandpunt encryptie naar de Kamer gestuurd. De vaste Kamercommissie was daar heel blij mee, maar heeft al aangekondigd vragen stellen over hoe dat standpunt zich dan verhoudt tot het wetsvoorstel. (SP-Gesthuizen)
- Vragen over toezicht op de uitvoering van de bevoegdheid door politiemensen (na toestemming RC), binnendringen in computers in het buitenland en de inzet van bestaande middelen (zoals samenwerking en informatie-uitwisseling|) (D66, Verhoeven, zie ook link https://d66.nl/17812-2/)

Als ik kan helpen met meelezen in teksten, laat het dan weten.

Groet,

10.2.e

Van: 10.2.e
Verzonden: woensdag 3 februari 2016 11:06
Aan: 10.2.e
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2

Heb je dat crypto standpoint voor mij?

Van: 10.2.e
Verzonden: woensdag 3 februari 2016 13:01
Aan: 10.2.e @politie.nl>; Plas, Theo van der (T.G.) @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @klpd.politie.nl>
CC: 10.2.e @rijnmond.politie.nl>
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.7)

Beste 10.2.e ea,

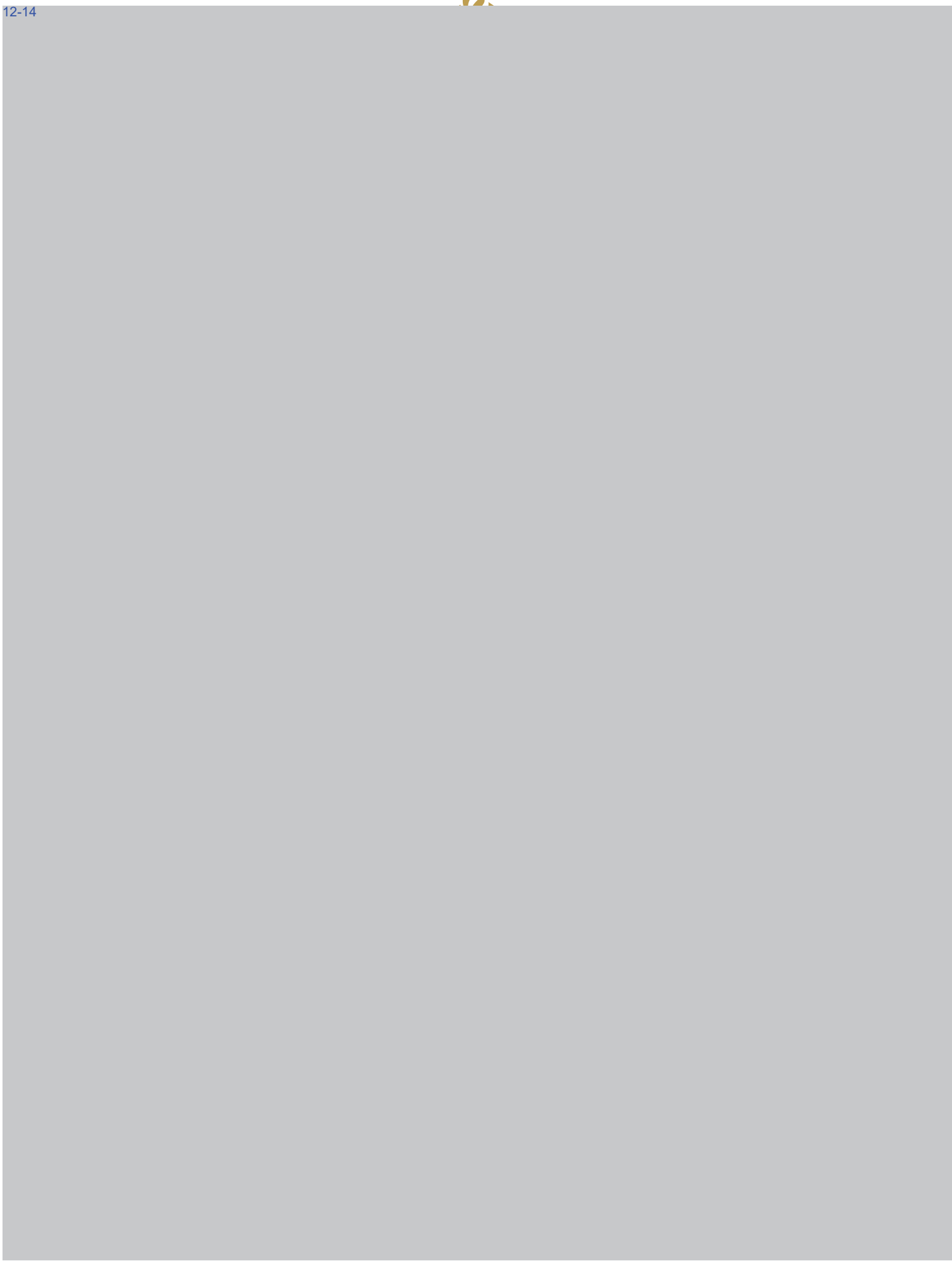
bijgaand een laatste versie van de gespreksnotitie. Hierin zijn opmerkingen verwerkt van 10.2.e 10.2.e , 10.2.e , 10.2.e , Bestuurszaken en mijzelf.

Ik hoor graag wat jullie er van vinden.

Met vriendelijke groet,

10.2.e

12-14



12-14

Van: 10.2.e . - BD/DWJZ/SSR
Verzonden: woensdag 3 februari 2016 17:45
Aan: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
Onderwerp: Rondetafel CC III

Dag 10. , 10.2.e en 10.2.e ,

Over dat rondetafel gesprek over CC III van volgende week donderdag nog even het volgende:
Ik begrijp van BSG dat de deelnemers is gevraagd om vooraf een schriftelijke opgave van de inbreng aan te leveren. Volgens BSG leert de ervaring dat hoe eerder die inbreng wordt aangeleverd, hoe meer kans dat de Kamerleden daar tijdens de rondetafel op in gaan. Het lijkt mij wel goed om dat nog even te communiceren met de deelnemers van politie, OM en NCSC.

Verder vraag ik mij af of niet enige voorlichting wenselijk is m.b.t. inhoud wetsvoorstel, specifiek t.a.v. de vertegenwoordigers van de politie.

Graag hierover nog even contact, ik heb morgenmiddag vanaf half vier nog ruimte voor overleg.

Gr.10.2.

Van: 10.2.e
Verzonden: woensdag 3 februari 2016 22:44
Aan: 10.2.e 10.2.e 10.2.e 10.2.e 10.2.e 10.2.e
CC: 10.2.e
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.7)

Beste collega's,

Ik had al naar 10.2.e gereageerd, maar handig om jullie mee te nemen gezien de tijd die we nog hebben om het stuk definitief af te maken….

Bij deze:
Fijn dat in deze versie de dubbelingen eruit zijn. Dat leest veel beter.
Ik vind echter de manier waarop nu de relatie wordt gemaakt met de contourennota en de bredere maatregelen niet helemaal gelukkig. Het gaat om de een na laatste paragraaf en de paragraaf daarvoor. Zie mijn opmerkingen daarover in de bijlage. Moeten we die wel opnemen?

Ik snap dat er de behoefte is breder de aandacht te vestigen op het belang van goede voorzieningen en goed personeel, maar dit is echt een hoorzitting puur gericht op dit wetsvoorstel en daar moet denk ik vooral de nadruk op liggen. Diverse partijen zullen ons volop gaan 'aanvallen'. Dit document is onze kans alvast onze verdediging neer te zetten.

Groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 4 februari 2016 9:48
Aan: 10.2.e 10.2.e .); Plas, Theo van der (T.G.); 10.2.e 10.2.e
CC: 10.2.e 10.2.e
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.7)

Hoi allemaal,

ik vind het op zich geen probleem om de stukken over de contourennota en de bredere maatregelen eruit te halen, maar als we dat doen missen we misschien toch een kans om ook in dit debat mee te geven dat het niet slechts om dit wetsvoorstel gaat, maar dat we als politie in het licht van de contourennota en de wetswijziging verder doorontwikkelen op het digitaliserings domein. Kan nooit waad om, de dag nadat de contourennota in de Kamer wordt behandeld nogmaals te benadrukken... maar meerderheid beslist!

Ik hoor het graag nog even. Mochten we het laten staan dan is denk de versie zoals die bijgevoegd (ik heb een paar kleine aanpassingen gemaakt) is dit de versie die naar de Kamer zal gaan? Zo niet, dan pas ik het nog even aan.

Ik hoor graag van jullie.

Met groet,

10.2.e

Van: 10.2.e BD/DRC/CV
Verzonden: donderdag 4 februari 2016 10:31
Aan: 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: FW: Rondetafel CC III

Ook hier graag meedenken

From: 10.2.e BD/DGPOL/PBT/PT
Sent: donderdag 4 februari 2016 10:46:35
To: 10.2.e @politie.nl)
Subject: FW: Rondetafel CC III

Hoi 10.2.e is politie om een schriftelijke inbreng voor de ronde tafel gevraagd? Zo ja, dan is het goed als mn dgrr denk ik, even meeleest. Ook is gevraagd of politie met dgrr en dw wil voorbespreken. Kan geen kwaad denk ik. Hoe zie jij dit?

Met vriendelijke groet,

10.2.e
9 beleidsmedewerker
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma Politiële Taken
Turfmarkt 147 | 2511 DP | Den Haag | Noord 24e etage
Postbus 20301 | 2500 EH | Den Haag

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: donderdag 4 februari 2016 12:45
Aan: 10.2.e 10.2.e
Onderwerp: RE: Rondetafel CC III

Ook voor jou 10.2.e

From: 10.2.e (PaG 's-Gravenhage) 10.2.e @om.nl]
Sent: Thursday, February 04, 2016 01:51 PM W. Europe Standard Time
To: 10.2.e
Cc: 10.2.e Landelijk Parket Rotterdam) 10.2.e @om.nl>
Subject: Proces voorbereiding rondetafelgesprek CCIII

Hoi 10.2.e

Zoals zojuist telefonisch besproken stuur ik je hierbij een voorstel toe voor de gezamenlijke voorbereiding van het rondetafelgesprek over CCIII. 10.2.e zou a.s. maandag (liefst 's ochtends), dinsdagmiddag (vanaf 15.00 uur) of woensdag kunnen afspreken. Dinsdag moet hij al bij het THTC in Driebergen zijn, dus misschien is dat wel het handigste moment om af te spreken. Voorstel is om Inge Philips, 10.2.e en/of 10.2.e aan te laten sluiten bij het overleg.
10.2.e en Inge moeten natuurlijk zorgen dat ze op één lijn zitten en ook de spreekteksten moeten op elkaar afgestemd zijn. Met 10.2.e zou 10.2.e nog van gedachten willen wisselen over een aantal technische aspecten. De concept Q&A's zouden tijdens dit gesprek ook besproken kunnen worden. We hebben waarschijnlijk Q&A's nodig over 'achterdeurtjes', het gebruik en de ontwikkeling van malware, ('ingebouwde') zwakheden in systemen, over de verhouding wetsvoorstel/standpunt encryptie en de kans dat we in computers van onschuldige slachtoffers binnendringen. Fijn om te horen dat jullie al begonnen zijn met de uitwerking van Q&A's. Het lijkt me goed dat jij, 10.2.e en ik meelezen.
Zouden wij jullie zienswijze mogen ontvangen als het stuk gereed is?
En wil jij nagaan wanneer Inge in de gelegenheid is om te overleggen? Ik hoor graag van je. Alvast bedankt.

Vriendelijke groet,

10.2.e
Parket-Generaal OM
9

From: 10.2.e
Sent: Thursday, February 04, 2016 02:06 PM W. Europe Standard Time
To: 10.2.e
Subject: Ronde tafel versie 0 91

zoiets?

From: 10.2.e
Sent: donderdag 4 februari 2016 14:22:40
To: 10.2.e 10.2.e - BD/DGPOL/PBT/PT
Subject: FW: Ronde tafel versie 0 91

Hoi,

Lezen jullie nog even mee?

Groete

10.2.

Van: 10.2.e
Verzonden: donderdag 4 februari 2016 14:52
Aan: 10.2.e 10.2.e); Plas, Theo van der (T.G.); 10.2.e
10.2.e
CC: 10.2.e
Onderwerp: RE: Gespreksnotitie CIE VenJ concept 0.2 (nu 0.91)
Bijlagen: Ronde tafel versie 0 91.docx

Beste allemaal,

bijgaand de allerlaatste versie. Volgens 10.2.e en mij is deze nu verzendklaar.
Mochten jullie het hier niet mee eens zijn, dan hoor ik dat graag. Bestuurszaken zal voor verzending zorgen.

Met groet,

10.2.e

Dubbel zie doc 313

Van: 10.2.e BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: donderdag 4 februari 2016 14:56
Aan: 10.2.e 10.2.e
Onderwerp: RE: Ronde tafel versie 0 91

12-14

Snap je wat ik bedoel?

Van: 10.2.e
Verzonden: donderdag 4 februari 2016 15:03
Aan: 10.2.e 10.2.e
CC: 10.2.e
Onderwerp: Fw: Proces voorbereiding rondetafelgesprek CCIII

Hoi 10.2.e en 10.2.e

PaG en LP zijn voorbereiding gestart en willen ook graag afstemmen. Zie hierbij een voorstel.

Kunnen jullie je daarin vinden en dan zelf zorgen voor een afspraak met 10.2.e Wat mij betreft ben ik daar niet bij, maar 10.2.e Tenzij zij niet kan en het handig is dat ik dan aansluit.

Met vriendelijke groet,

10.2.e
Staf Korpsleiding Politie
Directie Operatien
Verzonden vanaf mijn Blackberry

From 10.2.e @politie.nl>
Subject **FW: Proces voorbereiding rondetafelgesprek CCIII**
To 10.2.e @om.nl>, 10.2.e @om.nl>
Date 4 februari 2016 15:49:15 CET

Beste 10.2.e

naar aanleiding van onderstaande mail van 10.2.e en 10.2.e hierbij het voorstel om aanstaande dinsdag om 16.00 uur bij elkaar te gaan zitten. Wij (10.2.e (projectleider CCIII) en ik) hebben net een afspraak met 10.2.e gepland in de koffiecorner in Driebergen. Zou mooi zijn als je daarbij kunt aansluiten.

Ik heb 10.2.e en 10.2.e in de cc gezet. Ik hoop dat zij aan kunnen sluiten. Ik wil wel proberen om zo veel mogelijk weg te blijven bij de technische details tijdens het rondetafelgesprek, maar als achtergrondinfo kan die informatie natuurlijk geen kwaad. Ik weet dat Inge al bezig is met haar spreektekst.

Ik hoor graag of je aansluit aanstaande dinsdag.

Met groet,
10.2.e

10.2.e
9

Politie | Project CCIII
Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl
Werkdagen: maandag, dinsdag, donderdag en vrijdag

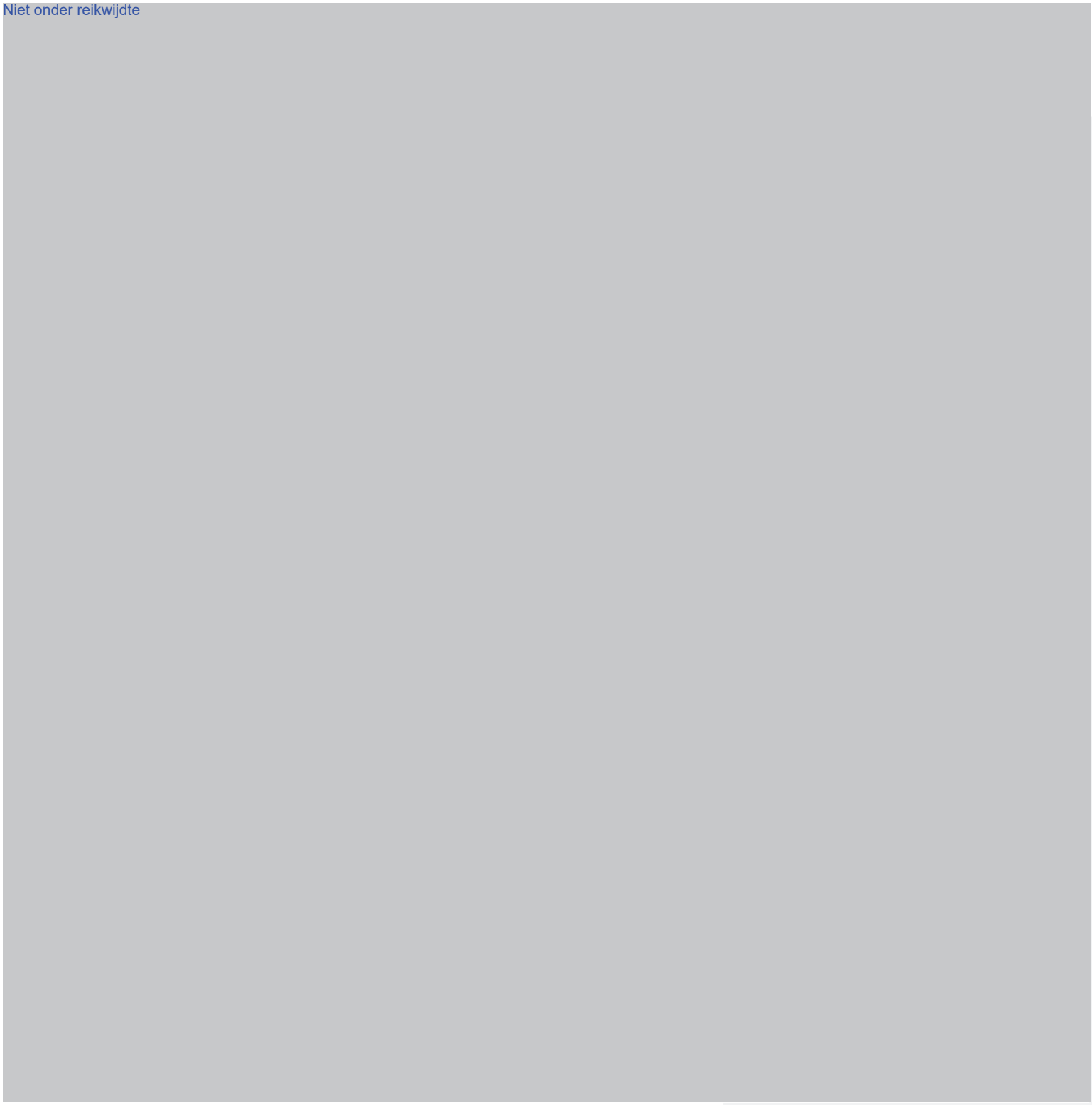
Van: 10.2.e) namens 10.2.e
Verzonden: donderdag 4 februari 2016 16:50
Aan: 10.2.e
CC: 10.2.e ; 10.2.e
Onderwerp: RE: Ronde tafel computercriminaliteit III

Hoi collega's,

We hebben vandaag aan de griffie telefonisch bevestigd dat Inge Philips idd de persoon is die namens de politie deelneemt aan de hoorzitting. Mogen wij ervan uit gaan dat verdere toestemming van de minister voor ambtelijke deelname van jullie rekening komt? Jullie krijgen morgen ter informatie de gespreksnotitie die voor de hoorzitting wordt gebruikt.

Groet,

10.2.e


Niet onder reikwijdte

Van: 10.2.e
Verzonden: vrijdag 5 februari 2016 11:51
Aan: 10.2.e 10.2.e
CC: 10.2.e ; 10.2.e)
Onderwerp: voorbereiding hoorzitting CIII
Bijlagen: Uitnodiging mevr. I. Philips.doc; Profiel Kamerleden.docx

Hoi 10.2.e , 10.2.e ,

Ter voorbereiding op de hoorzitting computercriminaliteit III het volgende:

1. Bijgaand vind je een profiel van alle Kamerleden (waarvan wij denken dat ze deelnemen aan de hoorzitting), inclusief links naar vragen die ze hebben gesteld over computercriminaliteit III of hieraan gerelateerde thema's.
2. Deelnemers van de organisaties hadden tot gisteren de tijd om aan te geven of ze op de uitnodiging van de commissie in gaan. Vandaag of begin deze week wordt de definitieve deelnemerslijst bekend. Deze wordt zsm doorgestuurd. De naam van Inge Philips is telefonisch bevestigd, we wachten nog op het officiële verzoek van toestemming van de minister (normale route bij ambtelijke deelname). DGPol Parlementair heeft alvast aangegeven dat dit uiteraard wordt geaccordeerd.
3. Voor de spreektijd moet je ongeveer uit gaan van een introductie van ca. 3-5 minuten. Daarna zullen Kamerleden vragen gaan stellen aan de individuele deelnemers. De bedoeling is dat uiteindelijk een dialoog ontstaat tussen Kamerleden en deelnemers.
4. De gespreksnotitie moet ik uiterlijk vanochtend versturen (ik werk vandaag tot 12.00 uur, als het later wordt, graag even een sms sturen zodat ik thuis inlog). Deze stuur ik louter ter informatie ook aan onze collega's van DGPol Parlementair.
5. De uitnodiging vind je nogmaals in de bijlage voor de praktische zaken (tijdstip, ingang, enzo).

Hartelijke groet,

10.2.e
Senior adviseur

Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken

Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag
M 10.2.e | 10.2.e @politie.nl

Werkdagen: maandag t/m vrijdagochtend

Tweede Kamer
DER STATEN-GENERAAL

Den Haag, 27 januari 2016

Is gelijk aan doc 273

Profiel

Parlement & Bestuur

Vaste Kamercommissie VenJ ● Profiel Kamerleden ● Hoorzitting Computercriminaliteit III

Foort van Oosten (VVD)

Nederland staat voor een forse uitdaging. Dan doel ik natuurlijk op de financiële toestand van ons land. Het valt bovendien niet mee om de economie draaiende te houden. Als Kamerlid wil ik graag een bijdrage leveren aan een gezonde economische situatie.

Achtergrond:
2001-2006: Advocaat AKD Prinsen Van Wijnen
2006-2011: Departementsadvocaat BZ
2006-2011: Lid en vz rekenkamer Leiderdorp
2007-2011: Gemeenteraadslid Schiedam
2011-2012: Wethouder Schiedam

Parlementair:
Schriftelijke vragen over:
- ***sexting***

Jeroen Recourt (PvdA)

Veel mensen denken dat de Nederlandse rechters te laag straffen. Dat klopt niet. Rechters zijn de laatste jaren juist zwaarder gaan straffen voor misdrijven als ernstige geweldpleging, doodslag en moord. We moeten vooral de pakkans verhogen en zorgen dat straffen effectief zijn. De politie moet op straat werken aan een veilige en leefbare buurt en moet minder achter het bureau zitten.

Achtergrond:
1993-1999: Reclasseringsmedewerker Dordrecht
2004-2006: Rechter Arrondissementsrechtbank Amsterdam
2006- 2010: Rechter Gemeenschappelijk Hof van de Nederlandse Antillen en Aruba

Parlementair:
Schriftelijke vragen over:
- ***over het strafbaar stellen van "wraakporno" (van partijgenoot Rebel-Volp)***

- ***over doorverkoop van toegangsbewijzen voor concerten (van partijgenoten Monasch en Van Dekken, gerelateerd aan internetoplichting)***
- ***over het bericht dat cybercrime Nederland jaarlijks 8,8 miljard euro kost***
- ***over het bericht "Via virtueel Filipijns meisje 1000 kindermisbruikers getraceerd"***

Eventueel kan partijgenoot Astrid Oosenbrug deze hoorzitting overnemen. Zij heeft bij een aantal organisaties en bedrijven als systeembeheerder gewerkt, en bekleedde deze functie bij de Forta Groep. Zij is woordvoerster ICT, overheidsdienstverlening, privacy, telecommunicatie en auteursrecht.

Madeleine van Toorenburg (CDA)

Gedurende ruim 20 jaar heb ik, na mijn rechtenstudie, (onder meer) werkervaring opgedaan. In die periode heb ik goed zicht gekregen op de praktijk. Juist nu wij streven naar een kleinere overheid is dat belangrijk omdat je, om effectief ruimte te kunnen geven, wel moet weten waar het knelt.

Achtergrond:
1998-1999: advocaat-stagaire
1999-2001: lid directie Penitentiaire Inrichting voor vrouwen "Ter Peel".
2000-2001: lid directie Penitentiaire Inrichting Dubrava (Kosovo)
2001-2007: locatiedirecteur jeugdinrichting "De Leij" te Vught

Parlementair:
Schriftelijke vragen over:

- ***de berichten dat online met aanschaf van bitcoins een semi-automatisch wapen is aangeschaft en een tiener zichzelf gedood heeft met een omgebouwd pistool (van partijgenoten Oskam en Van Hijum)***

Kees Verhoeven (D66)

Ik wil bereiken dat ondernemers de ruimte krijgen om hun bedrijf en de Nederlandse economie weer te laten groeien. Dat starters weer een kans krijgen op de huizenmarkt. En dat Nederland de mogelijkheden van ICT en internet veel beter dan nu benut.

Achtergrond:

2001-2002 Leraar 'Centro Educativo de Antigua' en 'Nino Obrero' te Antigua (Guatemala),
2002-2004 Beleidsadviseur, Kamer van Koophandel voor Amsterdam
2004-2006 Secretaris Nationale Winkelraad, MKB Nederland
2006-2010 Directeur MKB-Nederland, regio Amsterdam

Parlementair:
Schriftelijke vragen over:

- ***de indiening van het wetsvoorstel computercriminaliteit III bij de Tweede Kamer***
- ***over het hacken van servers door de politie terwijl de zogenaamde 'hackwet' nog niet door de Kamer is behandeld***
- ***het aanspreken van hostingproviders door de politie op cybercrime (door partijgenoot Verhoeven)***
- ***het bericht dat hackers 1,2 miljard inloggegevens en 500 miljoen e-mailadressen hebben gestolen***

Lilian Helder (PVV)

Ik wil in de Kamer bereiken wat de mensen op straat graag willen. Ik ben voorstander van het invoeren van minimumstraffen en het beperken van de beslissingsruimte van de rechterlijke macht.

Achtergrond:
Diverse aanstellingen in de advocatuur

Parlementair:

Michiel van Nispen (SP)

Als Kamerlid wil ik niet alleen op de hoogte zijn van alle brieven die het ministerie naar de Kamer stuurt, maar wil ik ook de werkelijkheid daarachter kennen. Mijn ervaring als beleidsmedewerker is dat de informatiestroom van de ministeries gekleurd is en verpakt in beleidstaal.

Achtergrond:
2004 -2007: Medewerker op advocatenkantoren
2007-2014: Beleidsmedewerker justitie SP Tweede Kamerfractie

Parlementair:
Schriftelijke vragen over:

- ***over het gebruik van omstreden spionagesoftware door de politie (door collega Gesthuizen)***
- ***over het voorgestelde decryptiebevel en het terughackvoorstel (van collega Gesthuizen)***

Eventueel kan partijgenoot Sharon Gesthuizen deze hoorzitting overnemen. Zij was eigenaar van een productiebedrijf voor foto, video en internet, fractiemedewerkster van de SP in de Tweede Kamer en gemeenteraadslid in Haarlem. Mevrouw Gesthuizen houdt

zich met name bezig met economische zaken, asiel- en immigratiebeleid en justitie.

Gert-Jan Segers (CU)

Door mijn werkverleden in Egypte heb ik bijzondere belangstelling voor de verhouding tussen het Midden-Oosten en het Westen en voor de integratie van islamitische nieuwkomers. Het debat daarover moet niet polariseren om het polariseren, maar wel ergens toe leiden.

Achtergrond:
1994-1997: Beleidsmedewerker RPF Tweede Kamerfractie
1999-2000: Journalist De Ochtenden (EO Radio 1)
2000-2007: Coördinator van een christelijk studie- en toerustingscentrum
2008-2012: Directeur Mr. G. Groen van Prinsterstichting

Parlementair:
Recente vragen over:

- ***over de aanpak van wraakporno en onderzoek naar sexting***

Van Tongeren (GL)

Als Kamerlid wil ik proberen niet overal achteraan te lopen. Ik wil mij focussen op wat ertoe doet. Om een open geest te houden lees ik regelmatig non-fictie van denkers met wie ik het niet eens ben en voor de ontspanning Engelstalige thrillers.

Achtergrond:
1984-1993: Australië (vluchtelingen en thuislozen)
1994-1997: directeur van een Haagse vrouwenopvang
1998-2001: senior projectadviseur, Dienst Maatschappelijke Ontwikkeling, gemeente Amsterdam
2001-2003: directeur sociale zaken, gemeente Purmerend
2003-2010: directeur Greenpeace

Parlementair:

Kees van der Staaij (SGP)

Ik stel er een eer in volksvertegenwoordiger te zijn: open ogen en oren te hebben voor iedereen die met concrete knelpunten komt. Kortom: vanuit een vaste overtuiging in woord en daad gericht te zijn op het welzijn van héél Nederland, met open oog voor de noden in het buitenland.

Achtergrond:
1992-1996: stafjurist Raad van State
1996-1998: chefjurist afdeling bestuursrechtspraak Raad van State

Parlementair:

Van: 10.2.e
Verzonden: vrijdag 5 februari 2016 12:26
Aan: 10.2.e
CC: 10.2.e 10.2.e 10.2.e
10.2.e ; 10.2.e
Onderwerp: RE: Uitnodiging voor het rondetafelgesprek over computercriminaliteit III op donderdag 11 februari van 10.00 tot 13.00 uur
Bijlagen: Gespreksnotitie_politie_hoorzitting_CIII.docx

Geachte griffie,

Zoals telefonisch beloofd, stuur ik u hierbij de gespreksnotitie van Inge Philips, plv. Diensthoofd Nationale Recherche, Landelijke Eenheid en spreker namens de politie tijdens de hoorzitting Computercriminaliteit III d.d. 11 februari. Zodra bekend, ontvangen we graag het schema en de gespreksnotities van de andere gasten. Ook gaan we ervan uit dat
het schriftelijk verzoek om toestemming van de minister voor ambtelijke deelname in behandeling bij het departement is en in goede orde komt.

Bij voorbaat hartelijk dank en alvast fijn weekend gewenst.

Met vriendelijke groet,

10.2.e
10.2.e
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

De aanpak van cybercrime is al geruime tijd onderdeel van de landelijke prioriteiten en is als prioriteit opgenomen in de Gemeenschappelijk Veiligheidsagenda 2015-2018. Om cybercrime en vormen van (ernstige) criminaliteit met een digitale component effectief aan te kunnen pakken, is het voor de politie van cruciaal belang om bevoegdheden te hebben die aansluiten bij de technologische ontwikkelingen. Dit wetsvoorstel is een stap in de goede richting en de politie is hiervan dan ook een groot voorstander.

Het wetsvoorstel Computercriminaliteit III past binnen de bredere ontwikkelingen op het terrein van digitalisering in de maatschappij. Aan de ene kant vormt deze digitalisering een bedreiging, omdat criminelen de digitale mogelijkheden gebruiken om nieuwe of gedigitaliseerde vormen van traditionele criminaliteit te plegen. Aan de andere kant biedt de digitalisering de politie potentieel ook mogelijkheden hiertegen op te treden. Dan moeten de bevoegdheden van de politie echter wel in de pas blijven lopen met de ontwikkelingen in de maatschappij. De wet Computercriminaliteit II is al 10 jaar oud en een actualisatie is noodzakelijk om de slagkracht en de effectiviteit van de politie op peil te houden. Met dit wetsvoorstel wordt het speelveld weer gelijk getrokken.

De focus van het wetsvoorstel CCIII ligt op de nieuwe bevoegdheid tot het op afstand heimelijk kunnen binnendringen in een geautomatiseerd werk en hierover vindt dan ook de maatschappelijke discussie plaats. Deze gaat vooral over de verhouding tussen de maatschappelijke veiligheid en de privacy van burgers. Het is voor de politie van belang om duidelijk te maken dat het gebruik van deze bevoegdheid met de allerhoogste waarborgen zal worden omgeven. Het wetsvoorstel beoogt inzet van deze bevoegdheid in zeer specifieke omstandigheden. Zo moet sprake zijn van bestrijding van ernstige strafbare feiten. Daarnaast is de inzet omgeven met de hoogst mogelijke toetsing binnen strafvordering en moet de inzet, net als de inzet van andere opsporingsmiddelen, voldoen aan de eisen van proportionaliteit of subsidiariteit. Een eventuele vrees dat de politie dus op grote schaal computers zal gaan binnendringen is onterecht.

Naast de bevoegdheid tot het op afstand kunnen binnendringen, bevat het wetsvoorstel ook wetswijzigingen op het terrein van online handelsfraude, heling van gegevens, ontoegankelijk maken en het corrumperen en grooming. Deze voorgestelde wijzigingen zijn voor de politie minstens zo belangrijk als de nieuwe bevoegdheid tot het op afstand binnendringen. Deze wijzigen maken het voor burgers, bedrijven en overheid eenvoudiger om aangifte te doen van deze vormen van criminaliteit, terwijl ook de opsporing en de bewijslast om uiteindelijk tot een veroordeling bij de rechter te kunnen komen wordt vergemakkelijkt.

De politie zal zich kleinschalig en landelijk voorbereiden op de zorgvuldige invoering van deze wetswijziging. Dit betekent onder andere dat de samenwerking zowel binnen de politie, als met haar partners, geïntensiveerd wordt met als doel de schaarse, specifieke digitale expertise en innovatie te bundelen en gezamenlijk verder te ontwikkelen. Daarnaast zal via zij-instroom expertise binnen worden gehaald die binnen de politie schaars is. Hiermee wordt ook uitvoering gegeven aan het fundamenteel verhogen van de kwaliteit van de opsporing zoals aangegeven in de countourennota Versterking Opsporing, die onlangs ook aan de vaste Kamercommissie is aangeboden.

Tot slot, de politie is blij met het voorliggende wetsvoorstel. Het geeft de politie handvatten die ze de afgelopen jaren heeft gemist in de bestrijding van de criminaliteit. Deze voorgestelde wetswijzigingen zorgen ervoor dat de politie ook in de gedigitaliseerde wereld recht kan doen aan haar motto “waakzaam en dienstbaar”.

Van: 10.2.e
Verzonden: maandag 8 februari 2016 11:22
Aan: 10.2.e ; 10.2.e 10.2.e Plas, Theo van der (T.G.); Philips, Inge (I.C.)
CC: 10.2.e); 10.2.e
Onderwerp: FW: Uitnodiging voor het rondetafelgesprek over computercriminaliteit III op donderdag 11 februari van 10.00 tot 13.00 uur
Bijlagen: Gespreksnotitie_politie_hoorzitting_CIII.docx

Beste collega,

bijgaand de gespreksnotitie zals die afgelopen vrijdag is verzonden. We werken nu aan Q&A's voor Inge (en het OM).

Met de hartelijke dank voor jullie input!

Met vriendelijke groet,
10.2.e

Is gelijk aan doc 341

Van: 10.2.e
Verzonden: woensdag 10 februari 2016 09:20
Aan: 10.2.e @politie.nl>
Onderwerp: Moties VAO Cybersecurity

Hoi 10.2.e

Gisteren was het VAO Cybersecurity. Hier zijn de volgende voor de politie relevante moties ingediend:

- SP (TK nr. 26643-387) – ONTRADEN DOOR DE STAATSSECRETARIS

De Kamer,

gehoord de beraadslaging,

constaterende dat de voormalig minister van Veiligheid en Justitie heeft gesteld dat het mogelijk is om onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op afstand een computersysteem te betreden;

constaterende dat bij de invoering van de bevoegdheid om een plaats te doorzoeken echter nooit is gesproken over het op afstand binnendringen van computers en dat, indien voor een dergelijk handelen een wettelijke grondslag zal worden gecreëerd, dit in de eerste plaats iets is waarover de Kamer zich zal moeten uitspreken;

verzoekt de regering, te garanderen dat politie en justitie in ieder geval niet overgaan tot het op afstand heimelijk binnendringen van een geautomatiseerd werk zolang de wet computercriminaliteit III niet door de Kamer is behandeld en zij zich hierover heeft kunnen uitspreken,
en gaat over tot de orde van de dag.

- VVD (TK nr. 26643-388) – ONDERSTEUNING VAN BELEID

De Kamer,

gehoord de beraadslaging,

constaterende dat het Cybersecuritybeeld Nederland 5 aangeeft dat de beschikbaarheid van digitale systemen steeds belangrijker wordt omdat belangrijke maatschappelijke processen hiervan afhankelijk zijn en analoge alternatieven steeds vaker ontbreken;

constaterende dat legacy bestaat uit ICT-systemen met verouderde software en hardware met een verhoogd risico op beveiligingslekken, waardoor het risico op hacks en storingen toeneemt en digitale systemen kwetsbaar worden;

overwegende dat binnen de Nederlandse vitale infrastructuur en diensten digitale systemen met legacy worden gebruikt en dit onnodig risico oplevert voor belangrijke maatschappelijke processen en daarmee voor de nationale veiligheid, mede door koppeling van verschillende vitale infrastructuren en ketenafhankelijkheden;

van mening dat legacy in de Nederlandse vitale infrastructuur, bij zowel de overheid als vitale sectoren, zo spoedig mogelijk moet worden vervangen en dat de rijksoverheid hierin een voorbeeldfunctie heeft;

verzoekt de regering, de legacyproblematiek actief, zowel binnen de rijksoverheid als binnen de vitale sectoren, tegen te gaan en daarbij dit punt in de toegezegde doorontwikkeling van de nationale cybersecuritystrategie te betrekken;

verzoekt de regering tevens om dit punt actief op te pakken in het kader van de implementatie van de NIB-richtlijn in het kader van sectorale zorgplichten op het gebied van digitale veiligheid,

en gaat over tot de orde van de dag.

Over de moties zal aanstaande dinsdag gestemd worden

Groet,

10.2.e
Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag
M 10.2.e 10.2.e @politie.nl
Werkdagen: maandag t/m vrijdagochtend

Van: Philips, Inge (I.C.)
Verzonden: woensdag 10 februari 2016 16:48
Aan: 10.2.e ; 10.2.e 10.2.e 10.2.e ; 10.2.e

Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Beste CCIII-vrienden,
Twee minuten is echt heeeel kort! Ik heb onderstaande tekst geoefend en krijg m net binnen twee minuten eruit. Heb me gericht op de vragen die BoF en consorten oproepen. Ik bewaar de voorbeelden in de veronderstelling dat ik die in de beantwoording van vragen kwijt kan.
Groet, Inge

Spreektekst Inge

Twee minuten precies:
1. De politie is voorstander van sterke crypto en andere vormen van bescherming van de persoonlijke levenssfeer. Goed hang- en sluitwerk. Wij willen geen verplichte achterdeurtjes of op wat voor wijze dan ook de online veiligheid schaden.
We zijn er om uw grondrechten te beschermen en de samenleving veiliger te maken. Als wij grondrechten schenden is dat van specifieke personen die verdacht worden van specifieke ernstige strafbare feiten zoals u als wetgever heeft vastgesteld, op de wijze die u als wetgever heeft vastgesteld. Daarin is geen onderscheid in fysiek of digitaal. Om bewijs te vergaren gebruiken we alle middelen die strafvordering ons toestaat, onder toeziend oog van het gezag. Interceptie valt door toenemend gebruik van cryptografie op termijn weg als bewijsmiddel. Dat betekent enerzijds dat wij zwaarder moeten gaan leunen op andere middelen, anderzijds dat wij per definitie steeds verder verwijderd raken van de werkwijze van criminelen. De enige plek waar we nog zicht kunnen hebben op communicatie is op de plek waar deze nog niet versleuteld is, en dat is aan de bron.

2. De politie wil niet structuureel grote hoeveelheden data naar zich toe trekken. Wij willen het vermogen alleen die gegevens te betrekken die kunnen dienen als bewijs voor ernstige strafbare feiten. We zijn geen inlichtingendienst en we neuzen niet rond.

3. De politie d niet. Hacken is onbevoegd binnendringen voor eigen belang zonder enige vorm van toetsing. Digitaal rechercheren is precisiewerk. Arbeidsdeling, werkvoorbereiding, toetsing vooraf door het gezag, forensische kopieen, hashing, verantwoording afleggen in PV. Toetsing achteraf door de rechter. Kan het voorkomen dat we binnendringen in een computer van een onschuldige burger? Zeer onwaarschijnlijk. Maar politiewerk blijft mensenwerk. Als wij iemand aanhouden kunnen we ons ook vergissen, kan sprake zijn van persoonsverwisseling. Bij geautomatiseerde werken is die kans nog kleiner aangezien we regel voor regel kunnen toetsen en bijstellen.

4. Binnendringen op afstand gaat niet over efficiency. Het gaat over penetratievermogen. Wil de samenleving een politie die als het moet, kan doordringen tot de diepste lagen van ernstige criminaliteit of houdt u de politie liever aan de oppervlakte? Want zeker is: we zijn de strijd aan het verliezen. Zonder de bevoegdheid en het vermogen om op afstand binnen te dringen en waar nodig ontoegankelijk te maken, halen we die achterstand nooit meer in.

reservetekst:
Het wetsvoorstel dat voorligt telt vijf bestanddelen:
-strafbaarstelling van online handelsfraude -strafbaarstelling van heling van online gestolen gegevens -verdergaande strafbaarstelling van grooming -binnendringen op afstand van een geautomatiseerd werk -ontoegankelijk maken van gegevens op die wijze aangetroffen

In het speedveld van de digitale opsporing domineren drie ontwikkelingen:
- anonimiteit in beweging en betaling
- laagdrempelige cryptografie
- internationale actieradius criminelen

Vergis u niet in die criminelen. 7-12 [redacted]

In deze context kunt u zich als wetgever afvragen: waarmee is deze samenleving gediend? Moet de politie steeds verder gaan in het veiligstellen van bewijs van ernstige strafbare feiten, een specifieke categorie die door u wettelijk omschreven is? Kan de politie naar eer en geweten voldoen aan het subsidiariteitsbeginsel als het instrumentarium uit balans raakt?

Tweede Kamer
DER STATEN-GENERAAL

Rondetafelgesprek: computercriminaliteit III op

Vaste commissie voor Veiligheid en Justitie
Datum: 11 februari 2016
Zaal: Thorbeckezaal
Tijd: 10.00 - 13.00 uur

- **Blok 1: Privacy - 10.00 tot 10.40 uur**

- Dhr. T. Siedsma, Bits of Freedom
- Dhr. N.A.N.M. van Eijk, hoogleraar informatierecht Universiteit van Amsterdam
- Dhr. J. Kohnstamm, Autoriteit Persoonsgegevens

Blok 2: Praktijk – 10.40 tot 11.50 uur

- Dhr. M. Egberts, Openbaar Ministerie
- Mevr. I. Philips, Nationale Politie
- Dhr. H. de Vries, Nationaal Cyber Security Centrum
- Dhr. C. Baardman, Raad voor de rechtspraak
- Mevr. D. Brouwer, Nederlandse Orde van Advocaten

Blok 3: Technologie/Economie – 11.50 tot 13.00 uur

- Dhr. R. Prins, Fox-IT
- Mevr. L. Postma, Google
- Dhr. B. Gosling, Amsterdam Internet Exchange
- Mevr. L. Holterman, Nederland ICT
- Dhr. B.P.F. Jacobs, Radboud Universiteit

U treft hierna de binnengekomen gespreksnotities.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank NL32ABNA0554706512
KvK 34 12 12 86

M +31 6 13380036
E ton.siedsma@bof.nl
W https://www.bof.nl

Vaste commissie voor Veiligheid en Justitie

Betreft
Bijdrage Bits of Freedom voor rondetafelgesprek wetsvoorstel computercriminaliteit III

Amsterdam
08-02-2016

Volgens Bits of Freedom heeft het wetsvoorstel computercriminaliteit III een averechts effect op de Nederlandse cyber security omdat de hackbevoegdheid de Nederlandse internetter onveiliger maakt in plaats van veiliger. Daarnaast ontbreekt de noodzaak voor deze bevoegdheid. Ook zijn in het wetsvoorstel veel essentiële vragen niet beantwoord. Tot slot is het noodzakelijk dat er een commissie komt die onafhankelijk toezicht op de opsporingsdiensten uitoefent.

1. Noodzaak niet aangetoond

Sinds in 2012 het eerste plan voor de hackvoorstel werd aangekondigd, is de noodzaak voor deze nieuwe bevoegdheid nog nooit aangetoond. Dat gebeurde niet in de Memorie van Toelichting bij de internetconsultatie in 2013 en dat gebeurt evenmin in de Memorie van Toelichting bij het huidige wetsvoorstel.

Dat niet wordt aangetoond waarom deze bevoegdheid daadwerkelijk noodzakelijk is, is buitengewoon verontrustend. Zonder noodzaak is er geen reden voor het bestaan van de bevoegdheid. Het ministerie van Veiligheid en Justitie moet die noodzaak dan ook bewijzen vóór we kunnen nadenken hoe deze bevoegdheid ingeregeld zou moeten worden.

Het aantonen van die noodzaak is des te prangender omdat de hackbevoegdheid een perverse prikkel vormt voor de Nederlandse overheid met betrekking tot de veiligheid van de internetgebruiker. De Nederlandse overheid heeft immers een belang bij het bestaan van (meer) onveilige apparaten bij verdachten, terwijl diezelfde apparaten ook door onschuldige burgers worden gebruikt. Die kunnen de dupe worden als de Nederlandse overheid kennis over zwakheden in software heeft, maar deze niet met het bedrijfsleven en gebruikers deelt.

2. Wetsvoorstel roept veel vragen op

Zelfs als over de ontbrekende noodzaak en de negatieve werking van de bevoegdheid op de veiligheid van onze apparaten en infrastructuur wordt heengestapt, dan blijven er in het wetsvoorstel veel problemen onopgelost. Ter illustratie daarvan worden hieronder de drie belangrijkste besproken.

2.1 Ontbreken technische waarborgen

Bij een wetsvoorstel dat bij uitstek gaat over de inzet van een technisch middel zijn juridische waarborgen bij de inzet niet genoeg. De regels voor de beheersing en integriteit van de techniek zijn cruciaal. Het Besluit technische hulpmiddelen voldoet op dit moment niet aan de eisen van digitale opsporingsbevoegdheden en moet worden herzien. Dat vindt het ministerie van Veiligheid en Justitie gelukkig ook.

Maar de daadwerkelijke inhoud van het nieuwe Besluit is nog niet bekend. Dat betekent dat de wet die nu in het parlement behandeld wordt onvolledig is. Er is immers geen volledig overzicht van de waarborgen maar ook niet van de mogelijke niet afgedekte (technische) risico's.

Het is daarom essentieel dat het Besluit technische hulpmiddelen wordt herzien vóórdat het parlement zich uitspreekt over het voorliggende wetsvoorstel, met een voorhangprocedure waarbij het Besluit ook op internetconsultatie wordt geplaatst. Alleen dan wordt daadwerkelijk duidelijk of – en hoe – de risico's bij het gebruik van deze bevoegdheid worden ingedamd.

2.2 Reikwijdte geautomatiseerd werk

De reikwijdte van het begrip 'geautomatiseerd werk' is zodanig geformuleerd dat niet voorzienbaar is welk apparaat wel of niet gehackt mag worden door de politie. Onder de voorgestelde definitie valt eigenlijk elk apparaat dat met het internet verbonden is of zou kunnen zijn. In aanmerking genomen dat het aantal apparaten dat daaronder valt exponentieel gaat groeien bij de ontwikkeling van het 'Internet of Things' roept dat de vraag op: tot hoe ver mag deze bevoegdheid gaan bij apparaten die zich in of rond het menselijk lichaam begeven?

Staatssecretaris Dijkhoff stelt dat ook pacemakers onder de definitie vallen. Maar is het echt nodig om zulke apparaten onder de categorie te hacken apparaten te laten vallen? En is het bijvoorbeeld de bedoeling om in de toekomst auto's te hacken om die vervolgens stil te zetten als de politie een verdachte aan wil houden?

Als er bij het ministerie van Veiligheid en Justitie of bij de Nationale Politie over zulke inzetten wordt nagedacht, dan zou dat voor het publiek duidelijk moeten worden, zodat er een helder debat kan plaatsvinden over de reikwijdte van de bevoegdheid. Nu, maar ook in de toekomst.

2.3 Reikwijdte inzet bevoegdheid

De bevoegdheid is volgens de wet en de Memorie van Toelichting, anders dan vaak wordt gezegd, niet alleen gericht op cybercriminelen. Sterker nog, de bevoegdheid is van toepassing op een hele brede groep van misdrijven verdachte personen. Voor een bevoegdheid die wordt voorgesteld als een ultimum redium is dat veel te breed, zeker met inachtneming van het volgende.

In de jaren '70 van de vorige eeuw werd de telefoontap ingevoerd. In de Handelingen bij de invoering van de bevoegdheid werd aangegeven dat deze slechts enkele keren per jaar zou worden ingezet. Intussen weten we dat die situatie nogal gewijzigd is. Het is niet uit te sluiten dat dat in de toekomst voor de hackbevoegdheid ook zo zal gaan.

In de financiële paragraaf bij het huidige wetsvoorstel wordt al aangegeven dat er kosten kunnen worden bespaard met de inzet van deze bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen. Dat betekent dat de deur naar de inzet van de hackbevoegdheid als efficiënter middel in andere domeinen op zijn minst al op een kier staat.

Bits of Freedom vindt dat een dergelijke zware bevoegdheid nooit uit efficiëntie-overwegingen moet worden ingezet.

Tot slot zou Bits of Freedom nog het volgende willen meegeven.

3. Voer een onafhankelijke commissie in voor toezicht op opsporingsdiensten

Er zijn steeds meer opsporingsbevoegdheden die zich in het digitale domein afspelen. Denk bijvoorbeeld aan het controleren of observeren van sociale media, maar ook *predictive policing* en natuurlijk het voorliggende hackvoorstel. De controle op de inzet van zulke bevoegdheden, die naar hun aard heimelijk worden toegepast, is essentieel. Nu vindt die controle vooraf plaats via de rechter-commissaris en eventueel achteraf in de rechtszaal.

Maar veel verdachten komen uiteindelijk niet voor de rechter en de rechter-commissaris toetst het individuele geval, maar kijkt niet per se naar de samenhang met andere zaken en de controle op de inzet van die bevoegdheid. Daarnaast kunnen sommige misstanden bij de inzet in de rechtszaal door de advocaat niet worden tegengeworpen aan het Openbaar Ministerie. Er zijn op die manier ook weinig prikkels om in dat opzicht verbeteringen door te voeren.

Bits of Freedom acht het verstandig om daarvoor een onafhankelijke commissie in te stellen, in zekere zin vergelijkbaar met de huidige CTIVD voor de geheime diensten. Die commissie zou dan opsporingsbreed kunnen kijken naar het hele proces, van totstandkoming van verzoeken om bevoegdheden in te zetten tot en met de wijze waarop de inzet plaatsvindt.

COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De Minister van Veiligheid en Justitie

Postbus 20301
2500 EH DEN HAAG

DATUM 17 februari 2014
ONS KENMERK z2013-00349
CONTACTPERSOON

UW BRIEF VAN 2 mei 2013
UW KENMERK

ONDERWERP Consultatie conceptwetsvoorstel Computercriminaliteit III

Geachte ,

Bij brief van 2 mei 2013 heeft u het College bescherming persoonsgegevens (CBP) het concept-wetsvoorstel Computercriminaliteit III toegezonden met het verzoek daarover advies uit te brengen op grond van het bepaalde in artikel 51, tweede lid, Wet bescherming persoonsgegevens. Het CBP heeft u bij brief van 23 mei 2013 bericht zijn advies te zullen uitbrengen wanneer de opmerkingen van de internetconsultatie zijn verwerkt in een aangepaste tekst. Bij e-mail van 23 januari 2014 heeft het CBP van uw ministerie een overzicht van de belangrijkste wijzigingen ontvangen. Het CBP voldoet hiermee aan uw verzoek.

Inhoud van het voorstel
Het conceptwetsvoorstel strekt tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III). Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Het wetsvoorstel vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer alsmede van het in het regeerakkoord van dit kabinet opgenomen voornemen om de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. Daartoe wordt voorgesteld te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen.

Beoordeling van het voorstel
Het CBP heeft zijn advies beperkt tot de bespreking van de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk. Zoals hierna in de bijlage bij deze brief is uiteengezet luidt zijn oordeel en vervolgens zijn advies hierover als volgt.

Het CBP onderkent dat het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit en strafbare feiten in zijn algemeenheid, zoveel mogelijk gelijke tred dient te houden met de technologische ontwikkelingen.

Het bereik van de thans voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk strekt zich uit tot een zeer grote hoeveelheid gegevens. Het betreft volledige toegang tot alle historische gegevens die op randapparatuur zijn opgeslagen en de gegevens die worden opgeslagen op en uitgewisseld via alle communicatiekanalen waarmee de randapparatuur is verbonden. Bovendien kan deze bevoegdheid ook betrekking hebben op toekomstige gegevens. Daarbij gaat het niet alleen om gegevens die de verdachte zelf betreffen, maar ook om gegevens van alle personen die worden genoemd in documenten of met wie hij/zij digitaal contact heeft gehad. Toepassing van deze bevoegdheid raakt daarmee een grote groep mensen tot wie de verdenking zich niet richt.

Juist om die reden is het van groot belang dat het wetsvoorstel blijk geeft van een zorgvuldige afweging binnen de grondwettelijke kaders van het recht op eerbiediging van de persoonlijke levenssfeer, zoals vastgelegd in artikel 10 Grondwet en artikel 8 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Op grond van het EVRM en de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) zijn inbreuken op fundamentele rechten slechts rechtmatig indien deze voldoen aan strikte voorwaarden, die zien op de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.

In de toelichting op het thans voorliggende wetsvoorstel zijn overwegingen opgenomen ten aanzien van de noodzaak, proportionaliteit en subsidiariteit. Het CBP is evenwel van oordeel dat het ingrijpende karakter van de voorgestelde bevoegdheid en de uitgebreide kring van personen die de inzet ervan kan betreffen, hierbij onvoldoende zijn onderkend. De overwegingen die ten grondslag liggen aan de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk, worden in belangrijke mate gebaseerd op een aantal concrete situaties dat – wat daar verder overigens van zij – de invoering van de beoogde bevoegdheid op zichzelf onvoldoende kan rechtvaardigen. De dringende noodzaak als bedoeld in artikel 8 EVRM behoeft daarnaast, mede in het licht van de telkens te maken afweging van proportionaliteit en subsidiariteit ook een zelfstandige, boven de casuïstiek verheven beschouwing en onderbouwing.

Gelet hierop adviseert het CBP u om bij de gronden en afwegingen die de noodzaak van aanpassing van de huidige wettelijke bepalingen moeten onderbouwen, nadere aandacht te besteden aan de door artikel 8 EVRM gestelde voorwaarden.

Advies

Het CBP adviseert u het voorstel niet aldus in te dienen.

DATUM 17 februari 2014
ONS KENMERK z2013-00349

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

DATUM 17 februari 2014
ONS KENMERK z2013-00349

Bijlage bij de brief van het College bescherming persoonsgegevens van 17 februari 2014 inzake het conceptwetsvoorstel Computercriminaliteit III

Opmerkingen vooraf
Het CBP heeft als wettelijke taak om op grond van het bepaalde in artikel 51, tweede lid, Wet bescherming persoonsgegevens te adviseren over voorstellen van wet die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Daartoe is het noodzakelijk dat het voorgelegde voorstel een afgeronde versie betreft en dat eventuele wijzigingen naar aanleiding van een internetconsultatie daarin zijn verwerkt. Ten tijde van de ontvangst van uw brief van 2 mei 2013 is de internetconsultatie inzake dit voorstel gestart. Het CBP heeft u bij brief van 23 mei 2013 bericht zijn advies te zullen uitbrengen wanneer de opmerkingen van internetconsultatie zijn verwerkt in een aangepaste tekst. Bij e-mail van 23 januari 2014 heeft het CBP van uw ministerie een overzicht van de belangrijkste wijzigingen ontvangen.

Daarnaast is uit uw brief van 12 december 2013 aan de Tweede Kamer gebleken dat u voornemens bent om een aanvullend voorstel als onderdeel van dit wetsvoorstel in januari 2014 aan de Raad van State voor te leggen[1]. Door uw ministerie werd per e-mail bevestigd dat deze aanvulling en tevens nog enkele andere wijzigingen direct aan de Raad van State zullen worden voorgelegd. Het CBP is (nog) niet in de gelegenheid gesteld om advies uit te brengen omtrent deze onderdelen van het wetsvoorstel.

Inhoud van het voorstel
Ten dele heeft het conceptwetsvoorstel, in **Artikel I**, betrekking op wijziging van het Wetboek van Strafrecht (Sr). Het CBP zal dit onderdeel niet bespreken in zijn advies, aangezien het dit vanuit oogpunt van dataprotectie niet aangewezen acht. De onderdelen C, D en F van **Artikel II**, dat betrekking heeft op wijziging van het Wetboek van Strafvordering (Sv) zal het CBP hierna bespreken voor zover dat uit oogpunt van dataprotectie van belang is.

Onderdeel C – Onderzoek in een geautomatiseerd werk
Dit onderdeel betreft de invoeging van een nieuw **artikel 125ja** Sv, inhoudende een nieuwe bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager die bij de verdachte in gebruik is, en het onderzoek doen met een technisch hulpmiddel.

Op grond van het **eerste lid** van dit ontwerp-artikel kan de officier van justitie in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten en dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, indien het onderzoek dit dringend vordert, bevelen dat een (volgens het gewijzigde voorstel:) *daartoe aangewezen* opsporingsambtenaar of buitengewoon

[1] Kamerstukken II 2013-2014, 31 015, nr. 95.

opsporingsambtenaar binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en onderzoek doet met een technisch hulpmiddel met het oog op:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;
b. het overnemen van bestaande of toekomstige gegevens van het geautomatiseerde werk, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
c. de ontoegankelijkmaking van gegevens;
d. een bevel tot het direct afluisteren of opnemen van telecommunicatie, het direct afluisteren of opnemen van telecommunicatie bij verdenking van ernstige criminaliteit in georganiseerd verband en het direct afluisteren of opnemen van telecommunicatie bij aanwijzingen van een terroristisch misdrijf;
e. een bevel tot stelselmatige observatie of stelselmatige observatie bij verdenking van ernstige criminaliteit in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.

In het belang van het onderzoek kunnen gegevens worden vastgelegd. Een toegevoegde wijziging op het conceptartikel is de bepaling dat de daartoe aangewezen opsporingsambtenaren dienen te voldoen aan eisen op het gebied van opleiding en expertise, die in het Besluit technische hulpmiddelen strafvordering zullen worden uitgewerkt. Het **tweede lid** omschrijft de inhoudelijke vereisten die aan het bevel worden gesteld. De wijziging van het voorstel houdt de toevoeging in dat indien het bevel de onderdelen a, b of c betreft, in het bevel tevens een duidelijke omschrijving van de handelingen wordt gegeven. Een nieuw onderdeel f. wordt toegevoegd dat de vermelding vereist van het tijdstip waarop, of de periode waarin het bevel ten uitvoer wordt gelegd. Het **derde lid** noemt de maximale periode waarvoor het bevel kan worden gegeven, te weten vier weken met een mogelijke verlenging van telkens vier weken. In het **vierde lid** wordt bepaald dat het bevel slechts kan worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. Bij dringende noodzaak (**vijfde lid**) kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven, in dat geval binnen drie dagen op schrift te stellen. Het **zesde lid** stelt dat in een algemene maatregel van bestuur (amvb) regels worden gesteld over de opslag, verstrekking en plaatsing van het technische hulpmiddel, de technische eisen waaraan het middel moet voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde gegevens, de vastlegging van gegevens over de uitvoering van het bevel en de werking van het technische hulpmiddel. De wijziging van het voorstel houdt de toevoeging van een onderdeel c. in dat de mogelijkheid biedt bij amvb nadere regels te stellen omtrent de autorisatie van de opsporingsambtenaren die kunnen worden belast met het verrichten van het onderzoek en de samenwerking met andere opsporingsambtenaren.

Onderdeel D – Decryptiebevel aan de verdachte

Dit onderdeel leidt tot wijziging van **artikel 125k** Sv, inhoudende dat het bevel tot ontsleuteling van gegevens onder de daarin gestelde voorwaarden kan worden gericht aan de verdachte. Aangezien dit onderdeel van het voorstel niet in overwegende mate betrekking heeft op de verwerking van persoonsgegevens zal het CBP het voorstel hierna niet verder bespreken.

Onderdeel F – Ontoegankelijkmaking van gegevens
Dit onderdeel stelt de invoeging voor van een nieuw **artikel 125p** Sv en betreft een te geven bevel tot ontoegankelijkmaking van gegevens door de officier van justitie aan een aanbieder van een communicatiedienst, na een voorafgaande machtiging daartoe door de rechter-commissaris.
Dit onderdeel kan weliswaar betrekking hebben op een verwerking van persoonsgegevens, maar dit leidt niet tot een nieuw soort verwerking van persoonsgegevens. Om die reden acht het CBP de bespreking hiervan binnen de context van dit voorstel uit oogpunt van dataprotectie niet opportuun.

Beoordeling van het voorstel

1.1 Toetsingskader
De voorgestelde nieuwe bevoegdheid om heimelijk, op afstand binnen te dringen in een geautomatiseerd werk maakt inbreuk op fundamentele rechten, in het bijzonder op artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet, die elk het recht op eerbiediging van de persoonlijke levenssfeer vaststellen. Op grond van het EVRM en de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) zijn inbreuken op fundamentele rechten slechts rechtmatig indien deze voldoen aan de volgende voorwaarden: de beperking moet zijn "in accordance with the law", "in pursuit of a legitimate aim" en "necessary in a democratic society". Voor de toets van noodzakelijkheid dient op de eerste plaats sprake te zijn van een dringende noodzaak ("pressing social need") die feitelijk moet worden aangetoond, waarbij tevens dient te blijken dat sprake is van maatschappelijke schade die door de voorgestelde maatregel effectief kan worden tegengegaan. Daarnaast moet de beperking evenredig zijn aan het daarmee beoogde doel en mag deze niet verder gaan dan nodig ter vervulling van het legitieme doel (toets van proportionaliteit en subsidiariteit). Hierbij is tevens van belang dat is voorzien in adequate waarborgen ten behoeve van de uitoefening van het fundamentele recht.

1.2 Noodzaak, proportionaliteit en subsidiariteit volgens het voorstel
In de ontwerp-memorie van toelichting worden de achtergrond en redenen voor de voorgestelde wijziging als volgt omschreven. 'Met dit wetsvoorstel wordt aangesloten bij de snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit. Deze ontwikkelingen roepen voortdurend de vraag op of de juridische instrumenten voldoende zijn toegesneden op een effectieve bestrijding van computercriminaliteit. Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een leemte in de bestaande wettelijke bevoegdheden. De bestaande opsporingsbevoegdheden schieten echter in toenemende mate tekort om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen.'[2]

[2] Zie ontwerp-toelichting, p. 46.

De toelichting noemt daarvoor de volgende, redengevende ontwikkelingen, die worden toegelicht aan de hand van voorbeelden[3].
- De versleuteling van elektronische gegevens vormt in toenemende mate een probleem voor de opsporing van strafbare feiten.
- Het gebruik van draadloze netwerken, niet alleen in een woning, maar ook op andere plaatsen. Als gebruik wordt gemaakt van verschillende toegangspunten tot het internet, wat in toenemende mate het geval is, is het aftappen van de volledige communicatie van de verdachte vrijwel onmogelijk.
- Het gebruik van Cloudcomputingdiensten. In toenemende mate wordt gebruik gemaakt van zogenaamde "webbased" toepassingen, waarbij gegevens worden opgeslagen in de "Cloud" op servers die zich elders in Nederland of in het buitenland bevinden.
Aan alternatieven om andere (bestaande) opsporingsbevoegdheden in te zetten, worden teveel bezwaren toegedicht[4].

1.3 Algemeen beoordelingskader
De technologische ontwikkelingen in de laatste decennia zijn van grote invloed geweest op ons maatschappelijke leven, in het bijzonder de invloed van elektronische communicatietechnologie. Een steeds groter deel van ons leven speelt zich (louter) digitaal af, zoals onder meer bankieren, winkelen, belasting betalen en onderwijs. De digitaal vastgelegde en uitgewisselde informatie betreft ook in toenemende mate zeer persoonlijke gegevens. Daarbij zijn de technologische mogelijkheden om digitale gegevens toegankelijk te maken en met elkaar te combineren eveneens toegenomen. Het maatschappelijk belang bij adequate bescherming van dit privéleven tegen de toegenomen technologische inbreukmogelijkheden is dan ook groot. Opsporingsbevoegdheden, maar ook privacybescherming moeten gelijke tred houden met de technologische ontwikkelingen. Het EHRM heeft in dat verband onder meer betoogd dat dit een zorgvuldige afweging van belangen vergt en dat een lidstaat die een pioniersrol wenst te vervullen in de ontwikkeling van nieuwe technologieën een bijzondere verantwoordelijkheid draagt dat in dat opzicht de juiste balans wordt gevonden.[5]

Het bereik van de voorgestelde bevoegdheid strekt zich uit tot een zeer grote hoeveelheid gegevens. Het betreft volledige toegang tot alle historische gegevens die op randapparatuur zijn opgeslagen en de gegevens die worden opgeslagen op en uitgewisseld via alle communicatiekanalen waarmee de randapparatuur is verbonden. Het omvat ook observatie van

[3] Zie ontwerp-toelichting p. 6-10
[4] Zie ontwerp-toelichting p. 11-12
[5] EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (S. and Marper/United Kingdom), ro. 112: "*The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.* (...) any State claiming a pioneer role in the development of new technologies bore special responsibility for striking the right balance in this regard."

historische correspondentie (e-mail en documenten) en zelfs van concepten en gewiste stukken (die veelal nog te achterhalen zijn op harde schijven). Bovendien is de bevoegdheid niet beperkt tot de vastlegging van reeds aanwezige gegevens, maar kan deze ook betrekking hebben op toekomstige gegevens. Bij het binnendringen in een geautomatiseerd werk gaat het niet alleen om gegevens die in de randapparatuur zijn opgeslagen, maar ook om toegang tot gegevens die elders - zoals in de *Cloud* - zijn opgeslagen. Dat kan een medisch dossier zijn, online toegang tot bank- en belastinggegevens, een overzicht van gebruikte zoektermen in een zoekmachine en/of toegang tot iemands profiel en al zijn contacten op een sociale netwerksite. Daarnaast biedt de bevoegdheid de mogelijkheid om ingebouwde camera's en microfoons op afstand aan te zetten. Het gaat daarbij niet alleen om gegevens die de verdachte zelf betreffen, maar ook om gegevens van alle personen die worden genoemd in documenten of met wie hij/zij digitaal contact heeft gehad. De privacyinbreuk treft daarmee in veel gevallen een grote groep burgers tot wie de verdenking zich niet richt. De bevoegdheid ziet bovendien niet alleen op het binnendringen van laptops en computers, maar ook van smartphones, smart tv's en allerlei andere apparatuur die digitaal kan communiceren. De uitbreiding die de voorgestelde nieuwe bevoegdheid biedt is daarmee ongekend omvangrijk.

1.4 Toetsing van noodzaak, proportionaliteit en subsidiariteit

Noodzaak
Voor wat betreft de aan te tonen noodzaak voert het voorstel aan de hand van de technologische ontwikkelingen aan dat de bestaande opsporingsbevoegdheden tekort schieten en noodzaken tot verdergaande bevoegdheden. Hoewel wordt gesteld dat de opsporing dringend behoefte heeft aan deze nieuwe bevoegdheid en daarvoor enkele situaties worden aangevoerd waarin de bestaande middelen geen soelaas zouden bieden, is in de toelichting onvoldoende geconcretiseerd noch is aangetoond waaruit de dringende noodzaak voor de samenleving bestaat die tot het invoeren van deze inbreukmakende maatregel noopt. De overwegingen die ten grondslag liggen aan de voorgestelde bevoegdheid worden weliswaar in belangrijke mate gebaseerd op een aantal concrete situaties, doch die kunnen de invoering van de beoogde bevoegdheid op zichzelf onvoldoende rechtvaardigen. De dringende noodzaak als bedoeld in artikel 8 EVRM behoeft daarnaast ook een zelfstandige, boven de casuïstiek verheven beschouwing en onderbouwing. De noodzaak ("pressing social need") voor de invoering van deze nieuwe bevoegdheid dient in objectieve bewoordingen onomstotelijk te worden vastgesteld en is in de toelichting onvoldoende onderbouwd. Het CBP adviseert om de ontbrekende overwegingen alsnog op te nemen.

Bovenstaande laat onverlet dat het CBP ten aanzien van enkele van de genoemde voorbeelden het volgende overweegt.

1. In de toelichting wordt onvoldoende onderscheid gemaakt tussen het versleutelen van bestanden en gegevens door verdachten, het versleutelen van communicatiestromen in transit, en het feit dat mensen gegevens elders opslaan, in de *cloud*. Dit onderscheid is echter wezenlijk om te bepalen in hoeverre toepassing van de bevoegdheid noodzakelijk is, en of er geen andere middelen zijn om dezelfde doelen te bereiken die een geringere inbreuk maken op de persoonlijke

levenssfeer van betrokkenen. In Nederland zijn alle aanbieders van openbare elektronische communicatienetwerken en -diensten verplicht om bij een internettap de communicatie die zij zelf versleutelen, ontsleuteld aan te leveren. Indien voor het opsporingsonderzoek dringend toegang is vereist tot gegevens die in beheer zijn bij de in de toelichting genoemde buitenlandse aanbieders als Google, Skype of Facebook, geldt dat de toelichting niet stelt of onderbouwt dat deze bedrijven niet zouden meewerken aan rechtshulpverzoeken. Het feit dat zij in toenemende mate de communicatie in transit versleutelen, laat onverlet dat zij toegang hebben of kunnen verschaffen tot de onversleutelde inhoud van e-mails en bestanden op hun servers, dan wel gevraagd kunnen worden mee te werken aan een tap op de communicatie van een specifieke verdachte. Indien een verdachte zelf bestanden heeft versleuteld met behulp van de in de toelichting genoemde programma's PGP of TrueCrypt, zou de opsporing gebruik kunnen maken van de eveneens in dit wetsvoorstel voorziene bevoegdheid tot het geven van een decryptiebevel, of van andere bestaande bijzondere opsporingsbevoegdheden. De toelichting onderbouwt niet de noodzaak om de bevoegdheid tot het binnendringen van een geautomatiseerd werk toe te passen, in relatie tot de omvang en ernst van de privacyinbreuk die dit oplevert. Ten aanzien van het gebruik van TOR-netwerken om communicatie in transit te versleutelen, geldt dat de toelichting dient te onderbouwen waarom andere veel gebruikte methoden om ernstige criminaliteit te bestrijden, niet effectief zijn (het vereiste van subsidiariteit).

2. Bij het bestrijden van botnets zijn situaties denkbaar dat specifieke command-and-control-servers zich in het buitenland bevinden of dat de locatie ervan niet kan worden achterhaald. In die gevallen volstaan de bestaande middelen niet en kan het middel van ontoegankelijkmaking door middel van het op afstand binnendringen van een geautomatiseerd werk mogelijk een oplossing bieden. Ook in geval van specifieke situaties waarin bijvoorbeeld een DDoS-aanval gaande is op een bank of andere essentiële voorziening, is denkbaar dat deze combinatie van bevoegdheden doel treft en de aanval op deze wijze kan worden gestopt. Daarnaast lijken in gevallen waarin gebruik wordt gemaakt van de zogenaamde *bulletproof hosting providers* evenmin voldoende effectieve andere middelen voorhanden, zodat in die gevallen de inzet van deze bevoegdheid een optie is. Aan de in de toelichting gevolgde redenering dat effectieve middelen in geval van *bulletproof hosting providers* ontbreken, kan echter niet de conclusie worden verbonden dat de opsporing heimelijk toegang dient te krijgen tot *alle* in de *cloud* opgeslagen gegevens.

Proportionaliteit
Voor wat het betreft de proportionaliteit miskent het voorstel de omvang van de inbreuk die het gevolg zal zijn van invoering van deze bevoegdheid. Die inbreuk is gelegen in enerzijds de grote hoeveelheid en het karakter van de betreffende persoonsgegevens en anderzijds de uitgebreide kring van personen wier recht op eerbiediging van de persoonlijke levenssfeer hierdoor wordt aangetast. De vereiste afweging of de ernst van de inbreuk die het middel tot gevolg heeft in verhouding staat tot het daarmee te dienen doel, ontbreekt in de toelichting.

Volgens het voorstel kan de bevoegdheid tot onderzoek in een geautomatiseerd werk slechts worden toegepast met het oog op de hiervoor onder a. tot en met e. geformuleerde doeleinden. Weliswaar wordt het doel onder a. (het vaststellen van de aanwezigheid van gegevens of het

bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker) in de toelichting als niet vergaand gekarakteriseerd, maar wanneer eenmaal de toegang is verkregen door middel van deze bevoegdheid is het resultaat onverminderd vergaand en heeft de opsporing de ongelimiteerde toegang tot *alle* beschikbare digitale gegevens. Dat geldt ook voor de toepassing voor de andere genoemde doeleinden. Na verkregen toegang tot het geautomatiseerde werk door middel van plaatsing van spyware, valt die toegang niet te beperken tot slechts hetgeen werd beoogd met het bevel. Dit is niet alleen disproportioneel te achten, maar leidt ook tot een bovenmatige verwerking van politiegegevens (artikel 3, tweede lid, Wet politiegegevens).

1.5 Waarborgen

Gelet op de reikwijdte van de bevoegdheid en de ernst van de inbreuk op de persoonlijke levenssfeer van de betrokkene dienen tegenover de toepassing van deze bevoegdheid strikte waarborgen te staan. Het voorstel voorziet in een aantal waarborgen, waaronder bepalingen die de toepassing beperken tot verdenking van misdrijven van een bepaalde ernst, de bepaling dat de bevoegdheid slechts met het oog op bepaalde doeleinden mag worden ingezet, het vereiste van de vermelding van de gronden voor het bevel en het vereiste van een voorafgaande machtiging van de officier van justitie door de rechter-commissaris. Naast de in het voorstel genoemde voorwaarden acht het CBP ook de volgende waarborgen wezenlijk.

- *Controlemaatregelen en logging*

Een belangrijke waarborg dient te zijn gelegen in de controleerbaarheid van de toepassing gedurende het gehele proces van de aanvraag tot en met de uitvoering. Artikel 4, derde lid, Wet politiegegevens, dat ziet op de verplichting tot het treffen van passende technische en organisatorische maatregelen, vereist dat een sluitend controlesysteem wordt opgezet bij bevoegdheden als de onderhavige, waarmee door middel van duidelijk controleerbare procedures verantwoording wordt afgelegd over de gehele periode van onderzoek. Tevens is hierbij kennis van en inzicht in de ingezette software noodzakelijk. Kwaliteit en betrouwbaarheid, alsmede eventuele verborgen kwetsbaarheden dienen voorwerp te zijn van voortdurende toetsing.

Naast de "gewone" journaal- en verbaliseerverplichting ten aanzien van de toegepaste middelen, is de logging van belang. Ten aanzien van logging vermeldt de toelichting dat te allen tijde kan worden gecontroleerd welke technische handelingen in dit kader hebben plaatsgevonden door middel van logging, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van de bevoegdheid.[6] Echter, logging kan vooralsnog niet altijd leiden tot het weergeven van alle relevante handelingen.[7] Daarbij geldt ook hier dat voor zinvolle logging de exacte werking van de gebruikte software bekend moet zijn, waaronder begrepen kennis van de broncode.

[6] Zie ontwerp-toelichting p. 24
[7] Bijvoorbeeld wanneer het binnendringen in het geautomatiseerde werk mislukt en het systeem crasht voordat logging heeft kunnen plaatsvinden.

- *Rechtsbescherming; systematiek strafvordering*

Deze nieuwe bevoegdheid is geplaatst in titel IV inzake enige bijzondere dwangmiddelen. Deze dwangmiddelen worden gekenmerkt door een zekere kenbaarheid van de toepassing voor de betrokkene. De voorgestelde bevoegdheid wordt daarentegen gekenmerkt door de heimelijke toepassing ervan en heeft daarmee onmiskenbaar het karakter van een bijzondere opsporingsbevoegdheid. De bijzondere opsporingsbevoegdheden zijn ondergebracht in afzonderlijke titels in het Wetboek van Strafvordering die voorzien in bijzondere waarborgen bij de toepassing hiervan, sedert de invoering van deze systematiek in 2000 door de Wet bijzondere opsporingsbevoegdheden. Uitgangspunt van deze wet vormde dat opsporingsmethoden die zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing, dan wel die een inbreuk maken op grondrechten van burgers, een voldoende specifieke basis behoeven in het Wetboek van Strafvordering[8]. De in het geding zijnde belangen en fundamentele rechten vereisen dit. De titel van de algemene bepalingen geldend voor alle bijzondere opsporingsbevoegdheden bevat specifieke waarborgen, die – tenminste ten dele – met de voorgestelde plaatsing in de titel van de dwangmiddelen aan de onderhavige bevoegdheid worden onthouden.

- *Kennisgeving aan betrokkene, toezicht en toetsing effectiviteit*

De kennisgeving aan de betrokkene door middel van een notificatie (achteraf) vormt, ook in het licht van de berichten over de gebrekkige mate waarin de notificatieplicht in zijn algemeenheid thans wordt nageleefd, een geringe waarborg voor de af te leggen verantwoording voor de toepassing van het middel. Gelet op de implicaties van de uitoefening van deze bevoegdheid verdient het dan ook aanbeveling dat het voorstel voorziet in een controle-instrument, waarmee direct en effectief toezicht wordt uitgeoefend op de wijze van uitvoering van de bevoegdheid, onder meer door middel van een verplichting regelmatig daarop betrekking hebbende statistieken en overzichten beschikbaar te stellen. Opname van een horizonbepaling is in dit verband eveneens onontbeerlijk te achten.

Tot slot

Het CBP wijst u nog op een omissie in het conceptwetsvoorstel ten aanzien van Artikel II onderdeel E, waarin na regel 2 de verdere bewoording van de zin lijkt te zijn weggevallen.

[8] Kamerstukken II 1996-1997, 25 403, nr. 3, p. 3

CBP adviseert over 'hackbevoegdheid' politie en opsporingsdiensten

Nieuwsbericht/17 februari 2014
Categorie:

- Internet en telecom
- Politie
- Bijzondere opsporing

Op verzoek van de minister van Veiligheid en Justitie heeft het College bescherming persoonsgegevens (CBP) geadviseerd over het conceptwetsvoorstel Computercriminaliteit III. Hierin worden onder meer nieuwe bevoegdheden voorgesteld om de opsporing en vervolging van computercriminaliteit te verbeteren. Het CBP adviseert het voorstel niet aldus in te dienen.

In zijn advies bespreekt het CBP de voorgestelde bevoegdheid voor de politie en opsporingsdiensten tot zogeheten 'onderzoek in een geautomatiseerd werk', ook wel aangeduid als 'hackbevoegdheid'. Volgens het CBP wordt onvoldoende onderkend dat deze nieuwe bevoegdheid een ongekend verreikend karakter heeft. Het gaat namelijk om zeer veel gegevens van een uitgebreide kring mensen.

De 'hackbevoegdheid' maakt onder meer volledige toegang mogelijk tot alle historische - en ook toekomstige - gegevens opgeslagen op randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Dit zijn niet alleen gegevens die de verdachte zelf betreffen, maar ook gegevens van iedereen die in documenten voorkomt of met wie er digitaal contact is geweest. Daarmee raakt de toepassing van deze bevoegdheid een grote groep mensen die geen verdachten zijn.

Daarom moet het wetsvoorstel blijk geven van een zorgvuldige afweging binnen de grondrechtelijke kaders van het recht op eerbiediging van de persoonlijke levenssfeer, aldus het CBP. Dit recht is vastgelegd in artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

Inbreuken op grondrechten zijn alleen rechtmatig als wordt voldaan aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Uit de toelichting op het wetsvoorstel blijken echter onvoldoende de gronden en overwegingen die de noodzaak van invoering van een zo ingrijpende bevoegdheid kunnen rechtvaardigen. Het CBP adviseert daarom het wetsvoorstel beter te onderbouwen.

De aanpak van cybercrime is al geruime tijd onderdeel van de landelijke prioriteiten en is als prioriteit opgenomen in de Gemeenschappelijk Veiligheidsagenda 2015-2018. Om cybercrime en vormen van (ernstige) criminaliteit met een digitale component effectief aan te kunnen pakken, is het voor de politie van cruciaal belang om bevoegdheden te hebben die aansluiten bij de technologische ontwikkelingen. Dit wetsvoorstel is een stap in de goede richting en de politie is hiervan dan ook een groot voorstander.

Het wetsvoorstel Computercriminaliteit III past binnen de bredere ontwikkelingen op het terrein van digitalisering in de maatschappij. Aan de ene kant vormt deze digitalisering een bedreiging, omdat criminelen de digitale mogelijkheden gebruiken om nieuwe of gedigitaliseerde vormen van traditionele criminaliteit te plegen. Aan de andere kant biedt de digitalisering de politie potentieel ook mogelijkheden hiertegen op te treden. Dan moeten de bevoegdheden van de politie echter wel in de pas blijven lopen met de ontwikkelingen in de maatschappij. De wet Computercriminaliteit II is al 10 jaar oud en een actualisatie is noodzakelijk om de slagkracht en de effectiviteit van de politie op peil te houden. Met dit wetsvoorstel wordt het speelveld weer gelijk getrokken.

De focus van het wetsvoorstel CCIII ligt op de nieuwe bevoegdheid tot het op afstand heimelijk kunnen binnendringen in een geautomatiseerd werk en hierover vindt dan ook de maatschappelijke discussie plaats. Deze gaat vooral over de verhouding tussen de maatschappelijke veiligheid en de privacy van burgers. Het is voor de politie van belang om duidelijk te maken dat het gebruik van deze bevoegdheid met de allerhoogste waarborgen zal worden omgeven. Het wetsvoorstel beoogt inzet van deze bevoegdheid in zeer specifieke omstandigheden. Zo moet sprake zijn van bestrijding van ernstige strafbare feiten. Daarnaast is de inzet omgeven met de hoogst mogelijke toetsing binnen strafvordering en moet de inzet, net als de inzet van andere opsporingsmiddelen, voldoen aan de eisen van proportionaliteit of subsidiariteit. Een eventuele vrees dat de politie dus op grote schaal computers zal gaan binnendringen is onterecht.

Naast de bevoegdheid tot het op afstand kunnen binnendringen, bevat het wetsvoorstel ook wetswijzigingen op het terrein van online handelsfraude, heling van gegevens, ontoegankelijk maken en het corrumperen en grooming. Deze voorgestelde wijzigingen zijn voor de politie minstens zo belangrijk als de nieuwe bevoegdheid tot het op afstand binnendringen. Deze wijzigen maken het voor burgers, bedrijven en overheid eenvoudiger om aangifte te doen van deze vormen van criminaliteit, terwijl ook de opsporing en de bewijslast om uiteindelijk tot een veroordeling bij de rechter te kunnen komen wordt vergemakkelijkt.

De politie zal zich kleinschalig en landelijk voorbereiden op de zorgvuldige invoering van deze wetswijziging. Dit betekent onder andere dat de samenwerking zowel binnen de politie, als met haar partners, geïntensiveerd wordt met als doel de schaarse, specifieke digitale expertise en innovatie te bundelen en gezamenlijk verder te ontwikkelen. Daarnaast zal via zij-instroom expertise binnen worden gehaald die binnen de politie schaars is. Hiermee wordt ook uitvoering gegeven aan het fundamenteel verhogen van de kwaliteit van de opsporing zoals aangegeven in de countourennota Versterking Opsporing, die onlangs ook aan de vaste Kamercommissie is aangeboden.

Tot slot, de politie is blij met het voorliggende wetsvoorstel. Het geeft de politie handvatten die ze de afgelopen jaren heeft gemist in de bestrijding van de criminaliteit. Deze voorgestelde wetswijzigingen zorgen ervoor dat de politie ook in de gedigitaliseerde wereld recht kan doen aan haar motto “waakzaam en dienstbaar”.

Tweede Kamer der Staten-Generaal
Leden van de Vaste commissie voor Veiligheid en Justitie

bezoekadres
Kneuterdijk 1
2514 EM Den Haag

correspondentieadres
Postbus 90613
2509 LP Den Haag

t (070) 361 97 23
f (070) 361 97 15
www.rechtspraak.nl

datum 10 februari 2016
onderwerp Rondetafelgesprek Wetsvoorstel computercriminaliteit III 11 02 2016

De Raad voor de rechtspraak (de "**Raad**") dankt de Vaste commissie voor Veiligheid en Justitie voor de uitnodiging voor dit rondetafelgesprek. De Raad heeft ondergetekende gevraagd om vanuit mijn expertise als senior raadsheer in het Gerechtshof Den Haag, voorzitter van de zogeheten cyberkamer van dit hof en coördinator van het landelijke Kenniscentrum Cybercrime vanuit de Rechtspraak aan dit gesprek deel te nemen. Dit wil overigens – voor de goede orde – niet zeggen dat mijn bijdrage in zijn geheel per se overeenkomt met reeds door de Raad in het kader van zijn wettelijke adviseringsrol ingenomen formele standpunten.

Het wetsvoorstel computercriminaliteit-III heeft een lange voorgeschiedenis.[1] Gezien het feit dat het hier deels om nieuwe opsporingsbevoegdheden gaat die een vergaande inbreuk op grondrechten van burgers (verdachten of derden) opleveren kan daar begrip voor worden opgebracht. Hier dient immers grote zorgvuldigheid te worden betracht. De Raad constateert met genoegen dat in het voortraject niet alleen vele belanghebbenden zijn geraadpleegd, maar dat met die inbreng ook daadwerkelijk iets is gedaan. De Raad hecht daarbij in het bijzonder aan de aanpassingen ten opzichte van het concept-wetsvoorstel met betrekking tot het encryptiebevel en de verhoging van de drempel voor het mogen binnendringen in een geautomatiseerd werk en voor het ontoegankelijk maken van gegevens. Ook positief beoordeelt de Raad de vele juridische technische aanpassingen van het concept-wetsvoorstel, waardoor het thans voorliggende wetsvoorstel aan duidelijkheid en uitvoerbaarheid heeft gewonnen.

Hoewel de Raad op meerdere onderdelen van het wetsvoorstel nog de nodige juridische probleem- en vraagpunten ziet, zal ik mijn inbreng beperken tot twee punten, die thans als het meest zwaarwegend kunnen worden aangemerkt. Dat betreft allereerst het punt van de toetsing achteraf van de inzet van het opsporingsmiddel "binnendringen in een geautomatiseerd werk" (art. 126nba Sv). Het tweede punt betreft de problematiek van het extra-territoriaal inzetten van dit opsporingsmiddel.

1. **Toetsing achteraf van de inzet van het opsporingsmiddel "binnendringen in een geautomatiseerd werk" (art. 126nba Sv).**

In de systematiek van het wetsvoorstel zal, indien inzet van dit opsporingsmiddel wordt overwogen, daarvoor eerst door een officier van justitie binnen de hiërarchie van het Openbaar Ministerie bijzondere toestemming moeten worden verkregen. Indien deze toestemming is verkregen, zal de officier van justitie, alvorens een

[1] Zie ook de adviezen van de Raad van 30 september 2010, 4 juli 2013 en 10 oktober 2014, alle gepubliceerd op www.rechtspraak.nl.

bevel te kunnen geven dit middel ook in te zetten, daarvoor tevens de machtiging behoeven van de rechter-commissaris in strafzaken. Deze zal daartoe het verzoek van de officier van justitie toetsen op rechtmatigheid, proportionaliteit en subsidiariteit. Indien de rechter-commissaris van mening is dat aan deze eisen is voldaan, zal de machtiging worden verleend.

Graag vraag ik er aandacht voor dat dit slechts een toetsing *vooraf* op de inzet van het opsporingsmiddel is, waarbij de rechter-commissaris bij zijn beoordeling bovendien volledig afhankelijk is van de juistheid en de omvang van de informatie die hem vanuit de politie en de officier van justitie wordt verstrekt. Indien geen verlenging wordt gevraagd, zal de rechter-commissaris ook geen zicht (kunnen) hebben op de wijze waarop met de eerder door hem verstrekte machtiging is omgegaan. De oorspronkelijke gedachte achter het Wetboek van Strafvordering was en is daarbij dat de inzet van deze opsporingsmiddelen vervolgens ook achteraf kan worden (of in ieder geval zou kunnen worden) getoetst door de zittingsrechter. Het volledige dossier behoort dan beschikbaar te zijn, en ingevolge het systeem van checks en balances kan de verdediging dan ook andere informatie aandragen dan die welke reeds in het dossier aanwezig is.

Het is echter juist een kenmerk van met name zaken welke zich in cyberspace afspelen, dat het veelal wel mogelijk blijkt de datastroom te volgen, maar dat het buitengewoon moeilijk blijkt daaraan ook individuele verdachten te koppelen. Dat kan zijn omdat zij zich achter anonimiteit verschuilen, maar ook omdat zij zich feitelijk bevinden in landen die geen medewerking verlenen aan het onderzoek of die verdachten niet uitleveren. In deze gevallen, maar ook in andere gevallen, waarin uiteindelijk niet tot een vervolging (in Nederland) wordt besloten, zal derhalve geen toetsing *achteraf* van de inzet van de digitale binnendringingsbevoegdheid meer plaatsvinden. Gezien de impact die de inzet van dit middel kan hebben en de maatschappelijke risico's die kunnen ontstaan indien opsporingsdiensten zulke vergaande middelen kunnen inzetten zonder dat deze inzet achteraf nog wordt gecontroleerd/getoetst, wordt aan het - waarschijnlijk in een aanzienlijk aantal gevallen - ontbreken van de rechterlijke toetsing achteraf in (de Memorie van Toelichting bij) het wetsvoorstel ten onrechte geen aandacht besteed.

Ik kan me voorstellen dat nader wordt onderzocht in hoeverre in deze lacune zou kunnen worden voorzien door het instellen van een Commissie van Toezicht, vergelijkbaar met de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten. Een dergelijke commissie zou dan achteraf toezicht uit kunnen oefenen op de rechtmatigheid van de uitvoering van de bevoegdheid als genoemd in artikel 126nba Sv en daarvan (grotendeels) openbaar verslag kunnen doen. Voorwaarde zal dan wel moeten zijn dat zo'n commissie inzicht krijgt in alle gewenste gegevens.

2. De extra-territorialiteitsproblematiek

In de voorbereiding van dit wetsvoorstel, alsook in de Memorie van Toelichting is aandacht besteed aan de problematiek van de toepassing van de binnendringingsbevoegdheid in het geval de lokatie van het geautomatiseerde werk niet kan worden gelokaliseerd of dat geautomatiseerde werk zich in het buitenland bevindt. De Raad heeft over een eerdere versie van het wetsvoorstel al opgemerkt dat desondanks het wetsvoorstel geen duidelijke normen stelt ten aanzien van de gevallen waarin dan wel, dan wel niet, van deze bevoegdheid gebruikt zou mogen worden gemaakt, en dat is nog steeds niet het geval. De enkele verwijzing naar een inhoudelijk nog onbekende amvb, zoals thans voorzien in artikel 126nba, lid 8 Sv, of beschouwingen daaromtrent in de Memorie van Toelichting lijken in dit opzicht zowel vanuit rechtstatelijk als vanuit

internationaalrechtelijk perspectief voor de rechtspraktijk onvoldoende aanknopingspunten voor beoordeling te bieden. Ik acht het ook minder gewenst dat deze normering zal worden vormgegeven in een Aanwijzing danwel een amvb, zoals thans in de Memorie van Toelichting genoemd, reeds omdat niet goed valt in te zien hoe deze ook leidend zou kunnen zijn voor de onafhankelijke toetsing door de rechter(-commissaris).

Aandacht verdient het feit dat, zoals ook in het rapport van prof. Koops[2] is omschreven, thans nog geen internationaalrechtelijke basis lijkt te bestaan voor de inzet van deze bevoegdheid op buiten Nederland gelegen geautomatiseerde werken. Men kan zich hier de vraag stellen of de Memorie van Toelichting op dit punt niet meer een zeker justitieel wenselijkheidsdenken weergeeft dan de juridische en politieke realiteit. De Raad wees er in dit verband al op dat, anders dan de Memorie van Toelichting suggereert, bijvoorbeeld ook het Cybercrimeverdrag niet toestaat dat er grensoverschrijdend streaming data wordt “afgetapt”, welke mogelijkheid echter in het wetsvoorstel in art. 126nba, lid 1 onder d. Sv nadrukkelijk wel als een van de functionaliteiten van de binnendringingsbevoegdheid is opgenomen.

Ik wil er in dit verband ook aandacht voor vragen dat het zonder voldoende internationaal- rechtelijke basis inzetten van de binnendringingsbevoegdheid op buitenlandse geautomatiseerde werken ook risico’s oplevert voor het daarbij betrokken justitiële personeel. Zij zullen zich dan namelijk naar het recht van zeer vele landen schuldig maken aan het misdrijf van computervredebreuk, met alle gevolgen van dien. Die strafrechtelijke aansprakelijkheid kan zich ook uitstrekken tot de officier van justitie en de rechter-commissaris. Daarboven dringt zich de integriteitsvraag op of men van justitiële ambtenaren kan vragen gebruik te maken van een opsporingsmiddel dat – naar brede juridische opvatting – in zo’n geval niet rechtmatig mag worden ingezet.

Tot op zekere hoogte lijkt vanuit het internationale recht wel verdedigbaar dat in uitzonderlijke gevallen, waarin grote belangen op het spel staan, aan een staat een zeker zelfverdedigingsrecht toekomt, met name om aan een bedreiging feitelijk een einde te maken. In dit verband verdient het, zoals ook reeds door de NOvA naar voren gebracht, naar het oordeel van de Raad serieuze overweging of niet – naar Duits voorbeeld – in de wet moet worden vastgelegd dat toepassing van voormelde bevoegdheid, of van bepaalde onderdelen van die bevoegdheid, op geautomatiseerde systemen waarvan op enig moment blijkt dat zij zich in het buitenland bevinden slechts in bijzondere gevallen zal mogen plaatsvinden, namelijk die waarin sprake is van:
1) lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen of
2) van gemeen gevaar voor goederen, dat een bedreiging oplevert voor het voortbestaan van de staat of de mensheid.

Met vriendelijke groet,

Mr. Chr. A. Baardman
Senior raadsheer Gerechtshof Den Haag / Coördinator Kenniscentrum Cybercrime

[2] Zie B.J. Koops & M. Goodwin (2014), Cyberspace, the cloud, and cross-border criminal investigation.

Allereerst wil ik bij deze uw commissie hartelijk danken voor de uitnodiging om namens AMS-IX, de Amsterdam Internet Exchange, deel te nemen aan een rondetafelgesprek over het op 24 januari jl. bij de Tweede Kamer ingediende wetsvoorstel computercriminaliteit III. Het is al weer enige tijd geleden dat het oorspronkelijke voorstel ter consultatie werd gepubliceerd, dat was in mei 2013, en het is daarom opmerkelijk dat de definitieve versie door het kabinet is aangekondigd als onderdeel van een urgent actieprogramma "Integrale aanpak jihadisme".

Zoals u wellicht weet bestaat het internet uit tienduizenden onafhankelijk van elkaar gemanagede IP-netwerken. De rol van AMS-IX is het faciliteren van interconnectiviteit tussen dergelijke netwerken. Daartoe beheren we een gedistribueerd platform in de Amsterdamse regio, welke bestaat uit volledig redundant met elkaar verbonden apparatuur in 11 verschillende datacenters. Partijen als ISP's en contentleveranciers kunnen daarop aansluiten om met elkaar verkeer uit te wisselen wanneer dat in beider belang is. Als zodanig is het AMS-IX platform een belangrijk, weliswaar enigszins verborgen, onderdeel van de technische internetinfrastructuur.

AMS-IX is een vereniging zonder winstoogmerk, en inmiddels zijn meer dan 750 netwerken aangesloten waarvan driekwart uit het buitenland afkomstig is. De laatsten komen specifiek naar Nederland om hier onderling zaken te doen, en met recht kun je dus spreken van een internationaal internetknooppunt: in termen van aangesloten partijen is AMS-IX wereldwijd zelfs de grootste in haar soort. Het is het hart van de Nederlandse digitale infrastructuur, door uw Kamer vorig jaar erkend als de 'derde mainport'. De focus van beleidsmakers op een open, neutraal, veilig en vrij internet, waarbij rechten van eindgebruikers, eerlijke concurrentie en innovatie voorop stonden, heeft mede bijgedragen aan dit succes. De economische belangen voor Nederland zijn onmiskenbaar, en het vertrouwen, zowel voor bedrijven als eindgebruikers, in de diensten die via het internet geleverd worden, is essentieel om onze internationale koppositie te behouden en ook om in de toekomst de vruchten te plukken van de kansen die de sector te bieden heeft. We zijn dan ook blij dat dit de insteek is van het Ministerie van Economische Zaken, naast het werk dat het Ministerie van Buitenlandse Zaken verricht om andere staten te overtuigen van het belang van een vrij, veilig en open internet.

AMS-IX is een neutrale, geheel onafhankelijke facilitator, en fungeert niet als spreekbuis namens de bij haar aangesloten partijen. Zoals uit het hieraan voorafgaande mag blijken, zijn de economische belangen echter zodanig groot en sector overstijgend, dat wij u ondanks onze neutrale positie graag van input voorzien. Als deelnemer in de stichting Digitale Infrastructuur Nederland (DINL) hebben we samen met een groot aantal andere betrokkenen uit de sector in mei 2015 onze zorgen geuit met betrekking tot de voornemens zoals omschreven in het indertijd ter consultatie geformuleerde voorstel. We zijn content met een aantal aanpassingen die in de laatste versie zijn terechtgekomen, zoals het enkel medewerking moeten verlenen aan een decryptiebevel bij verdenking van bepaalde zeer ernstige strafbare feiten en het strafbaarstellen van heling in computergegevens. In de kern zijn onze zorgen echter ongewijzigd.

Drie punten die ik hier wil aankaarten zijn: wat is eigenlijk de nut en noodzaak van de 'hackbevoegdheid' voor opsporing, oftewel is deze proportioneel? Hoe verhoudt de mogelijke inzet ervan zich tot andere wettelijke verplichtingen voor marktpartijen? En tot slot het essentiële punt dat het gebruik van zwakheden ten behoeve van het heimelijk binnentreden in geautomatiseerde werken het internet minder veilig maakt.

1. Overwegingen in de bij het wetsvoorstel horende Memorie van Toelichting (MvT) om de nieuwe bevoegdheid met betrekking tot het heimelijk binnendringen van een geautomatiseerd werk te motiveren, zijn vooral praktisch van aard:
   - internationale rechtshulpverzoeken zouden te traag verlopen;
   - wanneer data versleuteld is dan levert een tap niets op;

- nieuwe spelers in het veld vallen niet onder de Telecomwet en hoeven niet aan de tapplicht te voldoen;
- het gebruik van clouddiensten levert complicaties op voor opsporing;
- het uitzetten van een tap bij een openbare aanbieder is weinig effectief wanneer een verdachte (vaak) wisselt van (draadloos) netwerk.

Natuurlijk is er alom begrip, ook binnen onze sector, voor een veranderde omgeving en de uitdagingen waar opsporingsdiensten heden ten dage voor staan. Maar wat ons betreft is dit onvoldoende om de noodzakelijkheid en proportionaliteit van de nieuwe 'hackbevoegdheid' te onderbouwen. Potentiële negatieve gevolgen zijn immers verstrekkend: zowel in termen van de inbreuk op fundamentele rechten alsook als het gaat om de economische schade vanwege het schenden van vertrouwen. Het kan toch niet een kwestie zijn van: hacken in zowel binnen- als buitenland door onze opsporingsdiensten is technisch mogelijk, het werkt sneller en is relatief goedkoop, het maakt het leven voor de diensten makkelijker, en dus moeten we het kunnen en willen doen.

2. Partijen in de sector worden reeds aan een wettelijke zorgplicht onderworpen, en bestaande wet- en regelgeving wordt aangepast om tevens nieuwe spelers die buiten de traditionele wettelijke telecom-kaders vallen te reguleren. Het borgen van de veiligheid en integriteit van informatiesystemen, alsmede de daarmee samenhangende continuïteit van dienstverlening, ook vanwege vitale Nederlandse belangen, staan in deze context voorop. Tegelijkertijd zitten we nu aan tafel om de mogelijkheid te bespreken voor opsporingsdiensten om heimelijk toe te treden tot automatische werken die veelal beheerd worden door dezelfde private sector. Diensten zullen dus baat hebben bij het bestaan van kwetsbaarheden en onveiligheden, terwijl markpartijen er gelijktijdig alles aan moeten doen deze te vermijden en daarover dienen te rapporteren. Deze twee conflicterende overheidsmotieven zijn wat AMS-IX betreft niet met elkaar te rijmen.

3. Om heimelijk binnen te komen in een geautomatiseerd werk zijn per definitie zwakheden nodig. Zodra deze lekken zijn verholpen is dat binnentreden namelijk niet meer mogelijk. Wil een opsporingsambtenaar kunnen hacken in een systeem dan zijn zogenaamde 'zero-day vulnerabilities' nodig, ofwel andere kwetsbaarheden die nog niet publiek bekend zijn en nog niet door een leverancier zijn gerepareerd. Niet alleen zal men op zoek moeten gaan naar dergelijke lekken om ze te kunnen gebruiken, bijvoorbeeld door kennis daarover aan te schaffen, al dan niet via een derde. Ernstiger is dat de kwetsbaarheden voor iedereen beschikbaar zijn en blijven. Niet alleen voor onze opsporingsdiensten, maar ook voor twijfelachtige buitenlandse regimes, criminelen en organisaties die bedrijfsspionage willen plegen. En niet alleen de verdachte in kwestie, maar iedereen die gebruik maakt van betreffende (lekke) software is en blijft kwetsbaar. Bovendien kun je, wanneer Nederland het zelf ook doet, buitenlandse mogendheden er niet op aanspreken als zij, buiten hun eigen landsgrenzen, in Nederland heimelijk in geautomatiseerde werken binnentreden. Al met al wordt op deze manier een structurele bijdrage geleverd aan een onveiliger internet, en dat is wat AMS-IX betreft zeer ongewenst.

Bedrijven als Hacking Team leveren forensische tools om in te kunnen breken op systemen, en uit op wikileaks gelekte correspondentie[1] blijkt dat de Nederlandse politie daarover in contact is geweest met deze buitenlandse leverancier. Die overigens zelf recentelijk gehackt is. Als Nederland besluit tot aanschaf van dergelijke tools over te gaan, dan betekent het dat onze overheid financieel bijdraagt en indirect verantwoordelijk is voor het in standhouden van een ecosysteem dat handelt in software-kwetsbaarheden. Dit moeten we niet willen.

[1] https://wikileaks.org/hackingteam/emails/emailid/11256

Staatssecretaris Dijkhoff heeft na het AO met uw commissie op 20 januari jl. toegezegd om met een brief te komen namens het kabinet over het gebruik en het mogelijke aanschaffen van 'zero day exploits' door verschillende diensten. Ik ben zeer benieuwd waar het kabinet mee komt, en met name of dan ook verwezen gaat worden naar de eventuele aanschaf van tools bij derde partijen. In strikte zin zou met gebruik van een dergelijke tool de overheid zich namelijk niet zelf begeven op de markt voor 'zero day exploits' en andere kwetsbaarheden, maar het resultaat, ook in moreel opzicht, is natuurlijk hetzelfde: een industrie wordt in stand gehouden met als gevolg het minder snel dichten van lekken met een bijkomende onveiligheid op het internet.

U heeft ongetwijfeld kennisgenomen van het in april 2015 verschenen rapport van de WRR 'De publieke kern van het internet'. Het wachten is nog op een formele kabinetsreactie met betrekking tot deze studie, maar momenteel werkt het Ministerie van Buitenlandse Zaken aan een diplomatieke internetstrategie waarin de belangrijkste aanbevelingen van de WRR lijken te worden overgenomen. Ook stuurt men de belangrijkste auteur van het rapport alvast proactief op pad om in het buitenland de belangrijkste conclusies te promoten: namelijk dat Nederland ervoor moet pleiten dat er een zogenaamde kern van internetprotocollen en -infrastructuur is, welke te beschouwen moet worden als een publiek goed. En omdat voor Nederland het internet een grote sociaaleconomische betekenis heeft, is het van belang het functioneren en de integriteit van die publieke kern van het internet veilig te stellen en deze te beschermen tegen oneigenlijke interventies door staten en andere partijen. Een diplomatieke boodschap, aldus de WRR, die zich niet lijkt te verhouden tot de hackbevoegdheid voor opsporingsdiensten die nu voorgesteld wordt. Daar is AMS-IX het mee eens.

Ook al betreft het volgens de MvT een 'introduceren van een nieuwe bevoegdheid om, onder strikte voorwaarden, een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk te kunnen binnen dringen in het kader van de opsporing van ernstige strafbare feiten', feit blijft dat bij inzet van die bevoegdheid van zwakheden gebruikt zal moeten worden, en dat er dus een prikkel gecreëerd wordt om deze daadwerkelijk te gebruiken, ze te laten bestaan, ze niet publiek te maken, zodat ze niet worden gerepareerd. Deze houding lijkt haaks te staan op de rol die Nederland voor zichzelf ziet als aanjager van cyberdiplomatie. Als gastheer van de Global Conference on Cyber Space toonde Nederland zich vorig jaar een groot voorstander van internationale samenwerking bij de bestrijding van cybercrime. Dat is ook de lijn op dit moment van Nederland als voorzitter van de Europese Unie. Laten we vooral die lijn vasthouden en ons richten op een gezamenlijke aanpak: zowel met het bedrijfsleven, dat wil zeggen de sector, als met het buitenland. En in dat laatste geval valt er heel wat te winnen met het beter delen van informatie en het versnellen van procedures als rechtshulpverzoeken.

Bastiaan Goslings, AMS-IX regulatory officer

bastiaan.goslings@ams-ix.net

NEDERLAND ICT

Allereerst wil ik bij deze uw commissie hartelijk danken voor de uitnodiging om namens Nederland ICT te spreken bij een rondetafelgesprek over het wetsvoorstel computercriminaliteit III. Nederland ICT is een voorstander om computercriminaliteit aan te pakken en begrijpt dan ook de wens van de overheid om nieuwe bevoegdheden te introduceren in de wet Computercriminaliteit III. Echter Nederland ICT vraagt zich wel af of in de nieuwe wet de juiste balans is gezocht tussen collectieve veiligheid en individuele vrijheden, of de wet Nederland niet kwetsbaarder maakt in plaats van veiliger, of niet een onevenredig grote inbreuk op de grondrechten wordt gemaakt en of de wet geen enorme economische schade gaat toebrengen.

Ten opzichte van de concept versie uit 2013(!) is er een aantal verbeteringen aangebracht: de verplichting tot ontsleuteling is er uit, waardoor je niet meer hoeft mee te werken aan je eigen veroordeling. Ook is het positief dat helers van computergegevens strafbaar worden gesteld, waardoor hackers die bijvoorbeeld buitgemaakte persoonsgegevens willen verhandelen strafbaar gesteld kunnen worden. Echter met de Wet Computercriminaliteit III introduceert het kabinet ook een nieuwe bevoegdheid: het heimelijk binnendringen van een geautomatiseerd werk. Dit betekent concreet het mogen hacken van apparatuur zoals computers en mobiele telefoons, maar ook het hacken van clouds en slimme energiemeters valt onder de bevoegdheid. Nederland ICT vindt het onwenselijk wanneer de politie dit middel mag inzetten. Het verhogen van de de strafmaat naar een minimale celstraf van 8 jaar doet daar niets aan af. Ik leg u graag uit waarom.

Nederland heeft nu een zeer sterke positie op het gebied van internet. We waren nauw betrokken bij de totstandkoming van het internet en worden internationaal nog steeds gezien als autoriteit op het gebied van internet governance en voorvechter van een vrij en open internet. Met heldere standpunten op het gebied van netneutraliteit en recent nog encryptie gooit Nederland internationaal gezien hoge ogen. Het vestigingsklimaat is goed en er ontstaan op het moment allerlei veelbelovende startups. We hebben deze sterke positie te danken aan het feit dat de bevolking hoog opgeleid is, praktisch iedereen voorzien is van snelle vaste en mobiele internetverbindingen en Nederland met AMS-IX de beschikking heeft over één van de grootste internetknooppunten ter wereld. Recente investeringen van grote bedrijven als Google, IBM en Microsoft en het flinke aantal techstartups onderschrijven de sterke positie van Nederland en het vertrouwen dat bestaat in de Nederlandse internet en technologiesector. Hierdoor heeft Nederland de potentie om proeftuin voor nieuwe ICT-toepassingen te worden.

Echter vertrouwen in ICT is essentieel om deze positie te behouden: vertrouwen dat niemand meeleest met de communicatie, vertrouwen dat diegene met wie je communiceert ook daadwerkelijk is wie hij of zij zegt. Vertrouwen dat je data vertrouwelijk blijft en niet op straat komt te liggen en tenslotte het vertrouwen dat de diensten en apparaten waar je gebruik van maakt betrouwbaar zijn. Nederland ICT vindt de bevoegdheid om te hacken schadelijk voor dit vertrouwen omdat de wet leidt tot het stimuleren van een industrie van “politie gereedschappen” die er belang bij heeft kwetsbaarheden geheim te houden in plaats van te openbaren. Daarbij komt dat met het gebruik van dergelijke gereedschappen door de complexiteit van ICT-producten en diensten schade aangericht kan worden aan onschuldige omstanders. Dit kan al optreden bij het binnendringen, maar zeker ook bij het plaatsen van “policeware” of het op andere wijzen ingrijpen in geautomatiseerde werken. Ook heeft de hackbevoegdheid een ongewenstneveneffect omdat de politie niet alle kennis in huis heeft. Op deze manier houdt de Nederlandse overheid het bestaan van een zwarte markt van kwetsbaarheden in stand, die het met de wetgeving computercriminaliteit juist wil tegengaan.
Nederland ICT ziet een groeiend spanningsveld tussen een hackbevoegdheid waardoor digitale systemen worden verzwakt, tegenover dezelfde overheid die niet alleen een publiek private samenwerking in het cyberdomein stimuleert, maar ook bedrijven verplicht kwetsbaarheden te

melden in verschillende meldplichten, de Telecomwet of de Europese NIB-richtlijn. Het ene onderdeel van VenJ (NCSC) lijkt zo de strijdt aan te gaan met het andere onderdeel (NP).

De hack bij het Italiaanse Hackingteam vorige zomer, een bedrijf dat handelt in onder meer (zero-day) exploits, liet zien dat de Nederlandse politie alvast kennis kwam ophalen vooruitlopend op computercriminaliteit III. Het antwoord van de overheid na Kamervragen, in augustus 2015, baart Nederland ICT grote zorgen hoe open en transparant de politie zal zijn wanneer zij daadwerkelijk de bevoegdheid tot hacken krijgt. Ik citeer: “dat het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico’s met zich meebrengt voor de inzetbaarheid van die middelen.” Wij vragen dan ook: Kan de overheid garanderen dat ze de gemelde zwakheden niet gebruikt voor offensieve doeleinden? Kan de overheid garanderen dat het Nederlandse bedrijfsleven geen schade gaat ondervinden door de inzet van kwetsbaarheden? Gaat de overheid transparant zijn over het gebruik en de kosten van de hackbevoegdheid? Nog los van de vraag of de Nederlandse overheid überhaupt een dergelijk systeem waarbij bedrijven die handelen in veiligheidlekken zou moeten willen ondersteunen. Een verbod op het gebruik van zogenaamde zero-days exploits zou Nederland ICT dan ook zeer wenselijk vinden.

Ook vindt Nederland ICT het gebruik van technische kwetsbaarheden om binnen te dringen in geautomatiseerde werken door opsporingsinstanties zich niet verstaan met de vrijheden en de bescherming van de persoonlijke levenssfeer van niet-verdachten en omstanders. Het in standhouden en uitnutten van technische kwetsbaarheden is niet in het belang van een veilige en beschermde persoonlijke levenssfeer van burgers. Hoge eisen zullen dan ook gesteld moeten worden aan het specifiek inkaderen van een onderzoek. Met name van data die is opgeslagen in de cloud bestaat het risico dat in een onderzoek uiteindelijk data van veel meer partijen wordt meegenomen. Het zoeken in specifieke datasets zal dan ook zo specifiek mogelijk omschreven moeten worden zijn. Ook moeten we ons realiseren dat voor internationale ICT bedrijven wiens cloud zich onder meer in Nederland bevindt, de wet computercriminaliteit te weinig waarborgen omvat. Want hoe ‘integer’ is hun cloud wanneer de Nederlandse politie mag hacken? Hoe kunnen ze dit hun klanten garanderen? Dit soort onzekerheden waarbij er een disbalans lijkt te ontstaan tussen veiligheid en waarborgen is slecht voor het Nederlandse investeringsklimaat. Ook is Nederland ICT uitermate kritisch op de bevoegdheid om te hacken in het buitenland. In de memorie van toelichting is te lezen dat wanneer het geautomatiseerde werk zich in het buitenland bevindt een rechtshulpverzoek kan worden gedaan, behoudens uitzonderlijke omstandigheden. Vervolgens lezen we dat een verzoek aan een buitenlandse aanbieder tot het vertrekken van informatie over hun klant maar een beperkte kans van slagen heeft bij en ook nog vaak veel tijd kost. Is dit afdoende reden om zo’n zwaar middel in te zetten? Wij vinden van niet. Nederland ICT vindt dat de internationaal rechtelijke processen gevolgd moeten worden (bijstandsverzoeken vreemde overheden). En Nederland ICT is een groot pleitbezorger van samenwerking tussen politie en ICT-bedrijven, ook in internationaal verband.

Nederland ICT vraagt dan ook een grote betrokkenheid vanuit de politiek. De politiek dient kritisch te kijken naar de noodzaak van vergaande verruiming van de bevoegdheden voor de politie. Er is een spanningsveld tussen vrijheid en veiligheid, tussen Veiligheid en Justitie. Willen we in Nederland een publiek-private samenwerking op gang brengen zoals het Nationaal Cyber Security Centrum die voorstaat of willen we een overheid die er gebaat bij is kwetsbaarheden in stand te houden? Willen we een overheid die enerzijds pleit voor internationale samenwerking in het cyberdomein, om vervolgens op eigen houtje in te breken op systemen in het buitenland?. Het is nu aan de Tweede Kamer om te kiezen tussen deze twee gezichten.

Liesbeth Holterman, Nederland ICT

Wie onthult mijn geheimen?’ - over encryptie en hacken

10 februari 2016

VIDEO: http://www.ru.nl/cpo/cursussen/kennisclips/?reload=true

Het versleutelen van berichten is met de huidige technologie mogelijk. Maar mag u in het licht van allerlei wetgeving eigenlijk wel zo'n perfecte brandkast hebben? Dat alleen u de sleutel hebt en niemand anders deze berichten kan openen? Hebt u daar recht op, dan zullen de AIVD, politie en belastingdienst dat niet leuk vinden. Is dat niet het geval dan rijst meteen de vraag wie de tweede sleutel dan mag gebruiken: de provider, de overheid of een andere derde partij? En hoe zit het met de schade als er een 'achterluikje' wordt ontdekt? Denk bijvoorbeeld aan de zogenaamde onkraakbare ov-chip en autochips.

In deze kennisclip vertellen prof. mr. Ybo Buruma, CPO-hoogleraar Rechtsstaat, rechtsvorming en democratie (Radboud Universiteit) en prof. dr. Bart Jacobs, hoogleraar Computerbeveiliging (Radboud Universiteit) voor welke uitdagingen het kabinet staat. Op 4 januari 2016 verscheen een brief van de minister over ‘achterluikjes’. Deze brief, samen met het wetsontwerp Computercriminaliteit III, vormen mede de aanleiding voor deze kennisclip.

Verslag van de rondetafeldiscussie over het wetsvoorstel Computercriminaliteit III

Kamerleden:
PvdA Voorzitter L. Ypma,
PVV L.M.J.S. Helder,
PvdA J. Recourt,
SP S.M.J.G. Gesthuizen,
VVD O.C. Tellegen,
D66 K. Verhoeven,
CDA M.M. van Toorenburg,
PvdA Astrid Oosenbrug

Alle deelnemers is gevraagd een position paper in te dienen. Die zijn gepubliceerd op http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2016A00399

Blok 1: Privacy - 10.00 tot 10.40 uur

9 Bits of Freedom
9 de Universiteit van Amsterdam
9 Autoriteit Persoonsgegevens

Introductie standpunten:
14 van Bits of Freedom noemt de standpunten zoals eerder verwoord in het position paper. De noodzaak is onvoldoende aangetoond. Ze willen dat het besluit technische hulpmiddelen eerst wordt vernieuwd. Ze vinden dat de groep te hacken apparaten te breed is. Er zou ook niet zo vaak mogen gehackt. Het is zo zwaar dat het niet uit efficiëntie overwegingen zou mogen worden ingezet. Tenslotte willen ze dat er een onafhankelijke toetsingscommissie komt.

14 Hij signaleert dat Europese jurisprudentie telkens aangeeft dat er steeds zwaktes zitten in wetgeving. Dit met name door ontbreken van toezicht en randvoorwaarden die waarborgen bieden tegen misbruik. Transparantie is daarbij ook van belang.

14 van de Autoriteit Persoonsgegevens. Hij vindt het nieuwe voorstel al veel beter dan de vorige versie. Maar er zijn privacy problemen. Het kijken in de computer van een persoon, betekent ook het doorzoeken van gegevens van derden. Het leidt mogelijk tot anticiperend computer gebruik, de burger voelt zich niet vrij. Aanvullende waarborgen zijn vereist. Het is de vraag of de RC hier voldoende voor geëquipeerd is. Zij zouden gespecialiseerd moeten zijn. Daarnaast is hij voorstander van systematisch toezicht. Dat zou heel goed bij de AP kunnen liggen. Want zij houden ook toezicht op andere politie activiteiten. Het zou zonde zijn daar een andere club voor in het leven te roepen. Een horizonbepaling zou moeten worden opgenomen.

De vragen:
D66 Kamerlid Verhoeven. Aan 14 : Gebruik van kwetsbaarheden in software om te kunnen hacken. Wat betekent dat voor de alledaagse burger. Aan 14 toelichting op dat aanbod om het toezicht op zich te nemen.
Mevrouw Helder. Stelt nog even geen vragen.
De heer Recourt PvdA. 14 Jurisprudentie uit Straatsburg zou in strijd zijn met wetgeving uit Den Haag. Graag een toelichting.

Mevrouw Oosenbrug. Hoe beschermen we de privacy van de burger. En is dat wel mogelijk in deze wet. Voor[14]
Mevrouw Gesthuizen SP. Voor [14] Zou de wet stand houden voor het Europees Hof.[14] vindt hij dat de AP voldoende kennis in huis heeft om dergelijk toezicht uit te oefenen.
Tellingen van de VVD. Aan[14] onderschrijft u de noodzaak voor een wet die computercriminaliteit aanpakt en hoe dan. En u zegt dat u de wet alleen zou willen toepassen in geval van levensbedreigende situaties, maar hoe kan dat samengaan met toetsing vooraf.

De antwoorden:
[14] wil met name dat we eerst beter gaan samenwerken en andere oplossingen bedenken.

[14] Deze bevoegdheid heeft een chilling effect op de samenleving. Het kan ongewenste consequenties hebben. Het is belangrijk dat daar zicht en toezicht op is. Het Europees hof toetst voortdurend of de proportionaliteitstoets heeft plaatsgevonden. Er is ook veel aandacht voor “meaningful toezicht”, tegenspraak. Geen toezicht middels een stempelmachine. Nut, noodzaak en effectiviteit moet worden gecontroleerd. Dit creëert legitimiteit. Geen fishing expeditions / sleepnetten, maar goed toepassen van bevoegdheden. Hij waarschuwt ook voor de mogelijkheid van false positives.

[14] Geeft aan dat [13] [13] anders kunnen worden neergelegd? Er is geen andere instantie. Dan de vraag over opsporing vs privacy. Het woord proportionaliteit geeft al aan dat het een balans is, geen tegenstelling. Je moet focussen op waarborgen, zoals het toezicht. In het voorstel moet hier meer aandacht voor komen. Ook toetsing achteraf is nodig. De RC doet een heel concrete toets in een casus en op basis van wat de officier op dat moment zegt en weet. Je moet ook achteraf kijken of men zich aan de wet heeft gehouden. Als er geen verlenging wordt gevraagd en de zaak komt niet voor de rechter dan wordt er nu niet getoetst.

Blok 2: Praktijk – 10.40 tot 11.50 uur
- [9] Openbaar Ministerie
- [9], Nationale Politie
- [9] Nationaal Cyber Security Centrum
- [9] Raad voor de rechtspraak
- [9], Nederlandse Orde van Advocaten

De introductie:
[14] Hij beschrijft de toename van cybercriminaliteit. Dat levert problemen op voor opsporing, maar ook voor burgers en hun vertrouwen in de overheid. Bijvoorbeeld [7-12] [7-12], maar ook encryptie en afscherming. Dat is ook buiten cybercriminaliteit een probleem. Het moet bestaande bevoegdheden weer efficiënt maken, die dat nu niet altijd meer zijn. Tappen, OVC etc zijn opsporingsmethodes die nu ook mogen worden ingezet, maar kunnen worden tegengegaan. Het OM en de politie vragen niet om encryptie tegen te gaan, of beveiliging te verzwakken. De inzet die wij vragen gaat ook niet allemaal om zero-days waarmee je computers kunt binnendringen. Maar juist ook om het

kunnen inloggen met credentials die wij rechtmatig hebben verkregen (bv uit een tap of van een briefje).
Het gaat alleen om een inbreuk op de privacy van verdachten, niet om onschuldige burgers. Wiens privacy is voor u van belang? Cybercriminelen schenden de privacy van mensen op allerlei manieren. De slachtoffers hebben ook recht op privacy. Meer dan de verdachte.

Inge Philips van de politie. Zij noemt dat er meer in het voorstel staat dan alleen binnentreden. En dat het herstelwetgeving is. Er zijn drie problemen. Anonimiteit, zoals op het tor netwerk is een nieuw probleem. Zij noemt de casus waarin verdachte kortsluiting veroorzaakte waardoor zijn laptop uitging, en het bewijs weg was.
De politie is voorstander van sterke crypto, wij willen geen achterdeurtjes, wij willen dat het veiliger wordt. Wij maken inbreuk op de grondrechten van verdachten. Proportioneel en met toestemming. Encryptie is een ander probleem. Wij kunnen deze alleen omzeilen door naar de bron te gaan, en waar te nemen op het moment voor er encryptie is toegepast.
Wij grasduinen niet, wij neuzen niet rond. Wij zijn geen inlichtingendienst. Het is ook geen hacken, maar digitaal rechercheren met alle waarborgen en toetsing die daarmee samenhangt (hashen, normen, verbaliseren). Het is een precies middel.
Wij zijn de strijd aan het verliezen, zonder de bevoegdheid gaan wij de achterstand niet inhalen.

14 Hij zit hier eigenlijk in een andere hoedanigheid dan de andere genodigden. Zij doen niet aan opsporing. 14 constateert dat cybercriminaliteit en digitale spionage enorm toeneemt. Criminelen worden steeds vaardiger. Dit is ook te lezen in hun criminaliteitsbeeld.

14 Hij is blij dat er aanpassingen zijn gedaan in het voorstel. Benadrukt vooral dat toetsing achteraf erg belangrijk is. De RC is volledig afhankelijk van informatie vooraf van de officier. Maar hij hoort niet hoe het gegaan is. Op zitting kunnen alleen personen verschijnen. Maar als de verdachte niet is gevonden, gebeurt dat niet. Dat zal ook vaak zo zijn na de inzet van deze bevoegdheid. Dat moet wel worden onderzocht.
Het tweede punt is de rechtsmacht. Waar ligt de grens wanneer je niet weet waar de computers staan. Die normen staan niet duidelijk in het voorstel. Koops heeft geschreven dat er juridisch nog geen ruimte is om dit binnentreden in het buitenland te doen. Er wordt verwezen naar bevoegdheden van Duitsland België en Frankrijk. Het zou kunnen dat het invoeren van deze bevoegdheid in Nederland een aanzuigende werking heeft voor rechtshulpverzoeken vanuit landen waar minder mag.

14 Het is altijd lastig als de overheid zichzelf een bevoegdheid geeft om strafbare feiten te plegen. Daar zijn waarborgen voor nodig. Voor de lichte vorm van “hacken” is een strafbaar feit waar een jaar op staat voldoende. Dat is niet proportioneel. Want als het mag, dan gebeurt het ook. 126zpa hoeft niet tegen verdachte te worden ingezet, maar tegen elke persoon. En wat doen we met mede gebruikers van de gehackte computer? En de mensen die ten onrechte verdacht waren? Dan wordt er niet getoetst. Maar burgers op wiens grondrecht een inbreuk is gemaakt, moeten een “effective remedy” hebben. Notificatie is niet goed genoeg. Waarom niet een lijst van IMEI nrs en IP-adressen in de Staatscourant publiceren?

De vragen:

Meneer Verhoeven. [14] Het noemen van ontwikkelingen onderbouwt niet waarom deze bevoegdheid noodzakelijk is. De politie hackt niet, we hebben niet altijd zero-days nodig etc. Maar gaat u geen kwetsbaarheden gebruiken en inkopen, heel concreet.
Mevrouw Helder. De privacy van de burger is hier in het geding. Gaat u nu kijken in de systemen van niet verdachten? Hoe voorkomt u dat? U zegt dat u niet gaat grasduinen.
Recourt. De integriteit van internet is heel belangrijk. Hoe voorkomen we dat andere landen bij ons in de data centra willen rondkijken.
Oosenbrug. Ik vind dat de inbreuk door het doorkijken van foto's van allerlei mensen heel ver gaat. Ze maakt zich zorgen over proportionaliteit.
Gesthuizen. .. [vraag gemist]
Tellegen. Het lijkt voor de kamer de keuze tussen privacy en veiligheid te zijn. Terwijl het gaat om het bestrijden van computercriminaliteit. [14] ziet u de noodzaak van deze wet dan niet.
Mevr Toornburg wil weten of het decryptie bevel niet toch nodig is.

De antwoorden:
[14] Ziet het nut voor de opsporing. De noodzaak is een politieke afweging. Maar het is belangrijk dat het een muizengaatje blijft. Bijvoorbeeld door te beperken tot het systeem waarmee het strafbare feit is gepleegd. En niet dat het ieder systeem kan zijn. Dat moet je nu inkaderen.

[14] Wij werken samen met iedereen. Van Bits of Freedom tot de politie.

[14] De politie wil ook dat nauw omschreven is wat mag. Het is niet prettig te acteren in een strafrechtelijk vacuüm. Dat is vervelend omdat we dan altijd aan de veilige kant gaan zitten. Criminelen bedienen zich van allerlei methodes, ook verboden. Wij mikken erop chirurgisch in te grijpen en zo precies mogelijk bij bewijs komen. Of om een interventie te plegen, bv in geval van een ontvoering of terreur.
Welke computer dat is maakt ons niet uit, het systeem wat nodig is om bij die informatie te komen. We kunnen niet werken met dat de computer van verdachte moet zijn. Wij hechten aan goede verslaglegging in een proces verbaal. In een huis tijdens een doorzoeking gaat alles overhoop, maar in de digitale wereld kunnen we juist heel precies en goed zoeken.
Hoe doen we dat dan? Middels functie scheiding, dat is heel belangrijk. Het zal nooit worden uitegvoerd door iemand van het team. We doen uitvoerig vooronderzoek en leggen over elke stap verantwoording af. Over de vraag of wij kwetsbaarheden gaan gebruiken, natuurlijk gaan wij dat doen. Nieuwe kwetsbaarheden die we vinden worden gewoon gemeld bij de NCSC. Het kan zijn dat we het eerst gebruiken. Wij gaan het niet inbouwen, of achterdeurtjes vragen.

[14] over het decryptie bevel. Daar was het openbaar ministerie geen voorstander van. Het ligt op te gespannen voet met de rechten van verdachte. Het gaat erom dat we effectief moeten kunnen optreden. Het wordt niet minder veilig door de politie. Het gaat vooral om bekende kwetsbaarheden waar al updates voor beschikbaar zijn. Verdachte kan zijn systemen updaten, maar als hij dat niet doet dan zouden we het kunnen gebruiken. We gaan in ieder geval geen rol spelen in het tegenhouden van de miljarden industrie van beveiligingsbedrijven.
Over de onderbouwing. In de memorie staat al veel genoemd. We kunnen vaak de persoon en het geautomatiseerd werk niet vinden. We willen terrein terugwinnen wat we hebben verloren. We zouden veel verder kunnen gaan, maar ik denk dat er een balans zit in dit wetsvoorstel.

We gaan de bevoegdheid niet inzetten voor allerlei lichte delicten. Dat is niet proportioneel. We gebruiken ook al jaren OVC, dat doen we ook weinig en welbepaald. We doen dat bv ook niet in de slaapkamer. Ondanks dat dat wettelijk mag.

Vragen tweede ronde:
Torenburg snapt niet dat het OM ineens geen decryptie bevel wil.
Recourt: moet de reikwijdte niet kleiner.
Verhoeven: We zijn ook wereldkampioen telefoontappen. Dus is het belangrijk nu strak te regelen. Anders zitten we later met een veel te vaak toegepaste bevoegdheid.

De antwoorden:
14 heeft de stukken niet paraat. Maar nu heeft het OM geen behoefte aan zo een bevel. Het is heel moeilijk om wetten te maken die rekening houden met de toekomst. Hij noemt het voorbeeld dat bij OVC op een computer (middels een bug) een lokaal gebruikt wachtwoord niet mag worden afgevangen omdat het geen communicatie is. Als hij via het internet met dat wachtwoord zou inloggen op een server elders, dan is dat wachtwoord wel communicatie en mogen we dat wel afvangen. Maar op de computer niet. Wij kunnen dus leven met een beperkte reikwijdte van een bevoegdheid. Maar houdt rekening met de toekomstbestendigheid.
De vraag of we toezicht moeten inbouwen buiten de strafrechter. Als er meer toezicht moet komen, doe dat dan breder, niet alleen voor deze ene bevoegdheid.

14 de politie krijgt ook een wapen. We hebben een geweldsrapportage die intern verplicht is. Zoiets kunnen we prima regelen. Het is de vraag of je dat in de wet of intern wilt regelen. Wij liever het tweede.

14 Gaat nog even in op de taps. Er is een WODC rapport waarin staat dat 8 op de 10.000 aansluitingen worden afgeluisterd. Dus het beeld dat wij alles en iedereen tappen is niet juist. Andere bevoegdheden zoals werken onder dekmantel zetten we dan weer heel weinig in.

14 Hij wil iedereen uitnodigen voor de themadag van het Kenniscentrum omdat het daar ook over dit wetsvoorstel gaat.

Blok 3: Technologie/Economie – 11.50 tot 13.00 uur

9 , Fox-IT
9 Google
9 Amsterdam Internet Exchange
9 , Nederland ICT
9 Radboud Universiteit

Introductie van standpunten:
14 Momenteel wordt er nog erg weinig ingegrepen op cybercriminaliteit. Er zijn zat bekende kwetsbaarheden. Met slimme mensen en open source tools kom je ook een heel eind. 14 breekt vaak in zonder dure tools (met toestemming). Als ze een kwetsbaarheid tegenkomen dan melden ze die achteraf. Dat zou de politie ook kunnen doen. Zijn voornaamste probleem is dat de machines overal ter wereld staan. Er moet een oplossing komen voor de souvereiniteitsproblemen. Hacken is het enige middel om de cybercriminelen te vinden. Daarom vindt hij dat de politie dat ook moet kunnen. Bijvoorbeeld inbreken op een camera systeem tijdens een gijzeling. Verder vindt hij dat als je mag hacken, je dat decryptie

bevel niet nodig hebt. Hacken moet een laatste redmiddel zijn en met name gebruikt worden om de server te vinden.

14 vindt dat het internet onveiliger wordt van deze bevoegdheid. De politie krijgt een prikkel om kwetsbaarheden te misbruiken in plaats van te melden. Dat zeggen alle experts die zij spreekt. Het leidt tot minder vertrouwen in Nederland. Het leidt tot onzekerheid.

14 hamert op het belang van vertrouwen. Zowel van bedrijven als eindgebruikers. Bijvoorbeeld in het communicatiegeheim. Hoe verhoudt deze bevoegdheid zich tot de zorgplicht van bedrijven, zoals de meldplicht. Zij moeten continuïteit garanderen en integriteit van informatie. De bevoegdheid die gebruik gaat maken van zwaktes, dat werkt averechts tegen andere wettelijke verplichtingen. Het is een prikkel om te zoeken naar kwetsbaarheden en deze te kopen en er dus voor te betalen. De kwetsbaarheden blijven beschikbaar voor iedereen, veiligheidsdiensten buitenlandse mogendheden en criminelen. Als de overheid deze tools inkopen dan financieren ze deze slechte praktijk. Afkadering is nodig, want voornemens zijn leuk maar het gaat toch om wat er in de wet komt te staan.
Hij vindt het jammer dat de sector zelf niet betrokken is bij het voorstel.

14 De reikwijdte van geautomatiseerd werk is veel te groot. Nederland heeft nu een hele goede positie, met een goed vestigingsklimaat. Vertrouwen is hiervoor essentieel, in dat er niemand meekijkt met wat je schrijft en in de apparaten. De politie heeft niet alle kennis in huis en houdt daarmee de industrie van inbrekers in stand. Het lijkt erop dat de ministeries elkaar tegenwerken. 14 maakt zich zorgen over te weinig transparantie van de politie, bv na de vragen over de Hacking Team hack. Ze willen graag dat er een verbod op inkoop van de zero-days komt. Ze hebben ook bezwaren tegen het inbreken in de cloud omdat daar ook gegevens van anderen in staan. Ze vinden het geen reden dat een rechtshulpverzoek te omslachtig is.

14 Het klopt dat er meer encryptie gebruikt wordt. Dat is goed, maar heeft ook een keerzijde voor de overheid. Je kunt dan kiezen voor de verplichte achterdeur, hacken of decryptie bevel. Dat zou je in samenhang moeten afwegen. Bv dat het decryptie bevel in ieder geval niet heimelijk is.
Is het gevaarlijk voor internet? Vergelijk het met het beveiligen van een huis. Dat vindt de politie goed, zelfs al moeten ze soms inbreken in een huis. Hij pleit voor een onafhankelijke toezichthouder. 9 De politie kijkt alleen uit strafrechtelijk perspectief. Maar je moet ook kijken naar wat het voor internet betekent. Apart van andere bevoegdheden, want internet heeft zijn eigen domein en dus eigen specialisten nodig om daarover te kunnen oordelen.

De vragen.
Tellingen. Kunt u uw vergelijking afmaken. 14 hoe zouden we het dan moeten doen. Hoe gaan we dan computercriminaliteit aanpakken?
Oosenbrug. Vond het belangrijk dat de partijen met tegengestelde belangen te maken krijgen. Hoe zou dat dan moeten volgens 14
Recourt. De politie zegt dat zij zullen melden. Waarom vertrouwt u ze niet? Is daar reden voor?
Helder. 14 zegt dat zero-days niet nodig zijn, maar 14 zegt van wel.
Verhoeven. Kunnen we dan in de wet zetten dat er geen zero-days worden gebruikt.
En aan 14 egt dat het internet onveiliger maakt. Is dat zo en wat is het effect.

Antwoorden:

14 Het internet is nu heel onveilig omdat criminelen maar door blijven gaan. Het bedrijfsleven heeft er echt een groot belang bij als er beter kan worden opgetreden. Over zero-days. Het is heel fijn om zoiets op de plank te hebben liggen. En die kun je zelf ook vinden, dat doen wij ook. En de vraag is hoeveel minder onveilig wordt het internet van het melden van die ene zero-day kwetsbaarheid.

14 Je moet toch inbreken, met zero-days of met andere kwetsbaarheden. Als dat niet nodig is prima. Maar haal dat dan uit de wet. Laat ze alleen social engineering toepassen.

14 De politie moet zich juist richten op publiek private samenwerking. Ze zouden de bedrijven juist moeten beschermen.14 is bang dat Nederland een precedent schept. En dat Chinezen bij ons komen neuzen. En dan de vraag wie aansprakelijk is als bedrijven enerzijds een zorgplicht hebben en verantwoordelijk zijn voor veilige dienstverlening maar anderzijds bedreigd worden door deze bevoegdheid. Dat vindt 14 ook vervelend.

14 In de digitale wereld ontbreekt een voorlichting vergelijkbaar met veilig wonen. Het is niet goed die verantwoordelijk bij NCSC te leggen. De politie kan wellicht ook bedrijven vervolgen vanwege onveiligheid zoals Samsung die nu wordt aangeklaagd door gebruikers. Hij ziet een spanningsveld tussen wel of niet melden en stimuleren van beveiliging. De politie heeft niet letterlijk gezegd dat ze niet in zee gaan met schimmige bedrijven als Hacking Team. In ieder geval verstandig om open over security te spreken en samen te werken, zoals bij de OV chipkaart.

14 Belangrijk om encryptie te stimuleren. In plaats van hacken in buitenland werk aan het verbeteren van rechtshulpverzoeken. En deel beveiligingslekken.

Vragen

Verhoeven. De minister zegt dat de toegang van buitenlandse inlichtingendiensten onveiligheid opleveren.

Recourt. Is een meldplicht voor de politie van kwetsbaarheden dan een idee.

14 Computercriminaliteit III ondermijnt het vertrouwen in de techniek.

14 Hij zou wel voor een meldplicht beveiligingslekken. In beginsel dan, want vooral internationale samenwerking kan prevaleren. En hij heeft een gezond wantrouwen richting het apparaat dat het geweldsmonopolie heeft. Tenslotte hamert hij nogmaals op kundig toezicht.

Van: 10.2.e)
Verzonden: dinsdag 16 februari 2016 15:23
Aan: 10.2.e
CC: 10.2.e 10.2.e
Onderwerp: RE: Moties VAO Cybersecurity

Hoi 10.2.e

Ter info. De motie van VVD (zie hieronder) is zojuist aangenomen. Die van SP is verworpen.

Gr.,

10.2.

Van: 10.2.e)
Verzonden: woensdag 10 februari 2016 09:20
Aan: 10.2.e @politie.nl>
Onderwerp: Moties VAO Cybersecurity

Hoi 10.2.e

Gisteren was het VAO Cybersecurity. Hier zijn de volgende voor de politie relevante moties ingediend:

- SP (TK nr. 26643-387) – ONTRADEN DOOR DE STAATSSECRETARIS

De Kamer,

gehoord de beraadslaging,

constaterende dat de voormalig minister van Veiligheid en Justitie heeft gesteld dat het mogelijk is om onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op afstand een computersysteem te betreden;

constaterende dat bij de invoering van de bevoegdheid om een plaats te doorzoeken echter nooit is gesproken over het op afstand binnendringen van computers en dat, indien voor een dergelijk handelen een wettelijke grondslag zal worden gecreëerd, dit in de eerste plaats iets is waarover de Kamer zich zal moeten uitspreken;

verzoekt de regering, te garanderen dat politie en justitie in ieder geval niet overgaan tot het op afstand heimelijk binnendringen van een geautomatiseerd werk zolang de wet computercriminaliteit III niet door de Kamer is behandeld en zij zich hierover heeft kunnen uitspreken,
en gaat over tot de orde van de dag.

- VVD (TK nr. 26643-388) – ONDERSTEUNING VAN BELEID

De Kamer,

gehoord de beraadslaging,

constaterende dat het Cybersecuritybeeld Nederland 5 aangeeft dat de beschikbaarheid van digitale systemen steeds belangrijker wordt omdat belangrijke maatschappelijke processen hiervan afhankelijk zijn en analoge alternatieven steeds vaker ontbreken;

constaterende dat legacy bestaat uit ICT-systemen met verouderde software en hardware met een verhoogd risico op beveiligingslekken, waardoor het risico op hacks en storingen toeneemt en digitale systemen kwetsbaar worden;

overwegende dat binnen de Nederlandse vitale infrastructuur en diensten digitale systemen met legacy worden gebruikt en dit onnodig risico oplevert voor belangrijke maatschappelijke processen en

daarmee voor de nationale veiligheid, mede door koppeling van verschillende vitale infrastructuren en ketenafhankelijkheden;

van mening dat legacy in de Nederlandse vitale infrastructuur, bij zowel de overheid als vitale sectoren, zo spoedig mogelijk moet worden vervangen en dat de rijksoverheid hierin een voorbeeldfunctie heeft;

verzoekt de regering, de legacyproblematiek actief, zowel binnen de rijksoverheid als binnen de vitale sectoren, tegen te gaan en daarbij dit punt in de toegezegde doorontwikkeling van de nationale cybersecuritystrategie te betrekken;

verzoekt de regering tevens om dit punt actief op te pakken in het kader van de implementatie van de NIB-richtlijn in het kader van sectorale zorgplichten op het gebied van digitale veiligheid,

en gaat over tot de orde van de dag.

Over de moties zal aanstaande dinsdag gestemd worden

Groet,

10.2.e
Senior adviseur
Politie I Korpsstaf I Bestuursondersteuning I Bestuurszaken
Nieuwe Uitleg 1 I 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag
M 10.2.e | 10.2.e @politie.nl
Werkdagen: maandag t/m vrijdagochtend

From: 10.2.e
Sent: vrijdag 19 februari 2016 10:31:43
To: 10.2.e - BD/DGPOL/PBT/PT
Cc: 10.2.e 10.2.e 10.2.e 10.2.e
Subject: D66

Hoi 10.2.e

afgelopen maandag zat Inge Philips samen met onder andere Kees Verhoeven van D66 in de radio uitzending van de Haagsche Lobby. Na afloop kwam Kees nog naar Inge en gaf aan het wel een goed idee te vinden om nog eens nader met elkaar van gedachten te wisselen over CCIII.

Net met 10.2.e hierover gesproken en we willen graag van jou weten wat de beste manier is om dit te regelen. Kan ik hem rechtstreeks uitnodigen of wil DGPol hier de regie op houden?

Ik hoor graag van je.

Groet,
10.2.e r
10.2.e
9
Politie | Project CCIII
Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg

Van: 10.2.e
Verzonden: vrijdag 19 februari 2016 10:32
Aan: 10.2.e B. - BD/DGPOL/PBT/PT'
CC: 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: D66

Hoi 10.2.e

afgelopen maandag zat Inge Philips samen met onder andere Kees Verhoeven van D66 in de radio uitzending van de Haagsche Lobby. Na afloop kwam Kees nog naar Inge en gaf aan het wel een goed idee te vinden om nog eens nader met elkaar van gedachten te wisselen over CCIII.

Net met 10.2.e hierover gesproken en we willen graag van jou weten wat de beste manier is om dit te regelen. Kan ik hem rechtstreeks uitnodigen of wil DGPol hier de regie op houden?

Ik hoor graag van je.

Groet,
10.2.e

10.2.e

9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg

Postbus 100, 3970 AC Driebergen-Rijsenburg

M 10.2.e

Email : 10.2.e @politie.nl

Werkdagen: maandag, dinsdag, donderdag en vrijdag

Van: 9 @minvenj.nl>
Verzonden: maandag 22 februari 2016 15:20
Aan: 10.2.e
Onderwerp: deelname conferentie Jurisdiction in Cyberspace

Dag 10.2.e

Hierbij zoals gevraagd een kleine indicatie van wat voor mensen er vanuit de andere politieorganisaties komen:

10.2		Belgium	RC
10.2.e		Denmark	9 National Policy Cyber crime Center
10.2.		Germany	Federal Criminal Police Office, BKA
10.2.e		Latvia	State police
10.2.e		Lithuania	9 cybercrime Unit
10.2.e		Malta	9 Cyber crime Unit, Malta Police Force, Police Headquarters
10.2.e		Poland	9 Department for Fighting against Cybercrime, Nat. Police
			National Police, Cybercrime and Cybersecurity Operations Team
10.2.e		Spain	9
10.2.e		Sweden	9 , Swedish Cybercrime Center

En vanuit jullie komt natuurlijk ook Inge Philips. Vanuit NL OM komen 10.2.e en 10.2.e
10.2.e

Ik hoor graag wie er van jullie komt.

Hartelijke groet, 10.2.

10.2.e

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
M 10.2.e
10.2.e @minvenj.nl

From: 9 @minvenj.nl]
Sent: Monday, February 22, 2016 06:04 PM W. Europe Standard Time
To: 10.2.e
Cc: 10.2.e 10.2.e 10.2.e 10.2.e
Subject: RE: D66

Ha 10.2.e ,

Dank voor jou mail. Ik bespreek dit met dgrr ivm de planning om vaste kamercie uit te nodigen voor bezoek aan politie ivm cc III en daarom te kijken wat voor behandeling wetsvoorstel handig is.

Ik laat weten hoe wij dit zien, kunnen we kijken of jullie je daar in kunnen vinden.
Mocht dit toch separaat lopen met Verhoeven dan moet ik stas informeren maar nodigen jullie uit,

Je hoort nog!

Groet 10.2.e

Van: Philips, Inge (I.C.)
Verzonden: maandag 22 februari 2016 18:35
Aan: 10.2.e @minvenj.nl'; 10.2.e
CC: 10.2.e 10.2.e 10.2.e
Onderwerp: Re: D66

Beste Allen, zowel Verhoeven als Tellegen hebben aangegeven graag langs te komen als we ze uitnodigen. Ik stel voor dat we9 .
Als we te lang wachten heeft t geen zin meer. Groet Inge

Groet,

Inge Philips
Plv Diensthoofd
Politie - Landelijke Recherche

From: 10.2.e - BD/DRC/CV
Sent: woensdag 9 maart 2016 15:56:25
To: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DWJZ/SSR
Cc: 10.2.e - BD/DRC/CV
Subject: verslag 2e kamer ccIII

Hierbij de set vragen, groet 10.2.e

From: 10.2.e - BD/DRC/CV
Sent: woensdag 9 maart 2016 18:59:53
To: 10.2.e - BD/DGPOL/PBT/PT
Subject: FW: verslag 2e kamer ccIII

Hierbij verslag ccIII kamer groet 10.2.e

Van: 10.2.e . - BD/DGPOL/PBT/PT <10.2.e @minvenj.nl>
Verzonden: donderdag 10 maart 2016 20:43
Aan: 10.2.e
Onderwerp: FW: verslag 2e kamer ccIII
Bijlagen: VerslagccIII.pdf

Komt nog formeel jullie kant op want zal vast ook vragen voor jullie bevatten. Heb nog geen vragen met wie doet wat van wetgeving gekregen.
Wordt vervolgd!

Tweede Kamer der Staten-Generaal

0269 2

Vergaderjaar 2015–2016

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 5

VERSLAG

Vastgesteld 8 maart 2016

De vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

INHOUDSOPGAVE **blz.**

kst-34372-5
ISSN 0921 - 7371
's-Gravenhage 2016

I ALGEMEEN DEEL

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III). De snelle ontwikkelingen van technologie, internet en computercriminaliteit maken een modernisering en uitbreiding van de bevoegdheden voor opsporing en vervolging noodzakelijk. Het lijkt soms of met dit wetsvoorstel moet worden gekozen tussen privacy en veiligheid. Deze leden zien dat als een onterechte tegenstelling. Vaak wordt het toekennen van opsporingsbevoegdheden gezien als het inboeten op privacy. De aan het woord zijnde leden zien de bevoegdheden in onderhavig wetsvoorstel juist als een mogelijkheid om privacyschendingen, die dagelijkse realiteit zijn, te bestrijden. Heeft de burger liever dat criminelen, activisten of terroristen zijn computer hacken of heeft hij liever dat de politie geautomatiseerde werken van verdachten mag hacken om criminaliteit te bestrijden? Dagelijks wordt de privacy van burgers geschonden door criminele hackers die uit zijn op hun data. Door de politie de met strikte waarborgen omklede bevoegdheid te geven een geautomatiseerd werk dat in gebruik bij een verdachte is op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied opsporing van ernstige strafbare feiten, zal de privacy van burgers eerder versterkt dan geschonden worden. De politie is er juist om hackers die zichzelf ongeoorloofd toegang verschaffen tot bedrijfsgegevens, persoonsgegevens en gevoelige persoonsgegevens aan te pakken. De politie verdient in de ogen van de leden van de VVD-fractie in beginsel het vertrouwen dat zij op juiste wijze met deze taak en bevoegdheid om zal gaan. In de tweede plaats zal met name het interne toezicht binnen de politie en de hack unit op orde moeten zijn. De aan het woord zijnde leden van de VVD-fractie hebben nog enkele vragen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij zijn van mening dat naarmate de ontwikkeling van het internet en het gebruik van geautomatiseerde werken ook bij criminelen voortschrijdt, de ontwikkeling van strafrechtelijke bevoegdheden om deze vorm van criminaliteit aan te pakken daarmee gelijke tred moet houden. In die zin steunen de aan het woord zijnde leden de voorstellen waarmee meer van dergelijke bevoegdheden worden geïntroduceerd of versterkt. Echter, het gebruik van bevoegdheden dient, zeker als daarmee de privacy of de veiligheid van de internetgebruiker in het geding is, slechts met de nodige waarborgen omkleed en terughoudend ingezet te worden. De leden van de PvdA-fractie hebben daarom de volgende vragen en opmerkingen.

De leden van de SP-fractie hebben kennisgenomen van de inhoud van onderhavig wetsvoorstel en hebben hierover veel kritische vragen en opmerkingen. Zij zijn allereerst nog steeds niet voldoende overtuigd van de noodzaak van dit wetsvoorstel, vooral vanwege de vergaande inbreuk op de grondrechten. De vraag is in hoeverre de nieuwe bevoegdheid om heimelijk een geautomatiseerd werk binnen te dringen in het leven wordt geroepen omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is of omdat er echt misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid. Zo ja, is ook onderzocht of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is? Graag ontvangen deze leden een uitgebreide toelichting hierop.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van voorliggend wetsvoorstel. Zij zien hierin belangrijke voorstellen terugkomen in aanvulling op de Wet Computercriminaliteit I (1993) en de Wet computercriminaliteit II (2006). Deze leden constateren dat politie en justitie momenteel achter de feiten aanlopen voor wat betreft de bestrijding van digitale criminaliteit en digitale uitwisseling van criminelen ter voorbereiding op andersoortige (ernstige) delicten. Deze analyse wordt gedeeld, zo merken deze leden op, door zowel voor- als tegenstanders van onderhavig wetsvoorstel. Dit is hen gebleken uit de schriftelijke consultatieronde alsmede uit de inbreng van deskundigen in het rondetafelgesprek op 11 februari 2016 in de Kamer over dit wetsvoorstel. De leden van de CDA-fractie achten een spoedige inwerkingtreding van onderhavig wetsvoorstel dan ook gewenst. Deelt de regering deze mening en wil zij weliswaar zorgvuldig maar ook met enige voortvarendheid de vragen in dit verslag beantwoorden? Iedere dag, zo menen deze leden, dat onderhavig wetsvoorstel niet in werking treedt, is een gemiste kans in de strijd tegen ernstige vormen van criminaliteit, zoals het beramen van terroristische aanslagen en kindermisbruik. In dat kader betreuren deze leden dat pas vijf jaar na een inventarisatie van het juridisch kader voor cybersecurity en de juridische knelpunten het onderhavige wetsvoorstel aan de Kamer is gezonden (Kamerstukken 2011/12, 26 643, nr. 200 en 28 684, nr. 323). De aan het woord zijnde leden vragen waarom dit zo lang geduurd heeft. Dit kan immers niet enkel veroorzaakt zijn door de later toegevoegde bevoegdheden omtrent grooming? Ook na de aankondiging van het voorliggende wetsvoorstel in het Actieplan Jihadisme (augustus 2014) heeft het nog enige tijd geduurd voordat het aan de Kamer is gezonden. Graag vernemen deze leden hierop een reactie.
De leden van de CDA-fractie vragen of de regering de mening deelt dat met onderhavig wetsvoorstel niet de privacy van burgers onder druk komt te staan, maar dat het juist bijdraagt aan een nog zorgvuldiger optreden van politie en justitie dan thans het geval is in de opsporing. Immers, kan niet ook door digitaal speurwerk worden voorkomen dat klassieke opsporingsmethodes als huiszoekingen en (fysieke) inbeslagnames van apparatuur moeten worden ingezet, welke bevoegdheden (eveneens) een

inbreuk plegen op de privacy en diverse grondrechten van burgers? Graag vernemen deze leden een reactie van de regering hierop, ook gelet op haar opmerking dat het thans een inbreuk op de persoonlijke levenssfeer betekent als getracht wordt de verborgen (fysieke) locatie van computercriminelen te ontdekken en te ontmantelen.
Ondanks de positieve grondhouding die de leden van de CDA-fractie hebben bij onderhavig wetsvoorstel, maken zij zich wel zorgen over de verzwakking van de voorgestelde bevoegdheden die in het wetsvoorstel zijn geslopen na meerdere consultatierondes de afgelopen drie jaar. Meest in het oog springend is het schrappen van het decryptiebevel, maar ook enkele andere aanpassingen belemmeren en/of vertragen politie en justitie onnodig bij het opsporingsproces. Zij vragen de regering met klem geen gehoor te geven aan diverse geluiden, zoals geuit door enkele partijen en deskundigen in het hierboven genoemde rondetafelgesprek, om de voorgestelde bevoegdheden nog verder af te zwakken. Een dergelijke (politieke) keuze zou in de ogen van de leden van de CDA-fractie de doeltreffendheid van het wetsvoorstel onderuithalen en politie en justitie (opnieuw) achter de feiten aan doen lopen.
Graag leggen de leden van de CDA-fractie de regering de volgende vragen voor over de verzwakkingen van de oorspronkelijk voorgestelde bevoegdheden in het wetsvoorstel, met uitzondering van het decryptiebevel waar zij later nog uitgebreider op terugkomen.

1. Waarom heeft de regering er niet voor gekozen het toepassingsbereik van de bestaande bevoegdheid tot het ontoegankelijk maken van gegevens te verruimen ex artikel 54a van het Wetboek van Strafrecht (Sr)? Zou dit politie en justitie juist niet enorm helpen in de opsporingspraktijk én in het voorkomen van nieuwe strafbare feiten? Is deze keuze overlegd met politie en justitie? Wat waren hun wensen op dit punt? Kan de regering weergeven hoe wetstechnisch een verruiming zou kunnen worden vormgegeven op dit punt?
2. Waarom heeft de regering de voorgestelde bevoegdheid in het conceptwetsvoorstel van het geven van een mondelinge vordering van gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker geschrapt?
3. Waarom heeft de regering de voorgestelde bevoegdheid in het conceptwetsvoorstel van het geven van een mondelinge vordering ter zake van de zogenaamde NAW-gegevens (naam, adres, woonplaats) van een gebruiker van een communicatiedienst geschrapt?
4. Waarom heeft de regering de voorwaarde voor de inzet van de bevoegdheid tot het binnendringen in een geautomatiseerd werk aangescherpt, zodat de lat nu zeer hoog is gelegd, te weten bij een verdenking van een misdrijf waarop acht jaar gevangenisstraf staat en een ernstige inbreuk op de rechtsorde oplevert? Welke misdrijven vallen nu niet meer onder de reikwijdte van deze bevoegdheden in vergelijking met de formulering in het conceptwetsvoorstel?
5. Wat zijn de gevolgen voor de administratieve lasten (zoals tijd, inspanning maar ook effectiviteit) bij de opsporingsdiensten, nu de voorgestelde bevoegdheid tot binnendringen is geplaatst in titel IVA van het Wetboek van Strafvordering (Sv)? Aan welke voorwaarden tot het inzetten van bijzondere opsporingsbevoegdheden moet extra worden voldaan in vergelijking met de oorspronkelijk gemaakte keuze in het conceptwetsvoorstel (plaatsing in titel IV)?
6. Waarom heeft de regering extra (tijdrovende en tevens proceskosten veroorzakende) drempels opgeworpen door middel van de toets van de rechter-commissaris bij het inzetten van bevoegdheden, zoals bij het ontoegankelijk maken van gegevens? Wat betekentschrapping van de zelfstandige bevelsbevoegdheid van de officier van justitie uit het wetsvoorstel voor de effectiviteit van de opsporing en het voorkomen van nieuwe strafbare feiten?

7. Waarom heeft de regering de dwangsom uit het wetsvoorstel gehaald wanneer niet is voldaan aan het bevel om gegevens ontoegankelijk te maken? Wat betekent dit voor de afbreuk van de effectiviteit van dit bevel in de praktijk?

De leden van de CDA-fractie vragen voorts waarom de onder 2 en 3 genoemde mondelinge vorderingen uiteindelijk overgeheveld zijn naar een ander, nog niet bij de Kamer ingediend, wetsvoorstel. Is behalve wetssystematiek niet veel meer van belang voor de opsporing dat deze maatregelen zo spoedig mogelijk kunnen worden ingezet? Is de verwachting van de regering niet dat onderhavig wetsvoorstel eerder in werking zal treden dan het wetsvoorstel waar deze bevoegdheden nu naar zijn overgeheveld en dus voor het opsporingsbelang gewenst is dat deze bevoegdheden in onderhavig wetsvoorstel worden opgenomen? Komen deze bevoegdheden wel op precies dezelfde voorgestelde wijze terug als voorgesteld in het conceptwetsvoorstel? Wanneer kan de Kamer het nog niet ingediende wetsvoorstel verwachten? Heeft de regering deze gemaakte keuzes tot overheveling en de consequenties daarvan voor de inwerkingtreding overlegd met politie en justitie.

De leden van de D66-fractie hebben met evenveel verbazing als verontrusting kennisgenomen van het onderhavige wetsvoorstel, waarbij gebruik gemaakt wordt van fouten in de software. De Staatssecretaris van Veiligheid en Justitie heeft de Kamer tijdens het algemeen overleg over cybersecurity een brief toegezegd over het gebruik van technische kwetsbaarheden door middel van «zero days» door de politie. Deze leden vinden het teleurstellend dat die brief niet aan de Kamer is gestuurd voor de inbrengdatum voor dit verslag, waardoor een aantal belangrijke vragen over de toepassing niet op voorhand zijn verduidelijkt. Voornoemde leden vragen de regering die brief gelijktijdig met de nota naar aanleiding van het verslag aan de Kamer te doen toekomen. Deze leden staan kritische tegenover dit wetsvoorstel en hebben een groot aantal opmerkingen en vragen.
De leden van de D66-fractie constateren dat de Kamer drie jaar heeft moeten wachten op dit wetsvoorstel. Kan de regering toelichten waarom er tussen de consultatie en het toesturen aan de Kamer zoveel tijd heeft gezeten?
De aan het woord zijnde leden constateren dat het wetsvoorstel enkele weken na de aanslagen in Parijs is gepresenteerd als een antiterrorisme maatregel. In hoeverre kan dit wetsvoorstel gevolgen hebben voor de bestrijding van terrorisme? Wat is de reden dat de regering dit wetsvoorstel in tegenstelling tot de consultatielancering drie jaar geleden, nu als een antiterrorisme maatregel neerzet? Deelt de regering de mening dat dit wetsvoorstel voornamelijk gericht is op de traditionele criminaliteit, waarbij de daders gebruik maken van digitale communicatiemiddelen?
De leden van de D66-fractie constateren dat het wetsvoorstel ten opzichte van het conceptvoorstel op een aantal belangrijke punten is afgezwakt. Deze leden waarderen het dat de regering kritieken ter harte heeft genomen en het onderdeel decryptie, het verplicht ontsleutelen door de verdachte waarmee zelfincriminatie zou ontstaan, uit het wetsvoorstel heeft geschrapt. Zij waarderen ook de overweging om ten minste een toets van de rechter-commissaris in te bouwen voordat door opsporingsinstanties überhaupt toegang mag worden verschaft. Kan de regering toelichten op grond waarvan is besloten om de bevoegdheid tot een mondelinge vordering van bepaalde gegevens over te hevelen van onderhavig wetsvoorstel naar het wetsvoorstel voor een bewaarplicht telecommunicatie?
De leden van de D66-fractie hebben desalniettemin ook veel kanttekeningen bij de voorgestelde maatregelen. Hoe gaan de voorgestelde maatregelen de veiligheid van burgers in de samenleving vergroten en hoe worden vergaande inbreuken op grondrechten van burgers beperkt?

Vooral bij het heimelijk toegang verschaffen door gebruik te maken van technische kwetsbaarheden, hebben deze leden grote bezwaren. Zij constateren dat ook tijdens het rondetafelgesprek in de Kamer is gebleken van vele kanttekeningen bij het wetsvoorstel, in het bijzonder voor wat betreft het gebruik van technische kwetsbaarheden.
De leden van de D66-fractie lezen dat het doel van het wetsvoorstel is de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van ICT. In dit wetsvoorstel wordt onder andere voorgesteld een nieuwe bevoegdheid te creëren om een geautomatiseerd werk op afstand heimelijk binnen te kunnen dringen oftewel te kunnen hacken. Om te kunnen hacken zijn fouten in de software nodig, dezelfde fouten die criminelen of buitenlandse mogendheden gebruiken om cyberaanvallen te plegen. Deze leden vragen de regering in te gaan op de tegenstrijdigheid van deze beleidskeuze om cybercriminelen te bestrijden door de kwetsbaarheden, die zij gebruiken om hun criminelen activiteiten te ontplooien, niet proberen te dichten, maar juist open te houden en zelf te misbruiken. Voorts vragen de aan het woord zijnde leden de regering in te gaan op de mogelijke situatie dat de Nederlandse regering de nu nog schimmige markt in onbekende kwetsbaarheden, zogeheten «zero days», legitimeert en stimuleert door software te kopen van bijvoorbeeld een HackingTeam. Acht de regering het mogelijk dat hackers door de legitimering van de markt in «zero days» eerder geneigd zullen zijn om «zero days» te verkopen aan HackingTeam-achtige bedrijven of overheden?
De leden van de D66-fractie constateren dat het wetsvoorstel in consultatie is gegeven aan tal van relevante belanghebbenden, zoals het College van procureurs-generaal, de Raad voor de rechtspraak, de politie, de Nederlandse Orde van Advocaten. In deze lange lijst van belanghebbenden staan echter geen bedrijven of belangenorganisaties van bedrijven. Waarom is hier niet voor gekozen?
Voorts lezen de aan het woord zijnde leden dat de versleuteling van gegevens ongedaan kan worden gemaakt. Zij vragen de regering toe te lichten op wat voor manier de versleuteling ongedaan kan worden gemaakt. Gebeurt dat door kwetsbaarheden in de encryptiesoftware te misbruiken? Is de regering het met deze leden eens dat het onwenselijk is kwetsbaarheden in encryptiesoftware te misbruiken? Hoe verhoudt het eventueel misbruiken van fouten in software zich tot de brief van 4 januari 2016 van de regering over encryptie? Is de regering van plan fouten in encryptiesoftware te misbruiken om gegevens te ontsleutelen?
De leden van D66-fractie constateren dat de Wetenschappelijke Raad voor Regeringsbeleid (WRR) in zijn advies «De publieke kern van het internet» stelt dat «het geheimhouden van kwetsbaarheden er simpelweg toe leidt dat het internet onveiliger wordt. Kwetsbaarheden die worden «bewaard» om cyberaanvallen mogelijk te maken en het doelbewust inbouwen van zwakheden in standaarden en software die wij allemaal gebruiken [...] verslechteren de algehele veiligheid van het gehele internet en van al zijn gebruikers. Als we de integriteit, de beschikbaarheid en de vertrouwelijkheid van het internet niet meer kunnen vertrouwen, heeft dat gevolgen voor het sociaaleconomische bouwwerk dat we op die infrastructuur hebben geconstrueerd: van online bankieren tot communicatie.» Hoe verhoudt dit wetsvoorstel zich tot het advies van de WRR, zo vragen deze leden.

De leden van de fractie van de ChristenUnie hebben kennisgenomen van het voorliggende wetsvoorstel. Zij waarderen de inspanning van de regering om de opsporingsbevoegdheden en strafrechtelijke bepalingen in lijn te brengen met de technische mogelijkheden en wensen van deze tijd. Zij hebben tegelijk nog wel de nodige vragen over de voorgestelde,

zeer ingrijpende opsporingsbevoegdheden en de waarborgen daar omheen.

De leden van de GroenLinks-fractie hebben met de nodige bezorgdheid kennisgenomen van het voorliggende wetsvoorstel, dat onder meer een strafvorderlijke hackbevoegdheid introduceert. Deze leden zien in het heimelijk binnendringen in geautomatiseerde werken grote fundamentele en praktische problemen ontstaan. Zij hebben daarom nog vragen over dit wetsvoorstel.

De leden van de PvdD-fractie hebben met grote zorgen kennisgenomen van het onderhavige wetsvoorstel. Dit wetsvoorstel maakt buitenproportioneel veel inbreuk op de privacy van Nederlanders en tast de onlineveiligheid ernstig aan. Volgens hoogleraar informatierecht Nico van Eijk van de Universiteit van Amsterdam en het College bescherming persoonsgegevens (Cbp) zou de wet bovendien een grondwettelijke toetsing niet doorstaan.

2. Onderzoek in en geautomatiseerd werk

2.1 De noodzaak van de voorgestelde bevoegdheid

De leden van de PvdA-fractie begrijpen dat de technologische ontwikkelingen de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk noodzakelijk maken. De bevoegdheid om ter plaatse een gegevensdrager in beslag te mogen nemen of te doorzoeken wordt onvoldoende onderkend dat gegevens lang niet altijd meer op een duidelijk herkenbare fysieke locatie zijn opgeslagen. Deze leden nemen ook aan dat zonder de bevoegdheid om heimelijk en op afstand een geautomatiseerd werk binnen te mogen dringen de opsporing van ernstige strafbare feiten belemmerd wordt. Echter, het feit dat een bevoegdheid nodig is voor de opsporing van strafbare feiten, rechtvaardigt niet meteen de introductie of het gebruik daarvan. Niet ieder doel heiligt dat middel. Zo vragen de leden van de PvdA-fractie in hoeverre bij het gebruik van de nieuwe bevoegdheid niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben. Hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn? Hoe wordt gewaarborgd dat de bevoegdheid tot het doen van het op afstand en heimelijk onderzoeken in een geautomatiseerd werk het ultimum remedium is in de reeks van bestaande bevoegdheden? Maakt de rechter-commissaris hierin een afweging? Waarom is het «niet uitgesloten» dat er in plaats van het op afstand heimelijk binnendringen in een geautomatiseerd werk gekozen wordt voor een van de andere opsporingsbevoegdheden? Waarom wordt niet standaard eerst uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie?
De leden van de PvdA-fractie lezen dat ook bijzondere opsporingsdiensten, zoals de FIOD/ECD, de mogelijkheid krijgen van de nieuwe bevoegdheid gebruik te maken. Kan de regering uitleggen waarom dit nodig is? Zijn de vormen van criminaliteit waarmee deze diensten te maken krijgen ernstig genoeg om de inzet van de nieuwe bevoegdheid te rechtvaardigen? Is hier sprake van misdrijven die een ernstige inbreuk op de rechtsorde opleveren? Zo ja, welke?

De leden van de SP-fractie constateren dat veel kritiek is geuit op de reikwijdte van het begrip geautomatiseerd werk. Kan de regering

aangeven welke geautomatiseerde werken op dit moment onder deze 0270
definitie zal vallen en waarom? Waar ligt uiteindelijk de grens, wie bepaalt deze grens en wie controleert deze grens?
De aan het woord zijnde leden vragen hoe men weet waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig zijn Hoe groot is het risico dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing? Hoe wordt dit risico zoveel mogelijk weggenomen? Er kunnen bijvoorbeeld ongelooflijk veel gegevens verzameld worden bij toegang tot bijvoorbeeld de Cloud. Hiervoor zijn waarborgen ingebouwd, zoals toetsing door de rechter-commissaris naar de proportionaliteit, maar hoe wordt voorkomen dat ongericht gegevens wordt verzameld? Men weet immers niet altijd van tevoren waar welke gegevens vandaan gehaald moeten worden en welke gegevens nodig zijn. Hoe ziet de regering dit praktisch voor zich?
De leden van de SP-fractie begrijpen, zoals de regering stelt, dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn. Soms is het werk waar de gegevens op staan niet bekend en is het tijdrovend en privacy schendend om deze te achterhalen. Betekent dit dat het plaatsen van software niet altijd mogelijk is? Is het achterhalen van geautomatiseerd werk t minder privacy-schendend dan het anoniem inbreken op een geautomatiseerd werk?
De aan het woord zijnde leden vragen of het klopt dat het op dit moment niet mogelijk is gegevens te achterhalen die zijn opgeslagen in de Cloud. Kunnen praktijkvoorbeelden gegeven worden van opsporingsonder-zoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen? Op dit moment is niet voorzien in de mogelijkheid om een bug te plaatsen die door middel van software buitenaf, dus online, op de computer wordt geplaatst. Wordt hiermee eigenlijk ook niet gesuggereerd dat het inzetten van bepaalde spyware niet rechtmatig was, zoals wel werd aangegeven in het antwoord op de Kamervragen over de inzet van Finfisher (Aanhangsel Handelingen Tweede Kamer, vergaderjaar 2014–2015, nr. 202)? Deze leden ontvangen hier graag een toelichting op en ook op de uitspraak van FOX IT in de gespreksnotitie voor het rondetafelgesprek over onderhavig wetsvoorstel op 11 februari 2016, waarin wordt gesteld dat de politie al geoefend heeft met het instrument hacken. Dit betekent dus dat er wel degelijk reeds op afstand heimelijk is binnengedrongen op een geautomatiseerd werk. Op basis van welke wettelijke grondslag is dat dan gebeurd? De leden van de SP-fractie merken op dat er een verplichting komt tot vernietiging van de gegevens die onder het geheimhoudingsplicht vallen. Maar wie bepaalt welke gegevens om die redenen kunnen worden vernietigd en om welke gegevens het gaat? Bovendien zijn de gegevens op dat moment reeds ingezien. Hoe wordt daarmee omgegaan? Heeft de betreffende opsporingsambtenaar dan een afgeleide geheimhoudingsplicht? Deze leden begrijpen dat inmiddels ook gebruik wordt gemaakt van inter-nettaps, waardoor communicatiegegevens, die via internet gedeeld worden, afgetapt kunnen worden. Waarom is deze mogelijkheid blijkbaar onvoldoende zodat opsporingsambtenaren de bevoegdheid krijgen op afstand te kunnen hacken? Om welke opsporingsambtenaren gaat het en in welke situaties is het noodzakelijk? De leden van de SP-fractie zijn benieuwd op welke manier rekening wordt gehouden met de vrijheid van meningsuiting. Komt er een uitgebreide instructie aan de rechter-commissaris voor de afweging over afgifte van een machtiging om een site te blokkeren of te hacken als het gaat om het waarborgen van de vrijheid van meningsuiting en de bronbescherming? Hoe wordt rekening gehouden met de wettelijke bronbescherming bij het afgeven van een machtiging?

De leden van de D66-fractie merken op dat de regering meent dat er een noodzaak is tot het introduceren van een bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te kunnen dringen en onderzoek te kunnen doen naar de kenmerken van het geautomatiseerd werk en de gebruiker en vastlegging van gegevens die op het geautomatiseerde werk zijn opgeslagen, ontoegankelijk te kunnen maken of communicatie te kunnen opnemen en stelselmatig te kunnen observeren. Deze leden constateren dat het daarmee om een zeer brede waaier van binnendringen gaat via een geautomatiseerd werk. Het is hen niet duidelijk waar nu precies de noodzaak, tot het op deze wijze binnendringen van een geautomatiseerd werk, op is gebaseerd. Deze leden delen de opvatting dat sprake is van een voortschrijdende techniek en een wijdverbreid gebruik daarvan. Voornoemde leden menen tevens dat de opsporingsmogelijkheden daarop aangehaakt moeten worden. Dat vergt wel dat de inzet van vergaande ingrijpende bevoegdheden echt noodzakelijk is. Te meer nu de voorgestelde bevoegdheid als neveneffect kan betekenen dat het gebruik van apparaten en het internet juist onveiliger wordt doordat technische kwetsbaarheden nodig zijn om te kunnen binnendringen in die apparaten. Kan de regering ingaan op de noodzaak en naast enkele concrete gevallen ook een meer overstijgende algemene noodzaak formuleren voor de toevoeging van deze bevoegdheid? Kan het ook op een andere minder ingrijpende wijze plaatsvinden?
Daarbij vragen de leden van de D66-fractie ook een toelichting op de verwachte proportionaliteit en effectiviteit van de bevoegdheid en hoe die is afgewogen. Waaruit blijkt bijvoorbeeld dat sprake is van een leemte in de bestaande wettelijke bevoegdheden?
De aan het woord zijnde leden lezen dat de regering de noodzaak van het wetsvoorstel onder andere legt bij de toename in het gebruik van versleuteling van elektronische gegevens. In de eerder genoemde brief over encryptie onderschrijft de regering terecht «het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie.» Het belang van sterke encryptie voor de persoonlijke levenssfeer, voor de vertrouwelijke communicatie van overheden en bedrijven en voor de Nederlandse economie gaat dus boven het opsporingsbelang van de politie om de encryptie te verzwakken. Kan de regering toelichten waarom dit niet geldt voor het belang van veilige software? De overheid krijgt met dit wetsvoorstel immers een belang bij fouten in de software die nodig zijn om te kunnen hacken en die ook door criminelen gebruikt kunnen worden. Kan de regering toelichten bij hoeveel zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, in 2015 de versleuteling van gegevens een cruciale factor heeft gevormd waardoor niet tot vervolging is overgegaan? Hoeveel criminelen lopen nu vrij rond doordat zij gebruik maken van encryptie waardoor de politie bepaalde gegevens niet kunnen inzien? Kan de regering een statistisch overzicht geven van het aantal taps dat ineffectief is door het gebruik van encryptie?
Voorts lezen deze leden dat de toename van het gebruik van meerdere verschillende draadloze netwerken ook als noodzaak genoemd wordt voor dit wetsvoorstel. Kan de regering aangeven wat zij doet om eigenaren van Wi-Fi-netwerken erop te attenderen dat de beveiliging van het Wi-Fi-netwerk niet op orde is, waardoor onder andere criminelen er gebruik van kunnen maken? In Australië en de Verenigde Staten zijn pilots gedaan met «wardriving» door politieagenten om zo kwetsbare Wi-Fi-netwerken in kaart te brengen en de eigenaren te helpen de beveiliging op orde te brengen. Is de regering op de hoogte van deze pilots? Heeft zij zelf ervaring met deze praktijk? Waarom zet de regering niet in op het veiliger maken van Wi-Fi-netwerken, zodat criminelen minder snel gebruik kunnen

maken van de verschillende Wi-Fi-netwerken? Kan de regering een overzicht geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van verschillende Wi-Fi-netwerken? Kan de politie ook andere geautomatiseerde werken op een openbaar Wi-Fi-netwerken hacken als een verdachte ook gebruik maakt van dat netwerk?
De leden van de D66-fractie lezen dat de toename in het gebruik van cloudcomputingdiensten als noodzaak voor dit wetsvoorstel wordt genoemd. De regering stelt dat voor de aanbieders van cloudcomputingdiensten de plaats van opslag vanuit bedrijfseconomisch perspectief vooral van belang is in verband met de kosten daarvan en de zekerheid van de verbindingen. Is de regering zich bewust van het feit dat ook de veiligheid van de data van de klanten van de cloudcomputingdiensten een belangrijk aspect is voor de keuze van vestiging van een bedrijf of individueel datacenter van een bedrijf. Kan de regering aangeven of zij het hacken, dat wil zeggen het hacken door middel van fouten in software, van servers van cloudcomputingdiensten uitsluit? Zo nee, kan de regering aangeven hoe zij de gevolgen hiervan inschat voor de Nederlandse economie en het Nederlandse vestigingsklimaat? Kan de regering een overzicht geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van cloudcomputingdiensten?
Voorts vragen de leden van de D66-fractie de regering in te gaan op de voordelen van ICT-technologieën die het voor de politie de afgelopen jaren juist makkelijker hebben gemaakt om criminelen op te pakken, zoals beter beschikbare informatie via telefoons en iPads, het gebruik van drones, «gunshot-detection-systems», het monitoren van tweets en andere social media, het voorspellen van misdaad op basis van «big-data» of GPS-systemen. Kan de regering toelichten in hoeverre de technologische ontwikkelingen het werk van de politie de afgelopen jaren per saldo makkelijker of moeilijker hebben gemaakt? Kan de regering haar antwoord met statistieken onderbouwen?
De leden van de D66-fractie lezen dat de regering stelt dat de opsporingsbevoegdheden, die zijn gericht op het vastleggen van elektronische gegevens, niet langer voldoen. Kan de regering deze uitspraak cijfermatig onderbouwen? Hoe verhoudt zich dat tot hetgeen de Minister van Veiligheid en Justitie in 2014 in antwoord op bovengenoemde Kamervragen aan de Kamer heeft laten weten, te weten: «(d)e politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). Voorts is het onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen. In een aantal strafzaken waarin het ging om zeer ernstige feiten is hiervan sprake geweest.» Hieruit blijkt dat de politie al op basis van artikel 125i Sv zich toegang tot computersystemen kan verschaffen en gegevensbestanden kan doorzoeken. Kan de regering toelichten hoe de reeds bestaande mogelijkheden een verdere uitbreiding van de bevoegdheid tot het heimelijk toegang verschaffen noodzakelijk maakt zoals het wetsvoorstel pretendeert? In hoeverre kan hier louter worden volstaan met het toevoegen van enkele strikte waarborgen voor toepassing in plaats van nog verder uitbreiden van de bevoegdheden?

De aan het woord zijnde leden vragen waaruit blijkt dat de bestaande bevoegdheden in toenemende mate te kort schieten. Welke wezenlijke problemen en gebleken knelpunten zijn er? Bij het binnendringen van apparatuur is het de bedoeling dat de verdachte niet op de hoogte is van het feit dat de politie in hem of haar is geïnteresseerd. Begrijpen zij het goed dat de regering daarmee de voorgestelde bevoegdheid tot heimelijk binnendringen beschouwd als een uitgebreide vorm van observatie? Of ziet de regering het als een digitale vorm van huiszoeking? Bij dat laatste is de verdachte er wel van op de hoogte dat zijn privézaken worden doorzocht op belastend materiaal?
De leden van de D66-fractie vragen of de regering de constatering deelt dat de introductie van de voorgestelde bevoegdheid niet alleen tegemoet komt aan de technologische ontwikkelingen, maar tegelijkertijd ook de positie van de verdachte wijzigt doordat een verdachte al vergaand onderzocht kan worden voordat hij of zij ervan op de hoogte is dat de politie in hem of haar geïnteresseerd is en dus ook voordat de betreffende persoon in staat van beschuldiging is gesteld? Wat betekent dat voor de verdediging van de verdachte en hoe verwacht de regering dat de rechtspraak hiermee om zal gaan? Is de introductie van deze bevoegdheid dermate fundamenteel ingrijpend voor de positie van de verdachte dat deze eerst meegenomen dient te worden bij de vaststelling van de contouren van de modernisering van het Wetboek van Strafvordering?
De aan het woord zijnde leden vragen hoe het voorliggende wetsvoorstel zich verhoudt tot de aangekondigde Wet op de inlichtingendiensten en de aangekondigde Wet bewaarplicht? In hoeverre is sprake van overlap tussen deze wetsvoorstellen omdat zij voorzien in vergelijkbare bevoegdheden?
Hoe wordt, bij het heimelijk binnendringen van geautomatiseerde werken, voorkomen dat ook inzage ontstaat in communicatie van andere niet-verdachte personen? Hoe wordt gewaarborgd dat de heimelijke inbreuk alleen plaatsvindt op de desbetreffende persoon waarvoor via de rechter-commissaris een machtiging is afgegeven? Acht de regering het überhaupt mogelijk de kring van personen die het zou kunnen betreffen te beperken?
De leden van de D66-fractie lezen in het wetsvoorstel dat met behulp van deze bevoegdheid het geautomatiseerde werk of de gebruiker kan worden geïdentificeerd ten behoeve van een meer gericht bevel tot het aftappen en opnemen van communicatie. Dat wekt de indruk dat in eerste instantie met een sleepnetmethode wordt gewerkt en pas daarna meer gerichte onderzoekshandelingen plaatsvinden. Klopt die veronderstelling? De aan het woord zijnde leden constateren dat niet alleen de politie de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk krijgt, maar ook de Koninklijke Marechaussee en de bijzondere opsporingsdiensten, zoals de FIOD/ECD. Kan de regering toelichten waarom al deze organisaties deze vergaande bevoegdheid nodig hebben? Wat voor soort misdrijven bestrijden deze bijzondere opsporingsdiensten waarvoor deze bevoegdheid nodig is? Kan de regering voorts toelichten wat voor misdrijven vallen onder «ernstige vormen van fraude en witwassen» of «omvangrijke milieumisdrijven»?

De leden van de ChristenUnie-fractie vragen naar de reikwijdte van de term «geautomatiseerd werk». Wordt met de definitie in artikel 80sexies feitelijk ieder met internet verbonden werk bedoeld? Zo nee, welke werken vallen niet onder deze definitie? Deze leden menen dat de noodzaak van een brede reikwijdte van het genoemde begrip nadere onderbouwing vraagt. Kan de regering daarop reageren?

De leden van GroenLinks-fractie vragen hoe de introductie van een hackbevoegdheid zich verhoudt tot de rechtstatelijke uitgangspunten. In hoeveel gevallen in de afgelopen vijf jaar had zo'n hackbevoegdheid

kunnen worden ingezet en waarom schoten bestaande dwangmiddelenbevoegdheden te kort. Met andere woorden, hoeveel en welke zaken zijn misgegaan door het ontbreken van deze onderzoeksbevoegdheid. Graag ontvangen deze leden een nauwgezet overzicht.

De leden van de PvdD-fractie lichten graag een en ander toe. Het voorliggende wetsvoorstel maakt het mogelijk dat de politie op grote schaal met internet verbonden apparaten mag hacken. Bij hacken worden apparaten via zwakheden in de software binnengedrongen. Hier zit gelijk het pijnpunt van het wetsvoorstel. In tegenstelling tot wat de wet beoogt, vergroot het de veiligheid van Nederlanders niet. Sterker nog, door zwakheden in de software ongemoeid te laten en zelfs uit te buiten, kunnen ook kwaadwillende hackers hier gebruik van maken. Persoonlijke gegevens kunnen op grote schaal worden gestolen en de besturing van apparaten kan op afstand worden overgenomen.
Dat dit een reëel gevaar is, is de laatste dagen gebleken. De zogenoemde Glibc-bug is veelvuldig in het nieuws geweest, omdat miljoenen apparaten overgenomen zouden kunnen worden door kwetsbaarheid in een stukje code. Enkele jaren geleden was er grote paniek over de Heartbleed-bug, waardoor de persoonlijke gegevens van miljoenen gebruikers onbeschermd waren. Met het voorliggende wetsvoorstel zouden dit soort bugs niet gemeld en oplost worden, maar juist gebruikt worden door de opsporingsdiensten. Echter, als de politie een computer kan kraken, dan kan een kwaadwillende hacker dat ook. Vindt de regering het acceptabel dat de veiligheid van miljoenen apparaten aangetast wordt, alles in dienst van de hackbevoegdheid van de politie? Kan de regering uiteenzetten welke afweging is gemaakt tussen de het belang van de veiligheid van burgers tegenover de opsporingsbehoeften van de politie? Waar is de prioriteit gelegd? Graag ontvangen zij een reactie hierop van de regering.
De leden van de PvdD-fractie zijn geschrokken van de breedte van het in het wetsvoorstel gehanteerde begrip geautomatiseerd werk. Dit houdt in dat alle apparaten met een internetverbinding gehackt zouden mogen worden. In de toekomst van het «Internet of Things» zullen daar over een paar jaar vrijwel alle apparaten onder vallen, tot pacemakers, koelkasten en auto's aan toe. Het kan toch echter niet de bedoeling zijn dat de regering doelbewust zwakheden in pacemakers niet zal melden, waardoor deze ook door kwaadwillende hackers aangetast kunnen worden? Als de letter van de wet wordt gevolgd is dit namelijk de enige mogelijke conclusie. Als dit niet zo bedoeld is, is de regering dan bereid de wet aan te passen en specifiek aan te geven welke apparaten wel en niet gehackt mogen worden?
De aan het woord zijnde leden merken op dat hoewel het wetsvoorstel wordt genoemd als een belangrijk middel om cybercriminelen aan te pakken, de toepassing van het wetsvoorstel niet beperkt is tot cybercriminaliteit. Het opent de deur naar een veel bredere toepassing van de wet, breder dan nu kan worden overzien. Dat dit snel uit de hand kan lopen hebben we in de jaren '70 gezien, toen de telefoontap werd ingevoerd. Deze zou, zo werd bij de invoering gezegd, slechts enkele keren per jaar worden ingezet. Ondertussen weten wij wel beter. In het tijdperk van het Internet of Things geeft het wetsvoorstel de politie feitelijk een oncontroleerbare hackbevoegdheid om in alle met internet verbonden apparaten in te kunnen breken bij verdenking van een misdrijf. Bij welke misdrijven dit zou zijn toegestaan is onduidelijk, want de wet laat alle ruimte voor interpretatie. Is de regering bereid expliciet aan te geven welk misdrijf wel en welk misdrijf niet in aanmerking zal komen om onder de wet te kunnen vallen en hier harde criteria voor op te stellen?
De leden van de PvdD-fractie constateren dat het wetsvoorstel in principe de mogelijkheid openlaat dat bij een simpele burenruzie ingebroken kan worden op bijvoorbeeld een telefoon, om vervolgens de GPS aan te zetten

en de persoon in kwestie digitaal te volgen. Wellicht buitenproportioneel maar juridisch gezien niet onmogelijk en dat baart deze leden zorgen. Bovendien mag de politie ook camera's en microfoons aanzetten. Op deze manier kan een verdachte op afstand afgeluisterd worden. Maar hoe zit het dan met de huisgenoten van de verdachte? Een computer, bijvoorbeeld, bevat niet alleen gegevens van de persoon zelf maar ook van vrienden, familie en netwerken. Welke waarborgen geeft de wet dat hun privacy niet aangetast wordt? Hoe voorkomt de regering dat deze wet leidt tot een «dragnet», waar ook de omgeving van een verdachte in meegetrokken wordt?
Deze leden zetten vraagtekens bij de bredere inzet van het wetsvoorstel als efficiencymiddel. Wat is de implicatie van de financiële paragraaf, waarin staat dat er kosten kunnen worden bespaard met de inzet van de bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen? Is het uitgesloten dat de hackbevoegdheid ook in andere domeinen kan worden toegepast? Deelt de regering de mening dat efficiency nooit een drijfveer zou mogen zijn als het gaat om de veiligheid, de grondrechten en de privacy van burgers?

2.2 De reikwijdte van de voorgestelde bevoegdheid en de plaatsing in het Wetboek van Strafvordering

De leden van de PvdA-fractie vragen naar aanleiding van een reactie van de ANWB of tot een geautomatiseerd werk, zoals in het wetsvoorstel is bedoeld, ook een «connected car» of connecties infotainment/navigatiesysteem met de daarbij behorende servers behoren? Zo ja, krijgt daarmee de politie op grond van het voorliggend wetsvoorstel de bevoegdheid op afstand en heimelijk een dergelijk geautomatiseerd werk te onderzoeken? Mag de politie deze of een eventueel andere bevoegdheid gebruiken om dan ook op afstand een voertuig staande te houden? Zo ja, wat mag de politie doen om het voertuig op afstand te stoppen, waar wordt dat in de wet of onderlinge regelgeving vastgelegd en hoe verhoudt die bevoegdheid om op afstand een voertuig staande te houden zich tot de veiligheid van de verkeersdeelnemers? Zo nee, waarom is het uitgangspunt van de ANWB dat het voorliggend wetsvoorstel genoemde bevoegdheid zou creëren onjuist?

De leden van de CDA-fractie vragen de regering dieper in te gaan op de keuze het binnendringen in een geautomatiseerd werk als bijzondere opsporingsbevoegdheid aan te merken. Geldt voor alle bijzondere opsporingsbevoegdheden dat dit heimelijk gebeurt, dat wil zeggen zonder dat de verdachte daar kennis van draagt? Zo nee, waarom dan toch deze keuze? Kan de regering ingaan op de situatie dat de verdachte bij de toepassing van deze bevoegdheden wel degelijk lucht krijgt van het ingrijpen door politie en justitie. Vervalt dan de oorspronkelijke argumentatie van de regering om deze bevoegdheid aan te merken als bijzonder en hiermee samenhangend veel zwaardere voorwaarden te stellen voor de toepassing daarvan?
De aan het woord zijnde leden vragen met betrekking tot de verschoningsregeling, die wordt voorgesteld bij het inzetten van deze bevoegdheid, hoe in de praktijk bepaald wordt dat er sprake is van een geheimhoudingsrelatie. In het bijzonder de relatie met een geestelijke kan hier vragen oproepen, want kan hieronder bijvoorbeeld ook een imam geschaard worden? Vallen chatgesprekken en/of e-mailuitwisselingen tussen een radicaliserende verdachte en een zogeheten haatprediker hieronder? Deze leden vragen of de regering de mening deelt dat het in dat kader gewenst is dat dergelijke informatie inzichtelijk wordt voor politie en justitie. Zo ja, hoe gaat zij borgen in onderhavig wetsvoorstel dat hiervoor een uitzondering wordt gecreëerd? Zo nee, waarom niet, gelet op het Actieplan Jihadisme?

De leden van de CDA-fractie vragen nog los van de specifieke situatie met betrekking tot radicalisering hoe voorkomen gaat worden dat het verschoningsrecht zal worden misbruikt door kwaadwillenden. Als een map op de harde schijf van een personal computer (pc) «medisch dossier» of «gesprekken met mijn advocaat» wordt genoemd, staan de seinen dan direct op rood voor politie en justitie of mogen zij wel degelijk verder zoeken naar de informatie die hierachter ligt?
Hoe worden bovenstaande aandachtspunten verwerkt in het aangekondigde Besluit bewaren en vernietigen niet gevoegde stukken, zo vragen deze leden. Met betrekking tot dit besluit vragen zij of wordt gecontroleerd of door advocaten opgegeven nummers inderdaad nummers van advocaten betreffen en niet een dekmantel vormen voor contact met andere personen. Zo nee, waarom niet? Hoe kan gegarandeerd worden dat het verschoningsrecht op dit punt niet wordt misbruikt?
De leden van de CDA-fractie vragen tevens of de regering het medisch beroepsgeheim afdoende kan borgen en bewaken, ook en juist als de verschoningsgerechtigden zelf verdachte zijn.

De leden van de D66-fractie hebben grote vraagtekens bij het brede toepassingsterrein. Niet alleen bij ernstige vormen van computercriminaliteit maar ook bij criminaliteit gepleegd met behulp van geautomatiseerd werk kan de voorgestelde bevoegdheid tot heimelijk binnendringen worden ingezet. Deze leden vragen de regering een overzicht te geven van alle soorten misdrijven waarvoor de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruikt kan worden. Waarom is niet gekozen voor een gesloten lijst van delicten en, gezien de ingrijpendheid van de bevoegdheid, een beperking tot levensbedreigende en terroristische delicten?
De aan het woord zijnde leden merken op dat de voorgestelde bevoegdheid niet alleen ziet op reeds aanwezige gegevens, maar ook wordt beoogd daarmee toegang te kunnen krijgen tot nog niet aanwezige gegevens. In de memorie van toelichting wordt gesproken over inzet van de bevoegdheid met het oog op de toepassing van bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Naar welke doelen verwijst de regering?
De leden van de D66-fractie hebben een punt van zorg ten aanzien van de kring van personen die kunnen worden getroffen door deze bevoegdheid te weten, de verschoningsgerechtigden. De regering verwijst naar een bestaande regeling van artikel 126aa, tweede lid, Sv. Op grond waarvan acht de regering dat voldoende waarborg aanwezig is in het licht van de nieuwe bevoegdheid die zij voorstelt? De informatie is dan immers al door de handen van de politie gegaan. Dient op enig moment minstens een registratie van de kennisneming van gegevens en de vernietiging daarvan plaats te vinden, alsmede achteraf een notificatie jegens de verschoningsgerechtigde?
De aan het woord zijnde leden merken op dat voor de positie van journalisten wordt verwezen naar het wetsvoorstel bronbescherming in strafzaken. Betekent die verwijzing dat journalisten niet beschermd zijn tegen inbreuken, zoals in onderhavig wetsvoorstel voorgesteld, totdat de Wet bronbescherming in strafzaken in werking is getreden?
De leden van de D66-fractie lezen voorts dat de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk onder andere gebruikt mag worden bij DDoS-aanvallen. Klopt het dat DDoS-aanvallen uitgevoerd worden door gebruik te maken van Botnets, die zijn opgezet door gebruik te maken van fouten in software van computers, mobieltjes, tablets en andere apparaten? Klopt het dat de regering door middel van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruik maakt van fouten in de software? Klopt het dat de fouten in de software die gebruikt worden door de politie om een geautomatiseerd werk binnen te dringen dezelfde fouten zouden kunnen zijn als de fouten

die criminelen gebruiken om Botnets op te zetten? Ziet de regering de tegenstrijdigheid van deze benadering? Is het niet beter om ervoor te zorgen dat fouten gedicht worden zodat het überhaupt moeilijker wordt om Botnets op te zetten? Deelt de regering de mening dat dat een grotere impact zal hebben op het aantal DDoS-aanvallen?
De aan het woord zijnde leden lezen dat de procedure van nummerherkenning ook wordt gewaarborgd bij het onderzoek in een geautomatiseerd werk. Kan de regering toelichten hoe dit in de praktijk werkt? Stel dat er een «keylogger» wordt geïnstalleerd op een smartphone. Hoe wordt in dat geval de «logging» stil gezet zodra de verdachte een whatsapp bericht verstuurd naar zijn advocaat? Kan de regering toelichten hoe omgegaan wordt met een concept e-mailbericht van een verdachte aan een advocaat?
De leden van de D66-fractie constateren dat het begrip «geautomatiseerd werk» zeer breed is gedefinieerd, namelijk «een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken». Deze leden constateren dat elk apparaat dat aangesloten is op het internet of een apparaat dat verbonden is met een apparaat dat op het internet aangesloten is onder deze definitie valt. Dus ook auto's, pacemakers, smart tandenborstels, teddy beren, MRI-scanners, «wearables», medische apparatuur, etc. Kan de regering toelichten waarom voor deze brede definitie gekozen is? Waarom is niet gekozen voor een beperkte lijst van apparaten, zoals smartphones, tablets en pc's?

De leden van de GroenLinks-fractie vragen of de toepassing van deze hackbevoegdheid niet nauwkeuriger moet worden afgebakend. Het komt deze leden voor dat een breed scala aan delicten zich in beginsel leent voor toepassing. Ligt het niet meer voor de hand dit expliciet te beperken tot een aantal specifieke delicten?
Deze leden vragen voorts wat onder geautomatiseerde werken wordt verstaan. Vallen daar bijvoorbeeld ook motorvoertuighard- en software, geavanceerde medische hulpmiddelen en domotica (huisautomatisering) onder? Kan de regering een afbakening geven welke geautomatiseerde werken wel en welke niet voor toepassing van de hackbevoegdheid in aanmerking komen?

2.3 De doelen van het onderzoek in een geautomatiseerd werk

2.3.1 De vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan
De leden van de D66-fractie lezen in het wetsvoorstel dat het onderzoek in een geautomatiseerd werk uitsluitend kan plaatsvinden met het oog op het verrichten van bepaalde onderzoekshandelingen. De leden van de D66-fractie hebben daar vele vragen over.
Deze leden lezen dat er sprake is van een virtuele plaatsopneming of inkijkoperatie. Begrijpen zij het goed dat ook in de volgende fase, waarin verder wordt opgetreden ten aanzien van een geautomatiseerd werk, dat dat nog steeds heimelijk plaatsvindt en dus buiten de wetenschap van de onderzochte persoon om? Kan de regering in dit kader toelichten waar precies de overgang ligt tussen technisch optreden en tactisch optreden ten aanzien van geautomatiseerde werken?
De aan het woord zijn de leden merken voorts op dat de bevoegdheid van onderzoek in het geautomatiseerde werk is beperkt tot een geautomatiseerd werk dat bij de verdachte in gebruik is. Zij stellen dat «in gebruik» is niet hetzelfde als diens eigendom. Begrijpen de leden van de D66-fractie het goed dat het dus ook om geleende of gestolen apparaten kan gaan waarop zich informatie van anderen kan bevinden? Wat betekent dat voor de bewijsvoering waarbij aangetoond moet worden dat de gegevens

toebehoren aan de verdachte persoon als gebruiker en niet aan de persoon die het apparaat toebehoort?

2.3.2 De vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen
De leden van de VVD-fractie vragen of er bewaartermijnen zijn verbonden aan de vastgelegde gegevens die in het geautomatiseerde werk zijn of worden opgeslagen. Zo ja, hoe zien deze bewaartermijnen eruit?
Deze leden merken op dat de vastlegging betrekking heeft op gegevens die specifiek van belang zijn voor de waarheidsvinding inzake ernstige strafbare feiten. Wat gebeurt er met gegevens of informatie die tijdens het onderzoek worden ingezien die geen betrekking hebben op het specifieke doel van het onderzoek? Wat wordt er in dit kader bedoeld met gegevens die «redelijkerwijs» nodig zijn om de waarheid aan de dag te brengen? Hoe wordt voorkomen dat bij het verrichten van onderzoek in een geautomatiseerd werk de gegevens, en daarmee de privacy, van anderen dan de verdachte tegen wie het onderzoek gericht is, wordt geschonden, zo vragen de aan het woord zijnde leden.

De leden van de CDA-fractie vragen of het meekijken met emailverkeer tevens behelst dat niet alleen verzonden informatie kan worden bekeken, maar eveneens de door de regering eerder genoemde praktijk dat berichten in een concept-box worden geplaatst en aldaar door meerdere personen bekeken kunnen worden via het delen van inloggegevens.
Deze leden vragen ook in hoeverre toegang mogelijk is tot reeds verwijderde bestanden in het geheugensysteem van het betreffende apparaat, vergelijkbaar met de wijze waarop deze door de gebruiker zelf of door een systeembeheerder kunnen worden teruggevonden.
De leden van de D66-fractie lezen dat de vastlegging van gegevens, die in het geautomatiseerde werk zijn opgeslagen of die na het tijdstip van de afgifte van het bevel worden opgeslagen, een belangrijke bevoegdheid is. Staat er in het bevel een bepaalde termijn waarbinnen gegevens moeten worden vastgelegd of kan de politie jarenlang de hacksoftware op een apparaat houden, wachtend op mogelijke strafbare feiten? De regering stelt dat met speciale software het internetgebruik van een verdachte kan worden gevolgd. Welke software bedoelt de regering precies? Welke software gaat de regering gebruiken om invulling te geven aan de «keylogger»-functie? Hoe wordt de «keylogger» op de computer of smartphone aangebracht?

2.3.3 De ontoegankelijkmaking van gegevens
De leden van de CDA-fractie vragen of de beoordeling van de keuze welke maatregel het meest gewenst is, tevens behelst de afweging om gegevens bewust intact te laten in plaats van te verwijderen. Legitieme redenen hiervoor zouden kunnen zijn dat hiermee uiteindelijk (ernstige) strafbare feiten kunnen worden ontdekt en/of worden opgespoord. Een andere reden zou ook kunnen zijn de afweging om de verdachte niet wakker te schudden met (onbewust) achtergelaten sporen. Graag vernemen zij hierop een reactie van de regering.
De leden van de D66-fractie vragen aan welke strafbare feiten de regering denkt als wordt gesteld dat gegevens ook ontoegankelijk kunnen worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Hoe verhoudt het ontoegankelijk maken zich tot het doel juist heimelijk een geautomatiseerd werk binnen te dringen zonder dat de betreffende persoon daar weet van heeft?
Deze leden vragen over welke te verwijderen gegevens de regering het heeft als zij stelt dat «(o)nder ontoegankelijkmaking (mede) wordt (...) verstaan het verwijderen van gegevens uit geautomatiseerd werk, maar met behoud van gegevens ten behoeve van de strafvordering

(artikel 125o, tweede lid, Sv)». Als er geen strafrechtelijk relevante grond is om gegevens te behouden, waarom zou dan overgegaan moeten kunnen worden tot het verwijderen ervan?
De definitie van ontoegankelijk maken laat een aantal maatregelen toe, zoals tijdelijk onbruikbaar, versleutelen of wissen. De aan het woord zijnde leden vragen door wie wordt bepaald welke maatregel het meest effectief, proportioneel en subsidiair is. Hoe lang kan het ontoegankelijk maken van gegevens duren? Als het om een voorlopige maatregel gaat waarbij de rechter in de einduitspraak beslist over de ontoegankelijk gemaakte gegevens, hoe wordt de toegankelijkheid hersteld indien gegevens zijn gewist?
De leden van de D66-fractie lezen dat met behulp van hardware een ingang van een computer (tijdelijk) onbruikbaar kan worden gemaakt. Kan de regering dit toelichten? Wat voor hardware? Wat voor ingangen? Voorts stelt de regering over botnets dat «na een succesvolle besmetting ongemerkt meer kwaadaardige software kan worden geïnstalleerd, waaronder sniffers (computerprogramma waarmee het dataverkeer op het netwerk kan worden bekeken en geanalyseerd) en keyloggers (het vastleggen van toetsaanslagen).» Deze beschrijving van de gevolgen voor computers die onderdeel zijn van een botnet lijkt veel op de bevoegdheden die de politie met dit wetsvoorstel krijgt. Klopt het dat de apparaten die de politie gaat hacken, op basis van de bevoegdheden in dit wetsvoorstel, feitelijk een botnet zullen vormen? Klopt het dat de software die geplaatst wordt op de apparaten in contact staat met een server van de maker van de software in plaats van een server van de overheid? Voorts lezen deze leden dat het noodzakelijk is toegang te verkrijgen tot de servers die onderdeel vormen van een botnet. Gaat het in dit geval alleen om botnets waarbij aansturing vanuit een centrale server geschied of ook om peer-to-peer botnets? Betekent dit in het laatste geval dat de politie ook computers die onderdeel zijn van een botnet mogen hacken? In hoeverre is het overnemen van de servers van een centraal aangestuurde botnet een structurele oplossing? Is het niet beter om te investeren in het veiliger maken van apparaten en goede cyber hygiëne, zodat zij überhaupt geen onderdeel uit gaan maken van een botnet?

2.3.4 De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie
De leden van de SP-fractie willen weten of het aangepaste Besluit technische hulpmiddelen zal worden voorgehangen voordat het parlement zich over onderhavig wetsvoorstel uitspreekt en of het besluit ook ter consultatie op internet wordt geplaatst. Klopt het voorts dat betreffend besluit op dit moment niet voldoet aan de eisen van de digitale opsporingsbevoegdheden? Zo ja, deelt de regering de mening dat het juist van belang is dat dit besluit tijdig wordt gewijzigd, zodat de praktijk en het parlement kunnen bezien of dit zo is aangepast dat alle risico's zoveel mogelijk worden weggenomen?

De leden van de CDA-fractie vragen of het de opsporingspraktijk niet belemmert dat door middel van een apart bevel toestemming moet worden gevraagd teneinde een ander land te verzoeken instemming te verlenen een gebruiker af te tappen. Verwacht de regering niet dat juist digitale criminaliteit, waarop onderhavig wetsvoorstel betrekking heeft, in veel gevallen zich zal uitstrekken tot andere landen waar Nederland geen rechtsmacht heeft? Is het in dat kader niet wenselijk om de toestemming aan een ander land(hoeft nog geen instemming op te leveren) direct te koppelen aan de voorgestelde bevoegdheden tot aftappen en opnemen? Wat zijn de redenen die hieraan in de weg kunnen staan? Hoe zou dit wetstechnisch alsnog te realiseren zijn?
De leden van de D66-fractie constateren dat de regering verwijst naar het Cybercrimeverdrag op basis waarvan het opnemen van telecommunicatie

ook zonder de medewerking van de aanbieder kan plaatsvinden. Laat het Cybercrimeverdrag daarmee ook ruimte om zonder toestemming van de verdachte gebruiker, zijn geautomatiseerde werken heimelijk binnen te dringen en zo ja, op grond van welk artikel?
Deze leden merken op dat indien de gebruiker van het nummer dat zal worden afgetapt zich op het grondgebied van een ander land bevindt, instemming zal moeten worden verkregen van dat land voor toepassing van de bevoegdheid. Kan dat tot toepassingsknelpunten leiden bij landen die minder bereidwillig zijn mee te werken aan aftappen dan wel technisch niet zover zijn dan wel wetgeving hebben die zich daar tegen verzet? Zo ja, welke landen zouden eventueel problematisch kunnen zijn bij de uitvoering hiervan?
De leden van de D66-fractie vragen of de algemene maatregel van bestuur, waarin eisen worden gesteld aan het technische hulpmiddel dat voor het opnemen gebruikt kan worden, wordt voorgehangen zodat de Kamer kan kennisnemen van de gestelde eisen aan het technische hulpmiddel.

2.3.5 De uitvoering van een bevel tot stelselmatige observatie
De leden van de PvdA-fractie vragen of zij het goed begrijpen dat het voorliggende wetsvoorstel er ook toe strekt dat er een op zichzelf staand technisch hulpmiddel kan worden aangebracht teneinde een persoon te volgen, zoals een peilzender? Zo ja, wat heeft dat te maken met het op afstand binnendringen van een geautomatiseerd werk? Zo nee, wat wordt dan bedoeld?

De leden van de SP-fractie delen de opvatting van de Afdeling advisering van de Raad van State dat het opvallend is dat het permanent waarnemen wat zich in een woning afspeelt niet veel anders is dan het via software volgen van gegevensstromen. Dat eerste is niet toegestaan en dat laatste wordt geregeld met dit wetsvoorstel, terwijl met de hackbevoegdheid tot veel meer gegevens toegang kan worden verkregen en de inbreuk op de privacy nog groter wordt. Waarom is dat dan minder erg en vergaand dan het permanent waarnemen wat zich in een woning afspeelt door bijvoorbeeld camera's te plaatsen?

De leden van de CDA-fractie vragen of de betreffende ingezette software zo ingericht zal zijn dat de voorgestelde toepassingen ook daadwerkelijk heimelijk kunnen worden ingezet. Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software-applicaties op zijn smartphone worden geïnstalleerd?
De leden van de D66-fractie merken op dat in de toelichting een voorbeeld wordt aangehaald van een verdachte met een smartphone met een data-abonnement waarbij via de GPS-locatie kan worden nagegaan waar de verdachte zich bevindt. Kan alleen worden binnengedrongen op mobiele telefoons die voorzien zijn van een data-abonnement bij een provider? Kan dat ook op pre-paid telefoons?
Deze leden lezen dat de regering vindt dat het permanent waarnemen van wat zich in een woning afspeelt via het op afstand aanzetten van een webcam van bijvoorbeeld een smartphone of een laptop, even ingrijpend is als het betreden van een woning. Deelt de regering de mening dat het op afstand heimelijk aanzetten van een webcam ingrijpender is dan het betreden van een woning, omdat het heimelijk gebeurt en omdat dit het vertrouwen van mensen in digitale technologieën erodeert?
De leden van de D66-fractie constateren dat technische hulpmiddelen bij het hacken, zoals de software die daarvoor gebruikt wordt, moeten voldoen aan de eisen opgenomen in het Besluit technische hulpmiddelen strafvordering. Is de regering het met de leden eens dat dit besluit door beide Kamers goedgekeurd moet worden via een voorhangprocedure? Kan de regering toelichten welke eisen de regering in het besluit wil

opnemen? Deelt de regering de mening dat al bij de behandeling van dit wetsvoorstel duidelijk moet zijn wat voor eisen de regering wil stellen aan de hacksoftware? Is de regering bereid in het besluit op te nemen dat hacksoftware op apparaten niet in contact mag staan met servers van de maker van de software? Is de regering bereid in het besluit op te nemen dat hack software geen gebruik mag maken van fouten in software? Welke software gaat de regering aanschaffen om uitvoering te geven aan de hackbevoegdheid? Wat is het budget voor de aan te schaffen software? Gaat de regering software van het HackingTeam aanschaffen?
Voorts constateren de aan het woord zijnde leden dat ook eisen aan het automatische loggingsysteem nader geregeld wordet in het Besluit technische hulpmiddelen strafvordering. Deze leden menen dat dit een cruciaal onderdeel is van dit wetsvoorstel waarin de objectiviteit van de gedane handelingen en de eventueel overgenomen gegevens gegarandeerd moet worden. Kan de regering toelichten waarom er niet voor gekozen is de rechter-commissaris aanwezig te laten zijn tijdens het hacken, aangezien bij een huiszoeking de rechter-commissaris wel aanwezig is. Is het praktisch mogelijk voor de opsporingsambtenaren om de automatische logging uit te zetten en door te gaan met hacken? Is daarmee een situatie in theorie mogelijk dat de opsporingsambtenaar gegevens op een apparaat kan zetten die de verdachte niet zelf op het apparaat heeft geplaatst?
Voorts constateren de leden van de D66-fractie dat de ontwikkeling van de techniek ertoe leidt dat de reikwijdte van het verbod om een technisch hulpmiddel op een persoon te bevestigen minder strikt dient te worden uitgelegd dan voorheen. Betekent dit concreet dat de politie ook de mogelijkheid krijgt «wearables» en «pacemakers» of andere medische apparatuur te hacken? Is de regering van mening dat dit wenselijk is, gezien de gevoelige informatie die op dit soort apparaten staat en gezien het feit dat deze apparaten door de hackbevoegdheid onveilig blijven doordat fouten in de software in stand gehouden worden? Is de regering bereid de hackbevoegdheid niet te laten gelden voor geautomatiseerde werken die zich op (of in) een persoon bevinden?

2.4 De juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie merken op dat voor een inbreuk op het recht op vertrouwelijke communicatie een rechterlijke toets vooraf noodzakelijk is. Deze leden vragen hoe dit vooraf mogelijk is als niet op voorhand duidelijk is of in een geautomatiseerd werk privégegevens zijn opgeslagen. Moet er altijd van worden uitgegaan dat er mogelijk gestuit wordt op privégegevens? Dient er dus altijd een rechterlijke toets aan vooraf te gaan?

De leden van de CDA-fractie vragen de regering of zij de mening deelt dat het verzoek tot machtiging, en dus ook de verlening, zo zorgvuldig maar tegelijkertijd ook zo volledig mogelijk ingekleed dient te worden door politie en justitie. Dit gelet op het belang van het voorkomen van uiteindelijk onrechtmatig verkregen bewijs door politie en justitie. Wordt rekening gehouden met het aantreffen van mogelijk nieuwe strafbare feiten waarvoor de bevoegdheid kan worden ingezet? Zo ja, op welke wijze? Zal ook altijd rekening worden gehouden met de mogelijkheid dat meerdere personen gebruik kunnen maken van het betreffende apparaat, ook al is nog niet precies duidelijk hoe groot deze kring van personen is en uit wie deze bestaat? Of dient in dat laatste geval weer een nieuw bevel te worden afgegeven? Dat laatste zou zeer belemmerend zijn voor de opsporingspraktijk, zo menen deze leden. Deelt de regering deze mening? Zo ja, hoe lost zij dat op in onderhavig wetsvoorstel?

De leden van de CDA-fractie vragen of het gegeven dat onbekend of juist al duidelijk is dat de gegevens niet in Nederland zijn opgeslagen of vastgelegd, een legitieme grond kan vormen voor de rechter-commissaris om geen machtiging af te geven. Deelt de regering de mening dat een gebrek aan informatie op dit punt geen belemmering mag vormen voor het inzetten van bevoegdheden wanneer de verdenking van strafbare feiten (voor het overige) voldoende is aangetoond? Deelt de regering ook de mening dat het in het belang van de veiligheid van andere landen is indien opsporingsbevoegdheden (aldaar) kunnen worden ingezet? Hoe legt de regering de wijziging die zij heeft doorgevoerd naar aanleiding van het advies van Afdeling advisering van de Raad van State uit? Vormt dat niet een afzwakking van de inzet van de voorgestelde bevoegdheden door de opsporingsdiensten?
De leden van de CDA-fractie begrijpen de strikte scheiding die de regering beoogt tussen het opsporingsteam enerzijds en het technische team dat de bevoegdheden toepast anderzijds. Tegelijkertijd vragen zij of de regering de mening deelt dat in de praktijk juist van belang is dat deze teams goed met elkaar communiceren en geen verdere belemmeringen op dit punt worden opgelegd, ook niet in lagere regelgeving.

De leden van de D66-fractie merken op dat de regering erkent dat sprake is van een zeer ingrijpende bevoegdheid waarvoor strikte waarborgen nodig zijn. Niettemin lezen deze leden in het wetsvoorstel dat de bevoegdheid ook misdrijven kan betreffen die bij algemene maatregel van bestuur worden aangewezen, waarop geen gevangenisstraf van acht jaar of meer staat maar die wel worden gepleegd met behulp van een geautomatiseerd werk en waarbij duidelijk maatschappelijk belang is bij beëindiging van de strafbare situatie en de vervolging van de daders. Waarom wordt ervoor gekozen bij algemene maatregel van bestuur te voorzien in de reikwijdte van het wetsvoorstel en deze niet volledig in het wetboek te regelen? Wat betekent deze bepaling voor de strafvorderlijke waarborgen, die juist noodzakelijk zijn bij het toepassen van een zeer ingrijpende opsporingsbevoegdheid? Is de regering voornemens de algemene maatregel van bestuur aan de Kamer te doen toekomen in het kader van de verdere behandeling van onderhavig wetsvoorstel?
De leden van de D66-fractie merken op dat een toetsing van de bevoegdheid door de rechter moet zorgdragen voor bescherming van burgers tegen willekeurige inmenging door de overheid in zijn of haar privéleven. Daarbij dient de rechter-commissaris te toetsen aan alle wettelijke vereisten en strekt de machtiging zich uit over alle onderdelen van het bevel. Hoe meent de regering te gaan voorzien in voldoende specialistische kennis bij de rechterlijke macht, en rechter-commissarissen in het bijzonder, van de technische aspecten die met de toepassing van de bevoegdheid gepaard gaan en de ingrijpendheid van de bevoegdheid bepalen?
De aan het woord zijnde leden lezen dat het bevel van de officier van justitie ook aan een aantal nauwkeurig omschreven eisen dient te voldoen. Daarbij is kennis vereist van het technische hulpmiddel dat zal worden ingezet en welke handelingen met behulp van dat technische hulpmiddel kunnen worden verricht en wat dat betekent voor de verdachte die het betreft. Hoe meent de regering te voorzien in voldoende specialistische kennis bij de daartoe aangewezen officieren van justitie die een dergelijk bevel kunnen afgeven? Is in deze alleen een rol toebedacht aan de officier van justitie of heeft ook de hulpofficier van justitie hier enige rol? Zo ja, welke?
De leden van de D66-fractie lezen dat de regering van plan is routers binnen te dringen om achter de identificerende gegevens van een apparaat te komen (een IP-, of MAC-adres of IMEI of IMSI-nummer). Kan de regering toelichten wat voor soort routers zullen worden binnengedrongen? Gaat het hier vooral om thuisnetwerken of Wi-Fi-hotspots of

gaat het ook om zogenaamde enterprise routers die netwerken van internetaanbieders (ISP's) met elkaar verbinden? Wordt bij het binnendringen van de routers ook de software, de zogeheten firmware, aangepast? Welke software wordt er voor het binnendringen gebruikt? Wat wordt er gedaan met de datapakketjes die de router moet doorgeven? Worden er aanpassingen gedaan aan het routingprotocol? Worden de datapakketjes ingezien door middel van «deep-packet-inspection» of wordt alleen de «header» gelezen? Wat wordt er gedaan met de lijsten van IP-adressen die door het binnendringen van een router verkregen worden?
Het wetsvoorstel spreekt over het afgeven van een bevel en vervolgens een machtiging. Wie houdt tijdens de uitvoering van de bevoegdheid toezicht op de toepassing ervan? Begrijpen deze leden het voorstel juist als zij constateren dat alleen wordt voorzien in het zogeheten logging waarin de verrichtte handelingen worden vastgelegd? Indien dat laatste het geval is, wie controleert de logging op juistheid?
De leden van de D66-fractie constateren dat voor het binnendringen van geautomatiseerde werken, hetgeen het meest ingrijpend is voor de persoonlijke levenssfeer (zoals het doorzoeken van alle gegevens in het geautomatiseerde werk en het overnemen daarvan), de verdenking van een misdrijf vereist is waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen en dat een ernstige inbreuk op de rechtsorde oplevert. Voorts stelt de regering dat de bij algemene maatregel van bestuur aan te wijzen misdrijven, misdrijven betreffen waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld, maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Deelt de regering de mening dat deze definitie zeer breed is? Kan zij een overzicht geven wat voor misdrijven onder de bij algemene maatregel van bestuur aan te wijzen misdrijven vallen?

De leden van de ChristenUnie-fractie merken op dat in het Wetboek van Strafvordering vaker gebruik wordt gemaakt van de machtiging van de rechter-commissaris, zoals ook in dit wetsvoorstel. De situatie van artikel 126 nba, vierde lid, Sv is bijvoorbeeld te vergelijken met toestemming voor telefoontaps. Kan de regering aangeven hoe vaak een tapverzoek door de rechter-commissaris wordt afgewezen en hoe vaak de machtiging wel wordt verleend? Kunnen daarin ook categorieën van gronden voor afwijzing worden onderscheiden?
Deze leden constateren dat de regering niet geheel gevolg heeft gegeven aan het advies van Afdeling advisering van de Raad van State de binnendringingsbevoegdheid meer in lijn te brengen met de proportionaliteits- en subsidiariteitsvereisten in artikel 8 EVRM. Vindt de regering desondanks dat de juridische risico's met dit wetsvoorstel zijn ondervangen op dit punt? Zo ja, waarom? De aan het woord zijnde leden constateren dat van verschillende kanten is gewezen op de risico's van onvoldoende internationaalrechtelijke stevigheid voor het personeel dat de binnendringing uitvoert. Kan de regering daar specifiek op reageren?

2.5 De inzet van de bevoegdheid

De leden van de VVD-fractie lezen dat een globale inschatting wordt gemaakt van de barrières voor het onderzoek in het geautomatiseerde werk, in het bijzonder op het gebied van de beveiliging. Kan toegelicht worden op basis van welke informatie deze inschatting wordt gemaakt?
Deze leden lezen dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig in te schatten zijn en de risico's soms pas volledig(er) in beeld komen nadat is binnenge-

drongen. Wordt hier nog iets tegenover gesteld? Is er een waarborg die dit probleem ondervangt?
De leden van de VVD-fractie lezen dat de officier van justitie en de rechter-commissaris niet bij uitstek deskundig zijn om de technische risico's te beoordelen. Welke conclusie wordt hier aan verbonden? Dienen zij hun oordeel te baseren op de deskundigheid van de opsporingsambtenaren? Zo ja, is er dan nog in voldoende mate sprake van een onafhankelijke beoordeling?
De aan het woord zijn leden merken op dat het heimelijk binnendringen op afstand in een geautomatiseerd werk gebeurt door deskundige (technische) opsporingsambtenaren. Wordt er in de Contourennota Rijksrecherche en het opleidingsaanbod bij de Politieacademie rekening gehouden met de steeds grotere vraag bij de politie naar deze specialisten? Geldt zowel voor de tactische als voor de technische opsporingsdiensten dezelfde screening? Voor de inzet van softwareapplicaties is een voorafgaande keuring van het technische hulpmiddel vereist. De leden van de VVD-fractie vragen wie een dergelijke keuring uitvoert.
Deze leden vragen of mensen achteraf op de hoogte worden gesteld als hun geautomatiseerd werk, achteraf gezien onterecht, heimelijk is binnengedrongen. Zo nee, wat zijn de overwegingen om dit niet te doen?
De aan het woord zijnde constateren dat het decryptiebevel niet langer in het wetsvoorstel staat. Welke instrumenten staan de politie in plaats daarvan ter beschikking? Kan er bij het antwoord op deze vraag eveneens ingegaan worden op de discussie over zwakheden in het systeem die bekend zijn en die niet bekend zijn, de zogeheten «zero days»-discussie?

De leden van de PvdA-fractie merken op dat in de verkennende fase voor de daadwerkelijke inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk wordt bekeken welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn of er meerdere gebruikers zijn, welk besturingssysteem is geïnstalleerd enz. Echter, zo vragen deze leden, is voor die verkenning het niet meteen nodig om op afstand in dat geautomatiseerd systeem binnen te dringen en onderzoek te doen? Of kan met behulp van andere opsporingsbevoegdheden deze informatie ook verkregen worden? Zo ja, welke? Is er een verschil tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem? Zo ja, zijn daar dan ook verschillende bevoegdheden voor nodig? Kan een computer op afstand worden binnengedrongen zonder een machtiging van de rechter-commissaris voor het op afstand heimelijk onderzoeken van een geautomatiseerd werk? Wat gebeurt er met verdachte informatie die al tijdens de verkennende fase in een geautomatiseerd werk gevonden wordt? Stel bijvoorbeeld dat er een map met de naam «kinderporno» gevonden wordt, hoe moet de opsporingsambtenaar er dan in deze verkennende fase mee om gaan?
De leden van de PvdA-fractie lezen dat de politie gebruik kan maken van zwakten in een systeem om via die weg het systeem binnen te dringen. Zijn er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen? Zo ja, welke mogelijkheden zijn dat? Kan de politie zelf zwakten op afstand in een systeem aanbrengen? In welke mate zijn systeemzwakten van belang voor de politie om een geautomatiseerd systeem binnen te dringen? Kunnen via het lek dat de politie zelf creëert of waar het gebruik van maakt ook anderen dat systeem binnendringen? Waarom zouden «exploits» als kwetsbaarheid wel snel opgelost kunnen worden en de andere manieren die de politie gebruikt om een systeem binnen te dringen niet onschadelijk kunnen worden gemaakt? Wie gaat technische hulpmiddelen die gebruikt gaan worden vooraf keuren?
De leden van de PvdA-fractie zouden niet graag zien dat door de politie aangetroffen zwakheden in een systeem verhuld blijven omdat de politie die zwakheden voor opsporingsdoeleinden wil blijven gebruiken. Hoe

verhoudt de bevoegdheid om op afstand heimelijk een geautomatiseerd 0291
werk te onderzoeken zich tot de plicht om datalekken te melden? Is ook de politie aan die meldplicht gehouden?
De leden van de PvdA-fractie merken op dat een eigenaar van een geautomatiseerd werk die merkt dat iemand zijn systeem binnendringt of bijvoorbeeld pogingen doet daar een «trojan» of andere vormen van software heimelijk te plaatsen, is gerechtigd en onder voorwaarden zelfs verplicht daar maatregelen tegen te treffen. Het beschermen van de cybersecurity is immers van groot belang voor die eigenaar zelf en ook voor degenen die gebruik maken van zijn systemen. Toch zullen opsporingsambtenaren vanuit het oogpunt van het voorkomen van cybercrime gebruik gaan maken van zwakheden in een geautomatiseerd werk om daarin binnen te kunnen dringen en onderzoek te kunnen doen. In hoeverre kan het doel van de bescherming van de cybersecurity, daaronder de integriteit en veiligheid van het internet begrepen, botsen met het doel van het voorkomen van cybercrime waaronder het onderzoeken van geautomatiseerde werken? Is een eigenaar van een geautomatiseerd werk die merkt dat derden zijn werk binnendringen gerechtigd om daar maatregelen tegen te nemen, ook al gebeurt dat binnendringen door een daartoe tevens gerechtigde opsporingsambtenaar? Zo ja, waarom? Zo nee, waarom niet? Kan een eigenaar van een geautomatiseerd werk die merkt dat iemand zijn systeem probeert binnen te dringen onderscheid maken tussen iemand die dat met verkeerde bedoelingen doet en een opsporingsambtenaar? Mag een eigenaar van bijvoorbeeld een server, die zelf niet verdacht is en waar een opsporingsambtenaar heimelijk onderzoek wil doen, een dergelijke poging verhinderen? Maakt het daarbij uit of hij weet dat het een opsporingsambtenaar is dan wel iemand die niet gerechtigd is onderzoek op zijn server te doen? Maakt het daarbij uit of de eigenaar van een geautomatiseerd werk, die merkt dat iemand dat werk probeert binnen te dringen, specifieke maatregelen gericht tegen die aanval van buitenaf neemt of dat doet door bijvoorbeeld generiek de beveiliging van zijn systeem hard- of softwarematig beter te beveiligen? Zo ja, wat is het verschil?

De leden van de SP-fractie lezen dat kwetsbaarheden in een computer kunnen worden geëxploiteerd, zoals door fouten of lekken in de software te gebruiken. Het gaat hier bijvoorbeeld om zogenaamde «zero-days». Betekent dit niet ook dat het van belang kan zijn voor de overheid om deze lekken niet te dichten? In hoeverre wordt een softwarefabrikant, eindgebruiker of het Nationaal Cyber Security Centrum (NCSC) op de hoogte gesteld van een kwetsbaarheid als deze is geconstateerd door opsporingsinstanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan? Worden deze aan hen gemeld zodat deze kunnen worden opgelost?
Deze leden merken op dat de regering stelt dat de politie geen baat heeft bij instandhouding van onbeveiligde systemen vanwege de maatschappelijke kosten. Kan de regering dit nader toelichten? Kunnen politie en Openbaar Ministerie (OM) ook heimelijk binnendringen zonder gebruik te maken van «zero days»? Of zijn er per definitie kwetsbaarheden nodig? Hoe staat de conclusie van het in april 2015 verschenen rapport van de WRR («De publieke kern van het internet») dat het functioneren en de integriteit van de publieke kern van het internet veilig gesteld moet worden en beschermd moet worden tegen oneigenlijke interventies door staten en andere partijen, in verhouding tot de hackbevoegdheid voor opsporingsdiensten?
De leden van de SP-fractie hebben vragen over de vergelijking met de telefoontap. Ook daarvan werd aangegeven dat deze zo summier mogelijk zou worden ingezet. Hoe wordt voorkomen dat het heimelijk binnendringen uiteindelijk meer standaard wordt dan uitzondering?

De aan het woord zijnde leden lezen over «social-engineering» en het verleiden van personen om te reageren op bijvoorbeeld een e-mailbericht teneinde inloggegevens te verkrijgen. Waarom zijn deze opsporingsmethodes niet voldoende?
De leden van de SP-fractie vinden het opvallend dat Duitsland en Frankrijk hebben afgezien van het gebruik van spyware, omdat oneigenlijk gebruik door derden en politie niet viel uit te sluiten. Waarom gelden dit argument niet voor Nederland? Hoe groot is dit risico? In de memorie van toelichting wordt gesproken over het belang van goede keuring, maar dan is het deze leden niet duidelijk waarom Duitsland en Frankrijk dit onvoldoende hebben geacht om alsnog gebruik te maken van spyware. Als dit de oplossing is, waarom maken deze twee landen daar geen gebruik van?

De leden van de CDA-fractie vragen of de opsomming in de eerste alinea formele eisen betreft om over te gaan tot daadwerkelijk uitvoering. Indien dat het geval is, vragen zij hoe hieraan in de praktijk kan worden voldaan. Immers, hoe kan van tevoren worden vastgesteld wel programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturingssysteem is, wie er allemaal gebruik van maakt, etc.? Zijn dit niet juist allemaal onderdelen die door toepassing van de bevoegdheid inzichtelijk moeten worden voor politie en justitie?
Ten aanzien van de risico's vragen deze leden wat precies de formele voorwaarden zijn in de praktijk. Juist omdat niet duidelijk is wat kan worden aangetroffen, zal nooit een volledige inschatting te maken zijn van de inbreuk op de persoonlijke levenssfeer of schade die optreedt aan software van de gebruiker. Hetzelfde geldt voor de uiteindelijke kosten die hiermee gemoeid zullen zijn. De aan het woord zijnde leden vragen daarom of met een «uitgebreide» afweging in dit kader niet vooral een «zorgvuldige» afweging wordt bedoeld. Deze leden zijn van mening dat een globale risico-inschatting gewenst is, maar menen dat voorkomen moet worden dat opsporingsambtenaren in de praktijk per casus een volledig boekwerk moeten opstellen over de details van het apparaat dat zij op het oog hebben en omvang van de operatie die met het inzetten van de bevoegdheid gepaard gaat. Ziet de regering dit ook zo en hoe krijgt dit (beperkt) vorm in onderhavig wetsvoorstel en/of lagere regelgeving?
De aan het woord zijnde leden vragen naar de balans tussen het aanbieden van een redelijke vergoedingsmaatregel en het faciliteren door de overheid van het indienen van (talloze en onnodige) claims na iedere inbreuk op een apparaat. Hoe kan worden aangetoond dat bepaalde apparatuur en/of software daadwerkelijk is beschadigd door ingrijpen van de politie of dat het niet gewoon ouderdom van het apparaat betreft dan wel fouten in de oorspronkelijk geïnstalleerde software? Graag vernemen deze leden of de regering nog meer voorbeelden en/of uitzonderingen in gedachten heeft en hoe zij dit verwerkt in de aangekondigde regeling voor schadevergoeding. Ook vragen zij de regering heel expliciet de bewijslast voor eventueel ontstane schade neer te leggen bij de gebruiker, gelet op de administratieve en juridische lasten die dit met zich zou meebrengen voor de politie, maar ook in het licht van het voorkomen van een claimcultuur. Zij vragen de regering voorts om aan te geven of zij maximumbedragen aan vergoedingen in gedachten heeft bij de voorgestelde regeling. Dit bijvoorbeeld gelet op de mogelijkheid dat iemand die onherroepelijk is veroordeeld tot het vervaardigen en verspreiden van kinderpornografie, vervolgens met duizenden euro's door de Staat gecompenseerd wordt voor eventuele schade in diens apparaat of software. Deelt de regering de mening dat dit laatste niet is uit te leggen aan slachtoffers en/of nabestaanden van ernstige misdrijven?

De leden van de D66-fractie merken op dat vier fasen worden beschreven die plaatsvinden bij toepassing van de bevoegdheid. Wordt voor iedere

fase afzonderlijk een bevel door de officier van justitie en een machtiging door de rechter-commissaris afgegeven?
Deze leden lezen dat in de fase van het onderzoek van het geautomatiseerd werk eventueel een technische hulpmiddel wordt geplaatst. Kan de regering aangeven in welke gevallen het niet nodig is een technisch hulpmiddel te plaatsen en toch een geautomatiseerd werk binnengedrongen kan worden?
De aan het woord zijnde leden constateren dat de verkennende fase bedoeld is om, voorafgaand aan eventuele daadwerkelijke inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk, een goed beeld te verkrijgen van de mogelijkheden om daadwerkelijk toegang te verkrijgen tot het geautomatiseerde werk en de daaraan verbonden risico's. Dit zou betekenen dat er tijdens de verkennende fase nog geen binnendringing van geautomatiseerde werken plaats mag vinden. Toch lezen zij vervolgens dat voor de daadwerkelijke uitvoering van het onderzoek in een geautomatiseerd werk het van belang is dat bekend is welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn (zodat een technisch hulpmiddel onopvallend kan worden geplaatst), of er meerdere gebruikers zijn, hoe het beheer verloopt, welk besturingsprogramma van toepassing is en wat de risico's zijn. Kan de regering aangeven op wat voor manier, zonder de hackbevoegdheid te gebruiken, vastgesteld kan worden welke programma's zijn geïnstalleerd en welke bestandsmappen aanwezig zijn op het geautomatiseerd werk? Klopt het dat in de praktijk al in de verkennende fase routers gehackt moeten worden om al deze informatie van geautomatiseerde werken te verzamelen? Wat gebeurt er met de informatie van geautomatiseerde werken van niet-verdachten? Kan de regering aangeven welke software gebruikt wordt om de benodigde informatie te verzamelen in de verkennende fase?
Voorts stelt de regering dat er informatie verzameld wordt uit open bronnen. Kan de regering aangeven welke open bronnen bedoeld worden? Welke bijzondere opsporingsbevoegdheden kunnen ingezet worden om inloggegevens te achterhalen?
Voorts lezen de leden van de D66-fractie dat criminelen gebruik maken van diverse technieken om de feitelijke locatie van de gegevens of de identiteit en de locatie van het geautomatiseerd werk en zijn beheerder te verhullen. De regering stelt dat soms het benutten van zwakheden in de verhullingstechniek in dergelijke gevallen uitkomst kan bieden. Wat bedoelt de regering met verhullingstechnieken? Bedoelt de regering dat het kwestbaarheden in bijvoorbeeld VPN-diensten wil gebruiken? Is de regering op de hoogte van de zogeheten ASML-hack, waar een fout in de software van een VPN-dienst leidde tot economische schade voor het bedrijf? Hoe kijkt de regering aan tegen de economische consequenties van het gebruiken in plaats van dichten van dergelijke kwetsbaarheden?
De aan het woord zijnde leden lezen dat er verschillende technieken zijn om een geautomatiseerd werk binnen te dringen, namelijk via «social-engineering», «phishing» of via het plaatsen van malware waarbij fouten in software gebruikt worden. De leden constateren dat de regering de eerste twee technieken vooral ziet als een manier om malware te kunnen plaatsen op een geautomatiseerd werk. Kan de regering nader toelichten waarom hacken via «social-engineering» of «phishing» niet voldoende is om de problemen geschetst in het hoofdstuk over de noodzaak van dit wetsvoorstel te overkomen? Ook stelt de regering dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden. Kan de regering deze techniek nader toelichten? Voorts stelt de regering dat «in de derde plaats kwetsbaarheden in een computer kunnen worden geëxploiteerd, zoals het gebruik van fouten of lekken in de software. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd.» Kan de regering nader toelichten wat zij met «in beginsel» bedoelt? Bestaat de mogelijk dat de regering bedrijven zal dwingen of vragen om kwetsbaarheden in software

in te bouwen? Kan de regering bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten?
Voornoemde leden constateren dat de Afdeling advisering van de Raad van State grote vraagtekens zet bij de software die politie beoogd te gebruiken voor de hackbevoegdheid. Zij wijzen op de mogelijkheden van oneigenlijk gebruik van die software door derden, waaronder de leveranciers. Hoe denkt de politie te voorkomen dat derden daar gebruik van kunnen maken en in welke mate denkt de politie daar succesvol in te kunnen zijn? De regering verwijst vooral naar het belang van behoud van betrouwbaarheid van bewijs. Dat raakt slechts aan het ene geval dat wordt onderzocht en niet aan de implicaties van technische kwetsbaarheden voor alle andere gebruikers van diezelfde software/apparatuur. Hoe beschouwt de regering in dat licht de proportionaliteit van haar voorstel om gebruik te gaan maken van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten? Klopt het dat de malware die geïnstalleerd wordt op geautomatiseerde werken in contact staat met een server van de leverancier? Klopt het dat de leverancier de mogelijkheid heeft om zelfstandig updates in de malware uit te voeren en zelf de controle over de geautomatiseerde werken over te nemen? Klopt het dat andere klanten van de leverancier ook toegang kunnen krijgen tot de geautomatiseerde werken die geïnfecteerd zijn met malware van de leverancier? Klopt het dat de mogelijkheid bestaat dat de server van de leverancier die in contact staat met alle geïnfecteerde geautomatiseerde werken gehackt kan worden en de hackers de controle over alle geïnfecteerde geautomatiseerde werken kunnen overnemen?
Voorts lezen de leden van de D66-fractie dat de politie waar mogelijk zal proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Is de regering het met de leden eens dat dit vrijwel onmogelijk is? Kan de regering concrete voorbeelden geven waarin dit wel mogelijk is? Deze leden lezen vervolgens dat de politie, in reactie op vragen over het gebruik van kwetsbaarheden en een mogelijke perverse prikkel om kwetsbaarheden voor zichzelf te houden, «streeft naar een veiliger Nederland en geen belang of baat heeft bij de instandhouding van onbeveiligde systemen, gelet op de maatschappelijke kosten die hiermee gepaard gaan. De politie moedigt burgers en bedrijven juist aan hun systemen en gegevens goed te beveiligen door besturingssystemen en programma's actueel te houden, gebruik te maken van beveiligde verbindingen voor belangrijke zaken en zelfs door gegevens te versleutelen zodat zelfs wanneer een cybercrimineel weet binnen te komen, hij weinig of niets van waarde aantreft op het binnengedrongen systeem.» De aan het woord zijnde leden zijn van mening dat dit een zeer tegenstrijdige positie is, gezien de feitelijk afhankelijkheid van fouten in software als gevolg van de hackbevoegdheid. Klopt het dat de politie afhankelijk zal zijn van zowel onbekend als bekende fouten in software? Klopt het dat het zeer onwaarschijnlijk is dat de politie de fouten die de aan te kopen software gebruikt om een geautomatiseerd werk binnen te dringen zal melden bij de fabrikant zodat ze gedicht kunnen worden? Dit betekent toch dat de politie een belang heeft bij de instandhouding van onveilige software? Deelt de regering de mening dat het actueel houden van programma's geen soelaas biedt tegen het gebruiken van onbekende kwetsbaarheden zoals de politie beoogt te doen? Deelt de regering de mening dat de politie niet zowel een belang kan hebben bij onveilige software en tegelijk een belang bij het veiliger maken van software?
De leden van D66-fractie lezen dat het gebruik van kwetsbaarheden in de beveiliging van een computer door de politie in de praktijk lastig is. Het gebruik van «exploits» door de politie is niet alleen buitengewoon kostbaar, maar ook riskant omdat de kwetsbaarheid zeer snel kan zijn opgelost. Kan de regering aangeven waarom het toch de moeite waard is voor de politie om te kunnen hacken als het zo kostbaar en riskant is? Hoe kostbaar is het gebruik van «exploits» precies?

Deze leden vragen de regering nader toe te lichten hoe de keuring van aan te schaffen software eruit zal zien en wat voor eisen de regering aan de keuring zal stellen.
De leden van de D66-fractie vragen de regering nader toe te lichten in hoeverre er sprake is van obstructie van politieonderzoek als een persoon de malware van de politie detecteert en verwijderd.
De aan het woord zijnde leden constateren dat bij beëindiging van een onderzoek het technische hulpmiddel, de malware, zoveel mogelijk wordt verwijderd. Kan de regering nader toelichting wat zij bedoelt met «zoveel mogelijk»? Is de regering van plan om bij het binnendringen van routers de firmware aan te passen? Op wat voor manier wordt de firmware aangepast bij het beëindigen van het onderzoek? Wordt in een dergelijk geval de laatste versie van de firmware geïnstalleerd, ook als dit betekent dat de politie daarna niet meer de router kan binnendringen? Hoe is de aansprakelijkheid geregeld in het geval dat bij het plaatsen of verwijderen van een technisch hulpmiddel het geautomatiseerd werk schade berokkend wordt? Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd? Indien software en sporen niet verwijderd kunnen worden maar de verdachte achteraf wel is vrijgesproken, bestaat dan een recht op vergoeding voor eventuele schade die is toegebracht aan apparatuur door het heimelijke binnendringen en het plaatsen van software?
De leden van de D66-fractie lezen over een impact analyse naar een schadevergoedingsregeling die in het wetboek zou moeten komen. Die schadevergoeding wordt gekoppeld aan de modernisering van het Wetboek van Strafvordering. Deze leden vinden het een zeer opmerkelijke keuze dat de regering wel onderhavige bevoegdheid apart en vooruitlopend op de modernisering tracht te regelen, maar voor de schadevergoeding verwijst naar de modernisering. Zij vragen wanneer de regering verwacht dat de impact analyse naar de schadevergoeding gereed is. Is de regering bereid de Kamer de impactanalyse toe te sturen voorafgaande aan de verdere behandeling van onderhavig wetsvoorstel, zodat de Kamer een afweging kan maken over alle aspecten die horen bij dit wetsvoorstel?
Voorts lezen de aan het woord zijnde leden dat «wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, (...) vanuit de server van de politie het dataverkeer (wordt) stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk». Wie ziet er actief op toe dat, indien software niet verwijderd kan worden wegens risico's voor het systeem, het dataverkeer vanuit de server van de politie ook daadwerkelijk wordt stopgezet? Klopt het dat de geïnfecteerde geautomatiseerde werken tevens in verbinding staan met een server van de leverancier van de hacksoftware? Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?
Voornoemde leden lezen dat van de handelingen van het technische team proces-verbaal wordt opgemaakt en dat dit ten spoedigste dient plaats te vinden. Waarom is daarbij niet gekozen voor een harde termijn? Deze leden wijzen verder op de slordigheden die plaatsvinden bij het opstellen van processen-verbaal. Hoe is de voorgestelde zeer ingrijpende bevoegdheid voldoende controleerbaar voor de verdediging en in de rechtszaal als de inhoud van processen-verbaal in de praktijk regelmatig en tot ergernis van de rechtspraak en advocatuur niet op orde blijkt? Welke garantie biedt de regering dat dit met extra zorgvuldigheid zal gebeuren?

De leden van de ChristenUnie-fractie vragen waarom er voor is gekozen de binnendringing van een computer eerder gelijk te schakelen met het aftappen van telefoongegevens dan met een huiszoeking. Is overwogen om, net als bij een huiszoeking, de binnendringing onder lopend toezicht van een (gespecialiseerde) rechter-commissaris en een hem assisterende griffier te stellen?
Deze leden constateren dat met de binnendringingsbevoegdheid een spanning ontstaat tussen het gerichte belang van effectief opsporingsonderzoek en het publieke belang van het dichten van beveiligingslekken. Hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd?

De leden van de GroenLinks-fractie hebben de nodige bedenkingen rond de praktische toepassing van de dwangmiddelenbevoegdheid. Het binnendringen in een geautomatiseerd werk vindt, zo veronderstellen deze leden, in principe op dezelfde wijze plaats als een computerhack. De eenmaal geforceerde opening is niet meer te dichten. Het biedt de kans om ook na sluiting van het strafrechtelijk onderzoek het geautomatiseerde werk binnen te dringen. Hoe wordt verzekerd dat misbruik van dit soort datalekken (bijvoorbeeld het zonder nieuwe machtiging betreden van het werk) uitgesloten is?

2.6 De toetsing van de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie lezen dat ten behoeve van de controleerbaarheid van de onderzoekshandelingen aan een aantal eisen moet worden voldaan. Met behulp van de op deze wijze verzamelde gegevens kan de uitvoering van de bevoegdheid in voorkomende gevallen worden gecontroleerd, zo lezen zij. Kan nader toegelicht worden wat hier moet worden verstaan onder «op deze wijze» en «in voorkomende gevallen»? Deze leden vragen in hoeverre de officieren van justitie, de parketsecretarissen en de zittende magistratuur verplicht zijn zich bij te scholen en cursussen te volgen op het gebied van computercriminaliteit.

De leden van de PvdA-fractie begrijpen dat de inzet van de bevoegdheid om op afstand onderzoek te doen in een geautomatiseerd werk een machtiging van de rechter-commissaris vereist. Indien uit het opsporingsonderzoek bewijsmateriaal wordt verkregen dat tijdens een strafproces wordt gebruikt, is het aan de (zittings-)rechter om een oordeel over dat bewijsmateriaal te vellen en of het rechtmatig verkregen is. Echter, indien er van de bevoegdheid gebruik wordt gemaakt en dat geen voor een strafproces relevante informatie oplevert, vindt er achteraf geen toets op de rechtmatigheid meer plaats. Deze leden lezen ook dat er een notificatieplicht is voorzien op grond waarvan de betrokkene op de hoogte wordt gesteld dat er een opsporingsambtenaar op afstand in zijn pc, smartphone enz. heeft gekeken. Deelt de regering de mening dat het nakomen van die notificatieplicht van belang is om de controle op de inzet van deze bevoegdheid mede te waarborgen? Zo ja, waarom en hoe gaat zij ervoor zorgen dat die notificatieplicht ook daadwerkelijk nageleefd gaat worden? Staan er sancties op het niet nakomen van de notificatieplicht? Zo ja, welke en worden die in het geval van de bestaande opsporingsbevoegdheden ook al opgelegd? Zo nee, waarom niet?
De aan het woord zijnde leden lezen dat de Centrale Toetsingscommissie van het OM de voorgenomen inzet van de bevoegdheid tot onderzoek vooraf toetst. In het geval van de AIVD/MIVD toetst de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten achteraf het gebruik van de bevoegdheden van die diensten. Deelt de regering de mening van deze leden dat het goed zou zijn indien, ook in het geval van het gebruikmaken van de bevoegdheid om op afstand onderzoek te mogen gaan

doen in een geautomatiseerd werk, er een onafhankelijke toezichthouder zou komen die het gebruik van die bevoegdheid in zijn algemeenheid gaat toetsen op proportionaliteit, doelmatigheid en rechtmatigheid? Zo ja, hoe gaat de regering dit bewerkstelligen? Zo nee, waarom niet?

De leden van de SP-fractie vragen of het klopt dat alle onderzoekshandelingen met betrekking tot het heimelijk binnendringen in een geautomatiseerd werk worden vastgelegd. Ten behoeve waarvan wordt dit vastgelegd? Is dit onder andere ook om toezicht te houden op het correct uitvoeren van het bevel? Wie houdt er eigenlijk toezicht op de correcte uitvoering van een bevel? Klopt het dat dat niet wordt gedaan door de rechter-commissaris? Zo nee, waarom niet? Er wordt vooraf getoetst door een rechter-commissaris of een bevel kan worden afgegeven, maar vervolgens kan deze niet meer controleren of deze wordt uitgevoerd zoals is beoogd. Het waarborgen van grondrechten stopt niet bij het afgeven van een bevel, maar loopt gedurende het gehele opsporingstraject. De regering stelt dat de rechter-commissaris mag vertrouwen op correcte uitvoering van het bevel. Deze leden willen naar aanleiding hiervan graag benadrukken dat een rechtsstaat niet alleen gebaseerd is op vertrouwen, maar ook op onafhankelijke controle. Vooral waar het gaat om zaken die nooit voor de zittingsrechter komen. Graag ontvangen deze leden een uiteenzetting van de wijze waarop onafhankelijke controle plaatsvindt (en eventuele handhaving) van correcte uitvoering van een afgegeven bevel en rechtelijke machtiging, zodat toetsing niet alleen vooraf en achter plaatsvindt maar ook tijdens de inzet. Voornamelijk in zaken die om wat voor reden dan ook niet tot een rechtszaak komen.
De leden van de SP-fractie willen weten of bij het voorleggen van een bevel aan de rechter-commissaris ook meegenomen wordt hoe doelgericht wordt gezocht en tot hoeveel gegevens toegang zal worden verkregen. Zal een machtiging of bevel minder snel worden afgegeven naarmate het aantal gegevens dat (ongericht) wordt verzameld toeneemt? Hoe zwaar weegt dit bij de belangenafweging?
Gaan de aangepaste opleidingen niet alleen in op de nieuwe bevoegdheden maar ook op de begrippen proportionaliteit en subsidiariteit, zo vragen de leden van de SP-fractie.
De aan het woord zijnde leden begrijpen uit de memorie van toelichting dat rechters niet veel verstand zouden hebben van de technische kant van het onderzoeken van een geautomatiseerd werk. Er zal moeten worden afgegaan op de expertise van de opsporingsambtenaar. Hoezeer de leden ook uitgaan van deze expertise, toch vragen ze zich ernstig af hoe onafhankelijk deze expertise is. Techniek is aan verandering onderhevig en een rechter zal niet altijd goed kunnen beoordelen of een bestaande of nieuwe techniek wenselijk is. Bijvoorbeeld of deze niet een te groot risico vormt waar het gaat om privacyschending of hacken door derden. Hoe vindt de regering ervan een onafhankelijke toetsingscommissie in het leven te roepen, waarin onder andere ethische hackers, wetenschappers, ICT-bedrijven en opsporingsambtenaren plaatsnemen die regelmatig of zo vaak als nodig de legitimiteit dan wel de wenselijkheid toetsen van bepaalde technieken om te kunnen hacken? Als het gaat om toezicht vooraf, tijdens en na inzet van de opsporingsbevoegdheid kan ook worden gedacht aan de Autoriteit Persoonsgegevens. Dit is door deze instantie zelf gesuggereerd, mits voldoende capaciteit aanwezig is. Graag ontvangen deze leden een reactie op beide voorstellen.
Waar het gaat om het inzetten van ethische hackers om de veiligheid van een systeem te toetsen, krijgen de leden van de SP-fractie signalen dat de samenwerking met deze ethische hackers nog niet goed genoeg loopt. Wat is hierop de reactie van de regering? Hoe verloopt de samenwerking met en de inzet van ethische hackers?
De leden van de SP-fractie vragen of zij het goed begrijpen als zij stellen dat er een notificatieplicht komt aan betrokkene als het belang van het

onderzoek dat toelaat. Wanneer is daar sprake van? Wordt dan ook de reden aangegeven van het onderzoek in het geautomatiseerde werk, zodat betrokkene weet waar hij of zij eventueel verweer tegen moet voeren? Hoe wordt omgegaan met de notificatieplicht als het gaat om gegevens op een buitenlands of onbekend geautomatiseerd werk?
De aan het woord zijnde leden vragen of in de gevallen dat een betrokken niet op de hoogte wordt gebracht, het juist belangrijk is de inzet van de hackbevoegdheid te toetsen door een onafhankelijke instantie. Zo nee, hoe wordt dan rekening gehouden met artikel 13 EVRM, waarin staat dat mensen eventuele schending van hun grondrechten aan moeten kunnen kaarten?

De leden van de CDA-fractie vragen naar de snelheid waarmee de toetsing middels de Centrale Toetsingscommissie en het College van procureurs-generaal plaatsvindt, gelet op de spoedeisendheid die kan zijn geboden bij het inzetten van bepaalde bevoegdheden (bijvoorbeeld bij ontvoering of vermoedens van moord of-terroristische aanslag). Zijn in dit geval ook uitzonderingen mogelijk en wenselijk, bijvoorbeeld toetsing achteraf? Deze leden vragen naar de logica van een notificatieplicht. Immers, de kern van heimelijk binnendringen zal in beginsel toch zijn dat de betrokkene juist niet op de hoogte wordt gesteld? Is hierin een andere wettelijke constructie niet wenselijk, namelijk dat pas achteraf mededeling wordt gedaan van de inbreuk (na afloop van verstrijken maximale termijn van de bevoegdheid) en eventueel een wettelijke uitzondering hierop dat vooraf mededeling wordt gedaan? De vraag rijst dan voor deze leden nog wel in welke gevallen de regering het wel denkbaar acht dat vooraf betrokkene op de hoogte wordt gesteld. De leden van de CDA-fractie verzoeken deze vragen eveneens te beantwoorden in geval vermoedens zijn dat meerdere personen gebruik maken van het betreffende apparaat.

De leden van de D66-fractie merken op dat wordt voorzien in een Centrale Toetsingscommissie, een intern adviesorgaan van het OM. Alhoewel deze leden het wenselijk vinden dat in een toetsingscommissie wordt voorzien, vragen zij waarom niet is voorzien in systeemtoezicht meer op afstand, zoals door de Autoriteit Persoonsgegevens wordt bepleit?
Het valt voornoemde leden op dat straks uitvoerige technische kennis bij de politie aanwezig dient te zijn voor uitvoering van de voorgestelde bevoegdheid. Daarnaast dient bij ieder regioparket een cybercrime officier van justitie aanwezig te zijn en wordt voorzien in bijscholing. Bij de rechtspraak wordt gesproken over een cursus voor rechters. Het valt deze leden op dat hoe hoger in de controleketen hoe minder de inzet op specialistische kennis lijkt te zijn, terwijl de inzet op kennis vanwege de controlerende taak dan juist maximaal dient te zijn. Wat vindt de regering van het voorstel om ten minste te voorzien in specialistische rechter-commissarissen gelijk aan de cybercrime officieren van justitie bij ieder regioparket? Wat vindt de regering van het voorstel van de aan het woord zijnde leden om, net als de gespecialiseerde Ondernemingskamer, een speciale cyberkamer bij de rechtspraak in te richten die zich met dit soort zaken zal bezighouden en waarin kennis en ervaring met cyberzaken is gebundeld?

De leden van de ChristenUnie-fractie vragen naar de positie van (private en publieke) onderzoekers die nu op het (vrij en eenvoudig toegankelijke) «darkweb» meekijken en daar allerhande strafrechtelijke feiten tegen-komen. Welke verplichtingen hebben deze onderzoekers als ze strafrechte-lijke feiten tegen komen? Heeft de regering overwogen om in dit wetsvoorstel ook voor hen nadere voorzieningen te treffen? Heeft de regering een beeld van wat de juridische risico's zijn van dergelijk onderzoek? Of is overwogen daar nader onderzoek naar te doen?

Deze leden vragen wat de regering vindt van het door verschillende organisaties en experts gedane voorstel om, als extra waarborg, via een onafhankelijke commissie van toezicht binnendringing binnen opsporingsonderzoeken te laten monitoren?

De leden van de GroenLinks-fractie onderschrijven het advies van de Afdeling advisering van de Raad van State om te voorzien in structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd. Dat versterkt immers het rechtstatelijke gehalte van de toepassing van deze dwangmiddelenbevoegdheid.

De leden van de PvdD-fractie zijn van oordeel dat het toezicht op de hackbevoegdheid van de politie in het huidige wetsvoorstel ernstig ontoereikend is. Zo ontbreken technische waarborgen. Bij een wetsvoorstel dat gaat over de inzet van een technisch middel, zijn juridische waarborgen niet genoeg. Op dit moment is het niet mogelijk de technische aanpassingen die worden gedaan op de computer van een verdachte achteraf te traceren. Zolang er geen toezicht mogelijk is op het technisch handelen van de politie, is er überhaupt geen volledig toezicht mogelijk. Is de regering bereid het Besluit technische hulpmiddelen te herzien voordat de Kamer zich over het wetsvoorstel uitspreekt? Deze leden zijn van mening dat er een onafhankelijke commissie voor toezicht op de opsporingsdiensten moet komen. Is de regering bereid hierover met een voorstel te komen alvorens de Kamer over het wetsvoorstel zal stemmen?

2.7 De wettelijke regelingen in buurlanden (België, Duitsland en Frankrijk)

De leden van de SP-fractie zijn benieuwd op grond waarvan het Duitse Bundesverfassungsgericht heeft geoordeeld dat een heimelijke infiltratie van een computersysteem alleen is toegestaan als er aanwijzingen zijn voor een concreet gevaar van een belangrijk rechtsgoed, zoals gevaar voor leven of de vrijheid van een persoon of het staatsbelang. In hoeverre voldoet onderhavig wetsvoorstel aan deze eisen? Klopt het dat onderhavig wetsvoorstel sneller leidt tot inzet van de hackbevoegdheid? In hoeverre houdt dit wetsvoorstel dan ook stand voor de Nederlandse rechter en het Europees Hof voor de Rechten van de Mens? Waarom is niet aangesloten bij het oordeel van het Duitse Bundesverfassungsgericht? Kan de regering reageren op de uitspraak van de Autoriteit Persoonsgegevens tijdens het rondetafelgesprek over computercriminaliteit d.d. 11 februari 2016 dat zij ernstig twijfelt of onderhavige wet stand zal houden?

De leden van de CDA-fractie vragen of de regering met politie en justitie de wenselijkheid voor de opsporingspraktijk heeft besproken een bevel als in Duitsland te kunnen opleggen voor maximaal drie maanden met verlengingsmogelijkheden van telkens drie maanden. Biedt dit niet veel meer ruimte voor de opsporing om gedurende een langere periode ongestoord onderzoek te kunnen dan de nu voorgestelde termijn van vier weken? De Duitse regeling voldoet hiermee toch ook aan de gewenste (Europese) proportionaliteitstoets? Graag zouden deze leden een aanpassing op dit punt zien in onderhavig wetsvoorstel.

De leden van de D66-fractie vragen of het klopt dat Nederland met dit wetsvoorstel de meest vergaande hackwetgeving zou krijgen binnen de EU. Zij vragen de regering een overzicht te sturen met bevoegdheden rondom het hacken van geautomatiseerde werken van alle EU-lidstaten. Hoe verhoudt het wetsvoorstel zich tot de keuze van Frankrijk en Duitsland

om juist af te zien van het gebruik van spyware omdat oneigenlijk gebruik door derden en de politie niet viel uit te sluiten? De regering verwijst naar voorafgaande keuring van het technische hulpmiddel. Wil de regering daarmee zeggen dat de keuze van Frankrijk en Duitsland niet zozeer principieel als wel door een gebrek van keuring was ingegeven? Hoe wordt met keuring van het technische hulpmiddel misbruik precies voorkomen? Zij vragen de regering nader in te gaan op de gevolgen voor het digitale vestigingsklimaat van Nederland als gevolg van deze situatie. Voorts vragen deze leden een nadere toelichting van de inschatting van de regering van het risico dat landen als China of Rusland dit wetsvoorstel zullen aangrijpen om hacken in het buitenland te rechtvaardigen.
De leden van de D66-fractie vragen of de regering kennis heeft genomen van de stellingname van Apple, die juist vanwege de risico's van technische kwetsbaarheden voor alle andere gebruikers, weigert de beveiliging van de iPhone te kraken en een «gevaarlijke achterdeur» in te bouwen waardoor de FBI zich toegang kan verschaffen tot de iPhone van een vermeende terrorist. Hoe beschouwt de regering de keuze van Apple om niet ten behoeve van één persoon de beveiliging van alle iPhones wereldwijd op het spel te zetten door technische ontsleuteling te creëren van de beveiliging waar alle gebruikers van de iPhone wereldwijd op vertrouwen?

2.8 Onderzoek in een geautomatiseerd werk en rechtsmacht

2.8.1 Inleiding
De leden van de PvdA-fractie vragen of zij het goed begrijpen als zij stellen dat indien bekend is dat een geautomatiseerd systeem in het buitenland staat dat dan voor de bevoegdheid tot het op afstand onderzoeken gebruik zal worden gemaakt van een rechtshulpverzoek. Gebeurt dit standaard of zijn hierop uitzonderingen mogelijk? Wanneer gaat de noodzaak om snel in te grijpen voor op het achterhalen van de locatie van een server en het uitvaardigen van een rechtshulpverzoek? Wat gebeurt er in het geval bekend is dat het geautomatiseerd werk in een land staat waar Nederland geen relatie heeft voor het uitwisselen van rechtshulpverzoeken of wanneer de aangezochte staat geen rechtshulp verleent? Kan dan toch op afstand onderzoek worden gedaan?
De leden van de ChristenUnie-fractie vragen een nadere toelichting op de vraag of het mogelijk is computers of computergegevens die zich buitenslands bevinden binnen te dringen. Kan de regering nader onderbouwen waarom dit niet op internationaalrechtelijke bezwaren zal stuiten?

2.8.2 Uitvoerende rechtsmacht en de bestrijding van computercriminaliteit
De leden van de VVD-fractie merken op dat in sommige gevallen de feitelijke locatie van gegevens redelijkerwijs niet is te achterhalen. Dit kan betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk waarvan niet bekend is waar dit zich bevindt en waarbij geen rechtshulpverzoek kan worden gedaan. Een dergelijk zelfstandig optreden dient zeer zorgvuldig te worden ingekaderd op basis van een zoveel mogelijk stapsgewijze aanpak. Deze stappen en criteria zullen worden uitgewerkt in een aanwijzing door het OM. Wat zijn deze stappen en criteria?
De leden van de PvdA-fractie lezen dat toch in een geautomatiseerd werk kan worden binnengedrongen als de locatie van gegevens niet te achterhalen is. Volgens het College van procureurs-generaal geldt dan de ubiqiteitsleer op grond waarvan Nederland rechtsmacht heeft. Deelt de regering die mening? Kan de regering uitleggen hoe deze leer in dit verband werkt? Waar binnen het Nederlands recht wordt die leer nog

meer gebruikt om rechtsmacht te vestigen? Bestaat er relevante jurisprudentie? Zo ja, wat houdt die in?
Deze leden vragen of de regering het mogelijk acht dat het binnendringen in een buitenlandse geautomatiseerd werk zonder de toestemming van de autoriteiten in dat buitenland weliswaar geen schending van de soevereiniteit van dat land betekent, maar dat dat land in kwestie daar weleens heel anders over zou kunnen denken? Acht de regering het mogelijk dat dat land dat dan als rechtvaardiging ziet om ook in Nederlandse systemen binnen te dringen? Gebeurt dat al door opsporingsdiensten van landen waar reeds de mogelijkheid bestaat om op afstand heimelijk in geautomatiseerde werken binnen te dringen? Acht de regering het mogelijk dat op het moment dat Nederlandse opsporingsdiensten buitenlandse servers gaan binnendringen, daarmee het risico bestaat dat buitenlandse opsporingsdiensten dat andersom gaan doen? Zo ja, wat betekent dat voor de veiligheid van onze systemen? Zo nee, waarom niet?
De leden van de PvdA-fractie vragen of de bevoegdheid op afstand heimelijk onderzoek te doen in een geautomatiseerd werk of het ontoegankelijk maken van gegevens negatieve gevolgen voor het Nederlandse vestigingsklimaat kan hebben, niet zozeer omdat de Nederlandse overheid deze bevoegdheid heeft, maar veeleer omdat in het kader van de wederkerigheid buitenlandse entiteiten mogelijk makkelijker op een Nederlandse server binnendringen en daarmee Nederland niet veilig is voor hun gegevens. Hoe verhoudt deze bevoegdheid zich tot het bovengenoemde WRR-rapport waarin staat dat Nederland de integriteit van het world wide web zou moeten beschermen tegen statelijke actoren?

De leden van de CDA-fractie zeggen met enige zorgen kennis te hebben genomen van de opmerking dat internationale uitwisseling in strafzaken ten aanzien van computercriminaliteit nog niet erg ver gevorderd is. Ziet de regering voor zichzelf hier een rol weggelegd in de eerste helft van dit jaar als EU-voorzitter om op dit terrein vooruitgang te boeken? Zo ja, op welke wijze kan zij komen tot voorstellen om het zogeheten Cybercrime Verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290) te verruimen? Deze leden vragen dit, mede gelet op de aankondiging van de Minister van Buitenlandse Zaken op 12 februari 2016 dat Nederland komende maanden landen, bedrijven, denktanks en internetnetdeskundigen bij elkaar wil brengen om de cybersecurity te verbeteren. Dit lijkt deze leden niet alleen gewenst met betrekking tot de in het wetsvoorstel genoemde vormen van criminaliteit, maar ook ten aanzien van de huidige migratiecrisis en de daaraan verbonden samenwerking op terrein van mensensmokkel. Hoe beziet de regering de waarde van onderhavig wetsvoorstel in dat perspectief? Welke bijdrage levert zij hiertoe en wat is volgens de regering nog meer nodig om op Europees en internationaal niveau stappen te zetten tot een betere aanpak van mensenhandel en digitale voorbereidingen hiertoe?
De leden van de CDA-fractie vragen de regering ook met welke derde landen zij een 24/7 contactpunt heeft om rechtshulp snel af te kunnen handelen en of gewerkt wordt aan uitbreiding van deze lijst teneinde met zoveel mogelijk landen een dergelijk contact op te bouwen.

De leden van de D66-fractie lezen dat het bepaald niet is uitgesloten dat meerdere staten rechtsmacht hebben bij de opsporing en vervolging van vormen van computercriminaliteit. Welke medewerking en bereidheid tot onderling overleg kan Nederland verwachten in die gevallen zowel binnen als vooral buiten Europa? De regering verwijst hier naar het Cybercrimeverdrag. Wat zijn de ervaringen tot op heden met overleg in geval van overlappende rechtsmacht?
Deze leden merken op dat diverse landen een 24/7 contactpunt hebben ingericht voor de snelle afhandeling van rechtshulpverzoeken in cybercri-

mezaken. Ook Nederland heeft zo'n contactpunt bij het Team High Tech Crime. Hoeveel verzoeken komen daar jaarlijks binnen en in hoeveel gevallen is een rechtshulpverzoek van Nederland en aan Nederland afgewezen?

2.9 De bescherming van grondrechten

De leden van de SP-fractie begrijpen dat bij de afweging om een bevel tot heimelijk onderzoek in een geautomatiseerd werk sprake moet zijn van een dringend opsporingsbelang. Wanneer is een opsporingsbelang dringend en wanneer niet? Er moet voorts onderzoek worden gedaan in een zo beperkt mogelijk deel van een geautomatiseerd werk. Hoe weet men van tevoren waar men moet zijn? Men weet toch niet altijd waar gegevens opgeslagen staan? Wat wordt gedaan met gegevens die niet relevant zijn voor de opsporing?

De leden van de PvdD-fractie zijn van oordeel dat het voorliggende wetsvoorstel de privacy en rechten van Nederlanders in een zodanig grote mate aantast, zonder daar een sluitende legitimering voor te geven, dat het een grondrechtelijke toetsing waarschijnlijk niet zal doorstaan. Dit is de conclusie van hoogleraar Informatierecht Nico van Eijk. De afgelopen jaren zijn op Europees niveau verschillende rechterlijke uitspraken gedaan die gericht zijn op het vergroten van de privacy van Europese burgers. Denk hierbij aan de uitspraak in de Schrems-zaak en het opzeggen van het Safe Harbour-verdrag. In tegenstelling tot de Europese trend, lijkt Nederland juist het recht op privacy ernstig aan te tasten. Het onderhavige wetsvoorstel mist een goede toelichting op nut en noodzaak, proportionaliteit en subsidiariteit. De leden van de PvdD-fractie willen weten in hoeverre de regering recente Europese jurisprudentie heeft meegenomen in dit wetsvoorstel. Hoe beoordeelt de regering de bewering dat dit wetsvoorstel de privacy van Nederlanders aantast, zeker gezien de recente Europese ontwikkelingen om het recht op privacy juist te beschermen? Deze leden merken op dat daar nog bijkomt dat ook het College bescherming persoonsgegevens (Cbp) heeft geadviseerd het wetsvoorstel niet in te dienen. Het bereik van het wetsvoorstel strekt zich volgens het advies uit tot een zeer grote hoeveelheid gegevens, met volledige toegang tot historische gegevens die op randapparatuur zijn opgeslagen. Ook de gegevens die worden opgeslagen en uitgewisseld via alle communicatiekanalen waarmee de apparatuur verbonden is, zijn toegankelijk. Om deze reden stelt het Cbp dat het van groot belang is dat het wetsvoorstel blijk geeft van een zorgvuldige afweging binnen de grondwettelijke kaders, zowel op Nederlands als Europees niveau. Op grond van het EVRM zijn inbreuken op fundamentele rechten alleen rechtmatig als deze voldoen aan strikte voorwaarden, zoals noodzakelijkheid, proportionaliteit en subsidiariteit. Volgens het Cbp wordt het ingrijpende karakter van de verstrekkende bevoegdheid en de uitgebreide kring van personen die getroffen kunnen worden onvoldoende onderkend. Het wetsvoorstel zou een grondwettelijke toetsing daarom ook niet doorstaan. Is de regering bereid het wetsvoorstel in te trekken? Zo nee, waarom niet?
Tot slot merken de leden van de PvdD-fractie op dat privacy en bescherming van de persoonlijke levenssfeer een groot goed is en moet te allen tijde gewaarborgd worden. Hoewel cybercriminaliteit een bekend en groeiend probleem is, is dit geen vrijbrief om de grondrechten van miljoenen Nederlanders aan te tasten. Veiligheid moet voorop staan en een wet die het mogelijk maakt een pacemaker te hacken, mist elke vorm van proportionaliteit.

2.9.1 Het recht op eerbiediging van de persoonlijke levenssfeer[303]
De leden van de SP-fractie constateren dat er een aantal uitspraken is van Europese rechters waarbij ingegaan wordt op de proportionaliteit van het verzamelen van gegevens. Het gaat dan over de discussie met betrekking tot dataretentie, de zaak Scherms, de zaak Zakharov en de zaak Szabo. Bij de laatste twee zaken ging het om de grenzen met betrekking tot de inzet van elektronische surveillance. Op welke manier voldoet onderhavig wetsvoorstel aan de randvoorwaarden zoals die in deze rechtszaken door de verschillende rechters zijn gesteld aan proportionaliteit van de verzameling van gegevens en inzet van opsporingsbevoegdheden?

De leden van de D66-fractie merken op dat de regering aangeeft dat de burger erop mag vertrouwen dat de integriteit van zijn computersysteem gewaarborgd is en dat derden niet zonder toestemming kennis kunnen nemen van vertrouwelijke documenten of communicatie. Indien de regering niet kan uitsluiten dat door het gebruik van technische kwetsbaarheden de achterdeur ook open komt te staan voor kwaadwillende derden die dezelfde achterdeur willen gebruiken, hoe meent zij dan dat de burger kan vertrouwen op de integriteit van een computersysteem?

2.9.2 Het recht op bescherming van het brief-, telefoon- en telegraafgeheim
De leden van de VVD-fractie vragen hoe de bevoegdheden ten aanzien van het aftappen of opnemen van (vertrouwelijke) communicatie zich verhouden tot de bevoegdheden op dit gebied zoals opgenomen in de Wet op de inlichtingen- en veiligheidsdiensten. Komen de bijbehorende gronden en waarborgen overeen?

3. De ontoegankelijkmaking van gegevens

3.1 De noodzaak tot aanpassing van de huidige wettelijke regeling

De leden van de CDA-fractie vragen (nogmaals) of met het schrappen van een dwangsom uit het conceptwetsvoorstel ten aanzien van internetproviders nog wel afdoende maatregelen overblijven om handhavend effectief op te kunnen treden.
Deze leden vragen of het thans in de praktijk voorkomt dat dat de aanbieder van een communicatiedienst niet bereid is op basis van de geldende NTD-gedragscode gegevens ontoegankelijk te maken. Hoe kan daartegen worden opgetreden tot het moment dat onderhavig wetsvoorstel in werking treedt?
De leden van de CDA-fractie begrijpen de keuze van de regering om het advies van het College van procureurs-generaal over te nemen om het gegeven van een bevel tot ontoegankelijk maken van gegevens te beperken tot misdrijven ex artikel 67 Sv. Uiteraard moet het OM niet al haar tijd en energie steken in een rol als censurerende internetpolitie. Tegelijkertijd vragen deze leden of er dientengevolge geen overtreding/misdrijven gemist worden, waarbij het wel degelijk de moeite waard is om hieruit voortvloeiende gegevens te verwijderen. Zij vragen de regering in het kader van bestrijding van radicalisering en het uiten van verheerlijking van geweld en terrorisme, hoe onderhavig wetsvoorstel rekening houdt met strafbare uitingsdelicten als opruiing, haat zaaien en belediging. Kan hier wel tegen worden opgetreden door een bevel af te geven tot ontoegankelijk maken van gegevens?

3.2 De uitvoering van een bevel tot ontoegankelijkmaking van gegevens

De leden van de SP-fractie vragen of het correct lezen als zij constateren dat degene van wie de gegevens ontoegankelijk worden gemaakt kan klagen bij de rechtbank. Wat als de eigenaar van de gegevens niet bekend is of onvindbaar?

4. Het wederrechtelijk overnemen en «helen» van gegevens

4.1 De voorgestelde strafbaarstellingen

De leden van de SP-fractie constateren dat het strafbaar wordt om niet-openbare gegevens wederrechtelijk over te nemen. Het maakt hierbij dus niet uit om wat voor gegevens het gaat en wat de schade is van het delen. Is dat wel proportioneel? Strafbaar is het niet als het gaat om het algemeen belang. Wanneer is sprake van een algemeen belang? Is dat alleen wanneer er ophef over ontstaat in de media? Hoe wordt voorts getoetst of iemand te goeder trouw handelde of niet? Voorkomen moet worden dat klokkenluiders en journalisten bepaalde informatie niet zullen durven delen, omdat het nog maar de vraag is of zij voldoen aan de eis dat sprake moet zijn van een algemeen belang en bovendien te goeder trouw zijn. Graag ontvangen deze leden een reactie op deze zorgen.

De leden van de D66-fractie constateren dat het strafbaar wordt niet-openbare gegevens die door misdrijf zijn verkregen over te nemen, voorhanden te hebben of bekend te maken. Daarmee wordt het helen van die gegevens strafbaar. Dat roept vragen op over de mogelijkheden van klokkenluiders en journalisten om misstanden aan de kaak te kunnen stellen. In de toelichting bij het wetsvoorstel wordt gesteld dat van strafbaarheid van journalisten en klokkenluiders geen sprake behoort te zijn wanneer bekendmaking van de gegevens in het algemeen belang noodzakelijk is. Deze leden hebben instemmend kennisgenomen van het uitgangspunt dat dit wetsvoorstel niet mag voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders of van degenen die hen daarbij faciliteren. Zij onderschrijven ook dat een zelfstandige waarborg daartoe in de wet wordt opgenomen. Kan de regering een nadere toelichting geven op hetgeen op grond van jurisprudentie en naar haar opvatting als medewetgever wordt verstaan onder algemeen belang?
De aan het woord zijnde leden vragen de regering nader toe te lichten wat er gebeurt als gegevens van het internet worden geplukt die niet alleen niet-openbaar zijn maar ook onvoldoende beveiligd, waardoor als niet-openbare informatie betitelde informatie feitelijk wel toegankelijk is en door derden wordt gebruikt.
De leden van de D66-fractie vragen of de regering een onderscheid maakt in het soort gegevens dat uit een automatisch werk van een ander zijn ontvreemd, bekend gemaakt aan een ander, verkocht of op internet geplaatst? Geldt de niet-openbaarheid als uitsluitend criterium?

De leden van de ChristenUnie-fractie constateren dat het wetsvoorstel heling van computergegevens strafbaar maakt. Waarom heeft de regering niet gekozen voor een nadere differentiatie op grond van de aard van de betreffende gegevens?

5. De verruiming van de strafbaarheid van grooming en van verleiding van minderjarigen tot ontucht

De leden van de VVD-fractie merken op dat bij de inzet van lokpubers gebruik kan worden gemaakt van profielfoto's. Deze leden lezen dat deze profielfoto een willekeurige foto of afbeelding kan zijn. Kan dit nader

toegelicht worden? Aan welke voorwaarden dient het gebruik van zo'n foto te voldoen, bijvoorbeeld ten aanzien van de herkomst van de foto?
De aan het woord zijnde leden lezen dat burgerinitiatieven om pedofielen op te sporen niet geheel vallen uit te sluiten. Zij vragen wat hier tegenover staat. Burgers zijn immers toch niet bevoegd om over te gaan tot opsporing dan wel uitlokking?

De leden van de PvdA-fractie lezen dat bij de inzet van een lokpuber, mede in het licht van het Tallon-criterium, moet worden voorkomen dat er sprake zal zijn van uitlokking in de zin dat iemand tot iets wordt aangezet wat hij zonder de lokpuber niet van plan zou zijn geweest. In de praktijk betekent dat dat een opsporingsambtenaar in beginsel de communicatie niet start, maar afwacht totdat iemand contact met hem legt seksuele doeleinden. Wat wordt bedoeld met de woorden «in beginsel»? Zijn er omstandigheden waarin de opsporingsambtenaar wel zelf dat contact legt? Zo ja, wanneer is daar sprake van? Hoe verhoudt zich dat dan tot het Tallon-criterium?
Deze leden vragen wat de uitkomst is van het WODC-onderzoek naar de normstelling en samenhang van de zedentitel in het Wetboek van Strafrecht. Wanneer kan de Kamer dit onderzoek voorzien van een beleidsreactie tegemoet zien?

De leden van de SP-fractie vragen of zij het goed begrijpen als zij stellen dat grooming straks ook strafbaar is als sprake is van uitlokking door een opsporingsambtenaar die geen minderjarige is (kennelijk jonger dan achttien jaar). In de praktijk zal volgens de regering geen sprake zijn uitlokking, omdat de opsporingsambtenaar niet zelf de communicatie in beginsel zal starten. Wat betekent «in beginsel» in deze context? Hoe wordt voorkomen dat grooming niet bewezen kan worden omdat sprake was uitlokking? De regering geeft aan dat er in de jurisprudentie al veel vastligt over de inzet van een lokpuber en daarom codificatie niet hoeft. Is het niet verstandig om alsnog in de wet vast te leggen wanneer een lokpuber mag worden ingezet om misverstanden te voorkomen, vooral in het kader van rechtszekerheid en potentiële daders weten dat dit mogelijk is.
Deze leden vragen wat als de verdachte zelf minderjarig is, bijvoorbeeld zestien, en het slachtoffer bijvoorbeeld tien jaar? In hoeverre kan er dan ook sprake zijn van een strafbaar feit?

De leden van de CDA-fractie zijn kortgezegd zeer content met het invoegen van dit onderdeel in onderhavig wetsvoorstel. Zij steunen van harte het voornemen om hiermee het seksueel benaderen van kinderen door volwassenen te bestrijden. Ook het gegeven dat hiermee de inzet van de lokpuber weer mogelijk wordt, stemt deze leden tevreden, gelet op het feit dat dit een gemis in de huidige opsporingspraktijk is.
Zekerheidshalve vragen deze leden of de regering met onderhavig wetsvoorstel nu ook haar toezegging volledig gestand heeft gedaan «sexting» (het verspreiden of delen van seksueel getinte foto's of berichten via mobiele telefoons of andere mobiele media) wettelijk te bestrijden (zie Kamerstuk 28 684, nr. 443).
Ten aanzien van het Verdrag van Lanzarote inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik vragen de leden van de CDA-fractie of Nederland als EU-voorzitter voor zichzelf geen rol ziet weggelegd om juist nu andere lidstaten te bewegen om grooming ook op nationaal niveau strafbaar te stellen.

De leden van de ChristenUnie-fractie vragen zich af of het wenselijk is om nadere elementen van uitlokking in ons strafrechtelijke stelsel mogelijk te maken. Kan de regering nader onderbouwen waarom zij de inzet van een «lokpuber» bij grooming een gerechtvaardigd middel acht. Kan de

regering aangeven op welke plekken in het Wetboek van Strafrecht dergelijke uitlokking reeds mogelijk is?

De leden van GroenLinks-fractie onderkennen een zekere spanning bij de inzet van zogenoemde lokpubers. Zonder afbreuk te doen aan de ernst van het delict van grooming, vragen deze leden zich af hoe in de praktijk voorkomen wordt dat verdachten niet op eigen initiatief, maar min of meer ertoe worden gebracht een afspraak tot stand proberen te brengen. Kan de regering uiteenzetten hoe uitlokking in de praktijk voorkomen wordt? Daarnaast zien deze leden dat voor een begin van uitvoering voldoende wordt geacht dat de verdachte een voorstel voor een ontmoeting doet. Tussen het moment van het voorstellen voor een ontmoeting en de ontmoeting zelf zou verdachte op eigen initiatief kunnen afzien van die geplande ontmoeting. Moet niet voor strafbaarheid vereist worden dat verdachte ook daadwerkelijk de daad bij het woord voegt? Het is immers niet uitgesloten dat verdachten pas achteraf in beeld komen en vervolgd worden voor een groomingafspraak, waarbij uiteindelijk door verdachte is afgezien van daadwerkelijke uitvoering. De aan het woord zijnde leden vragen zich voorts af wat in de brief van het wetenschappelijke bureau van het OM (van 13 april 2015) wordt bedoeld met de opmerking dat opsporing door het niet-inzetten van lokpubers vrijwel onmogelijk is geworden. Bestaan er zo beschouwd nog mogelijkheden tot opsporing? Waaruit bestaan die en in hoeverre bieden deze opsporingsmogelijkheden subsidiaire alternatieven voor de voorgestelde wettekst?

6. De online handelsfraude

De leden van de SP-fractie zijn verheugd te lezen dat online handelsfraude specifiek strafbaar wordt gesteld. Men moet zich bij herhaling schuldig maken aan het verkopen of aanbieden zonder te leveren. Wat is bij herhaling? De leden lezen voorts weinig over de rol van online advertentiesites, zoals Marktplaats en Ebay. Wat is hun rol bij de aanpak van online handelsfraude? Hoe vindt samenwerking plaats tussen overheid, opsporingsinstanties en deze private partijen?

De leden van de CDA-fractie vragen of de voorgestelde regeling alle genoemde grenzen in de huidige rechtspraktijk nu volledig wegneemt om online handelsfraude effectief te kunnen bestrijden.

De leden van de D66-fractie lezen dat vanwege de schaarse capaciteit voor opsporing en vervolging het OM en de politie prioriteiten moeten stellen en dat niet bij ieder geval van internetfraude kan worden overgegaan tot opsporing en vervolging. Hoe wordt die keuze gemaakt? Tegen de achtergrond van het zeer ingrijpende voorliggende wetsvoorstel vragen deze leden hoe deze voetnoot bij opsporing en vervolging van internetfraude zich verhoudt tot de verwachtingen die de Wet computercriminaliteit III, en vooral de ronkende persberichten van de regering hierover, bij mensen zijn gewekt. Wat mag en kan wel worden verwacht bij de aanpak van internetfraude?

7. Financiële paragraaf

De leden van de SP-fractie lezen dat er wederom als uitgangspunt wordt genomen dat uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk dekken binnen het reguliere budget. Dit lezen voornoemde leden nu zo ongeveer in elk wetsvoorstel van de regering. In hoeverre zal hier in de gaten worden gehouden of uitvoerende organisaties, vooral politie en rechtspraak, genoeg middelen hebben om deze taken uit te voeren? Hoe is er rekening gehouden met de

bezuinigingen op ICT bij de politie? Is er voldoende expertise bij de politie om deze extra bevoegdheden op te vangen? Zijn er bovendien genoeg middelen om alle experts op te leiden om niet alleen om te gaan met de bevoegdheid, maar ook met de techniek die erbij komt kijken?
Kan de regering een overzicht geven van de extra bevoegdheden die de rechter-commissarissen de afgelopen jaren erbij hebben gekregen en welk (extra) budget daartegenover heeft gestaan?
Deze leden vragen nogmaals aandacht voor de capaciteit bij de politie. Er wordt 2.000 fte weggehaald bij de politie. Hoeveel extra capaciteit kan dan worden ingezet bij uitvoering van bevoegdheden op grond van dit wetsvoorstel? Komt deze capaciteit van binnen de nationale politie? Zo ja, waar vandaan? Of worden er nieuwe mensen aangetrokken? Kan de regering haar antwoord toelichten?

De leden van de CDA-fractie vragen of de regering het verschil in de werklaststijging voor met name de rechter-commissaris kan weergeven tussen onderhavig wetsvoorstel en het conceptwetsvoorstel. In hoeverre is het in dat kader verstandig geweest om de zelfstandige bevelsbevoegdheid uit het conceptwetsvoorstel voor de officier van justitie te schrappen?
Met verwondering hebben de leden van de CDA-fractie kennisgenomen van het standpunt dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk moeten dekken binnen het reguliere budget zonder dat de regering daarbij aangeeft wat die precieze kosten zijn. Alleen voor de Raad voor de rechtspraak (Rvdr) is een verwachte inschatting gegeven (€ 500.000) en alleen al daarvan kunnen deze leden zich voorstellen dat het geen eenvoudige klus zal zijn voor de Rvdr om dit binnen de huidige financiële (beperkte) begroting in te passen. Hoe ziet de regering dit aspect?
De aan het woord zijnde leden vragen of de regering de mening deelt dat het bizar is dat de Kamer gelijktijdig met onderhavig wetsvoorstel wel een privacy impactanalyse ontvangt maar geen impactanalyse van de werklastgevolgen voor de betrokken organisaties. Gelet op de omvangrijke lobby van privacyorganisaties bij onderhavig wetsvoorstel en de financiële en personele problemen bij de strafrechtsketen, hadden deze leden dit liever andersom gezien.
De leden van de CDA-fractie lezen echter in de adviezen van de nationale politie (van 16 juli 2013 en 12 december 2014) dat er wel degelijk een impactanalyse heeft plaatsgevonden in verband met de consequenties van het conceptwetsvoorstel. Waarom heeft de regering deze impactanalyse niet aan de Kamer gezonden dan wel de resultaten hiervan verwerkt in onderhavig wetsvoorstel? Is zij alsnog bereid zo spoedig mogelijk na ontvangt van dit verslag deze impactanalyse aan de Kamer te zenden? Wat zijn precies de aanzienlijke consequenties waarover de nationale politie het heeft in haar advies van 12 december 2014? Wat betekent onderhavig wetsvoorstel niet alleen budgettair, maar ook qua aantal benodigde extra fte voor de uitvoering hiervan? In het bijzonder vragen deze leden of er voldoende capaciteit in de technische teams is aanwezig is. Valt te verwachten dat er veel meer gebruik zal worden gemaakt van de voorgestelde bevoegdheden? Zo ja, past zij hierop de personele bezetting van technische en tactische teams dan ook aan?
Deze leden vragen wat de stand van zaken is van het implementatieplan van de nationale politie, waarnaar wordt verwezen in het hierboven genoemde advies.
De leden van de CDA-fractie vragen of er nog meer impactanalyses zijn opgesteld, bijvoorbeeld ten aanzien van het OM. Indien dat het geval is, vragen zij de regering deze aan de Kamer te doen toekomen. Zo lezen zij ook dat er een «quick-scan online handelsfraude» is uitgevoerd. Ook deze zouden zij graag ontvangen in het kader van de behandeling van dit wetsvoorstel.

De leden van de D66-fractie constateren dat de regering ervan uitgaat dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk dekken binnen het reguliere budget. De Rvdr verwacht dat de extra kosten zullen oplopen tot 500.000 euro per jaar. Voor de politie en het OM ontbreken de bedragen. Deze leden missen de financiële gevolgen die uit het wetsvoorstel zullen voortvloeien voor de politie. Indien het regering aangeeft dat gevolgen ten koste komen van het totaal beschikbare budget voor de politie, aan welke bedragen moet dan gedacht worden en wat betekenen de financiële gevolgen van het voorstel voor andere activiteiten van de politie die uit hetzelfde bestaande budget gefinancierd worden?
Deze leden vragen de regering de Kamer een impactanalyse met kostenplaatje te doen toekomen gelijktijdig met nota naar aanleiding van het verslag zodat de Kamer ook daar kennis van kan nemen.
De leden van de D66-fractie vragen om een reactie op het bericht van de politie dat zij de nieuwe online opsporingstaken niet kan gaan uitvoeren als er voor 40 miljoen euro moet worden bezuinigd op de ICT, zoals de regering wil. Het plaatsvervangend hoofd van de Landelijke Recherche noemt de twee ambities van de regering «volstrekt onverenigbaar» en zegt dat «de politiek heel veel vraagt van de politie en zich goed moet afvragen waar de prioriteit ligt.» Wat is uw reactie op deze noodklok van de recherche en hoe denkt u er in te voorzien dat de ICT-faciliteiten van de politie geschikt zijn om de nieuwe hackbevoegdheden te kunnen uitvoeren?

8. De adviezen over het wetsvoorstel

8.1 Het onderzoek in een geautomatiseerd werk

De leden van de SP-fractie merken op dat de Autoriteit Persoonsgegevens erop wijst dat het bereik van de voorgestelde bevoegdheid zich uitstrekt tot een zeer grote hoeveelheid gegevens. Deze leden hebben hier eerder al hun zorgen over geuit. Hoe groot is de kans dat opsporingsdiensten stuiten op gegevens van niet-verdachten? Hoe wordt hiermee omgegaan? Volgens de regering blijkt uit een masterscriptie dat het voorgestelde artikel 126nba Sv in beginsel de noodzakelijkheidstoets van artikel 8, tweede lid, EVRM kan doorstaan. Wat wordt bedoeld met in beginsel? Wanneer niet?
Ook willen de leden van de SP-fractie weten hoe wordt gecontroleerd of de software buiten de grenzen van de bevoegdheid kan worden ingezet, zoals Bits of Freedom opmerkt. Wat zijn de ervaringen van de Duitse autoriteiten hiermee, maar ook waar het gaat om aanvallen van derden? In hoeverre zijn IT-bedrijven en instanties betrokken bij de totstandkoming van onderhavig wetsvoorstel? Zo, nee zij niet betrokken zijn, waarom niet?
De leden van de SP-fractie vragen een reactie op de zorgen van de Rvdr over de binnendringingsbevoegdheid op buitenlandse geautomatiseerde werken. Betrokken justitieel personeel zal zich dan namelijk naar het recht van zeer veel landen schuldig maken aan het misdrijf van computervredebreuk, met alle gevolgen van dien.

De leden van de CDA-fractie vragen of de regering met verbazing de bijdragen van het OM en in iets mindere mate de nationale politie heeft beluisterd tijdens het rondetafelgesprek dat de Kamer op 11 februari 216 over onderhavig wetsvoorstel heeft georganiseerd. Het betreft dan specifiek de standpuntbepaling van de vertegenwoordiger van het OM (en het zwijgen van de vertegenwoordiger van de Nationale Politie op dit punt) over de toegevoegde waarde van het encryptiebevel waarmee verdachten gedwongen kunnen worden gegevens te ontsleutelen.
De betreffende vertegenwoordiger van het OM gaf aan geen kennis te hebben van eerdere adviezen die het OM hierover had verstrekt, meer

specifiek ook het schriftelijke advies van 8 juli 2013 van het College van procureurs-generaal in de consultatieronde. Los van dat feit verbaasde het deze leden dat door het OM op deze wijze expliciet afstand werd genomen van de waarde van het encryptiebevel voor de opsporing. Kan de regering aangeven hoe het OM de betreffende vertegenwoordiger heeft voorbereid op deze hoorzitting? Wat is nu precies het standpunt van het OM ten aanzien van het terugkomen in het wetsvoorstel van het encryptiebevel? Ook vragen deze leden de regering dit nogmaals te inventariseren bij de nationale politie en bij andere betrokken veiligheidsdiensten in de keten.
In het genoemde advies van 8 juli 2013 geeft het College van procureurs-generaal aan om het decryptiebevel mogelijk te maken bij verdenking van een misdrijf waarop 8 jaar of meer gevangenisstraf staat en er aanwijzingen bestaan voor een concreet gevaar voor het leven of de vrijheid van een persoon of de veiligheid van de staat. Dit verwoordt het College van procureurs-generaal naar aanleiding van de keuze van de regering in het conceptwetsvoorstel om enkel dit bevel mogelijk te maken bij terroristische misdrijven en kinderpornografie. Voor beiden is wat betreft de leden van de CDA-fractie veel te zeggen, maar het volledig schrappen is in hun ogen een gemiste kans.
De aan het woord zijnde vragen hoe het schrappen van het decryptiebevel valt te plaatsen in het licht van eerdere uitlatingen van de voormalige Minister van Veiligheid en Justitie. Naar aanleiding van vragen vanuit de Kamer heeft de Minister onderzoek laten doen naar de ervaringen met het decryptiebevel in het Verenigd Koninkrijk. Hierover schrijft hij op 27 januari 2012 dat deze aanpak «positief gewaardeerd» wordt en dat hij een positieve houding inneemt over de mogelijkheden van een vergelijkbare regeling in Nederland (Kamerstuk 31 015, nr. 77, p. 6). Op 12 oktober 2012 bericht de Minister de Kamer opnieuw over dit onderwerp. Hij geeft aan deze ontsleutelplicht verenigbaar is met het nemo tenetur-beginsel (dat verdachten niet actief hoeven mee te werken aan hun eigen veroordeling) mits de regeling met goede waarborgen is omkleed (Kamerstuk 31 015, nr. 79, p. 6). Wat is er sedertdien veranderd dat de regering gevolg heeft gegeven aan de argumentatie van de Afdeling advisering van de Raad van State dat de ontsleutelplicht zich niet goed verhoudt tot het nemo tenetur-beginsel als onderdeel van artikel 6 EVRM? Immers, pas na dit advies heeft de regering haar standpunt gewijzigd. Dat was eerder na de consultatieronde nog niet het geval. Opmerkelijk genoeg kunnen de leden van de CDA-fractie in het advies van de Afdeling advisering geen verwijzingen naar Europese jurisprudentie terugvinden, waaruit zou blijken dat het encryptiebevel niet kan worden gegeven in het licht van artikel 6 EVRM. Deelt de regering deze mening? Zo ja, kan de regering dan toelichten waarom zij desalniettemin deze keuze heeft gemaakt?
De aan het woord zijnde leden vragen de regering voorts in te gaan op de gevolgen die deze keuze heeft voor de bestrijding op nationaal- en internationaal niveau van onder meer kinderpornonetwerken. Ziet de regering nog steeds het nut in van haar oorspronkelijke voorstel dan wel in de voorgestelde wijziging door het College van procureurs-generaal (8 juli 2013), zodat in de meest gruwelijke en ernstige feiten het bevel voor een doorbraak in het opsporingsonderzoek kan zorgen? Zo ja, is zij bereid dit onderdeel alsnog in het wetsvoorstel op te nemen?

8.2 Het wederrechtelijk overnemen en helen van gegevens

De leden van de CDA-fractie vinden het een gemiste kans dat in het wetsvoorstel geen regeling is opgenomen om een domeinnaam van een website te verwijderen. Ondanks de genoemde mogelijkheden om dit te ontwijken, geeft dit toch een mogelijkheid om tegen misleidende websites op te treden? Gaat bovendien van deze verwijdering niet een belangrijke signaalwerking uit, niet in de laatste plaats richting de betreffende

persoon daar hij/zij letterlijk en figuurlijk in beeld is bij politie en justitie? Wat stelt de regering voor in plaats daarvan te doen? Ook het College van procureurs-generaal stelt voor een wettelijke bevoegdheid te creëren waardoor het mogelijk wordt te bevelen dat een domeinnaam wordt doorgehaald of wordt overgeschreven naar de overheid. De leden van de CDA-fractie vragen of de regering bereid is haar keuze op dit punt te heroverwegen.

II ARTIKELSGEWIJZE TOELICHTING

Artikel I, onderdeel C

Artikel 138c

De leden van de CDA-fractie delen de mening van de Nederlandse Vereniging voor Rechtspraak (NVvR) dat de voorgestelde strafbedreiging van een jaar te laag is. De vergelijking met een andere strafbedreiging gaat hier volgens deze leden mank, gelet op de ernstig en impact die bijvoorbeeld bedrijfsspionage heeft, hetgeen overigens ook kan worden beweerd voor schending van een bedrijfsgeheim (artikel 273 Wetboek van Strafrecht (Sr)). Deze leden vragen hoe de regering er daarom over denkt om een hogere strafmaat op te nemen voor niet alleen het voorgestelde artikel maar ook ten aanzien van het al bestaande artikel 273 Sr.

Artikel I, onderdelen F en G

Artikelen 248a en 248e

De leden van de SP-fractie vinden het moeilijk voor te stellen hoe bij grooming bewezen kan worden dat een verdachte het oogmerk had van seksueel misbruik van een kind beneden de leeftijd van zestien jaren. Wat als er slechts een vermoeden is? Er wordt gesteld dat veroordeling kan plaatsvinden als er meerdere keren is aangedrongen op een ontmoeting. Daarmee is echter nog niet automatisch vastgesteld dat sprake is van het oogmerk van seksueel misbruik van een kind van beneden de leeftijd van zestien jaren of zien deze leden dat verkeerd?

Artikel I, onderdeel I

Artikel 326d

De leden van de CDA-fractie vinden de mogelijkheid van voorlopige hechtenis verstandig, maar begrijpen niet goed waarom de regering hieraan heeft gekoppeld dat voor oplegging hiervan eerst vijf jaar moeten zijn verstreken sinds een eerdere onherroepelijke veroordeling. De ernst van het gepleegde feit rechtvaardigt volgens deze leden al dat hiervoor voorlopige hechtenis kan worden opgelegd. Dat kan voorts in het belang van zijn een effectieve opsporing door politie en justitie, maar ook in het kader van voorkomen van het plegen van nieuwe strafbare feiten. Hoe ziet de regering dit?

Artikel II, onderdeel A

Artikel 67

De leden van de CDA-fractie vragen waarom de regering niet bij meer van de voorgestelde strafbaarstellingen de toepassing van voorlopige hechtenis mogelijk maakt, gelet op hierboven genoemde argumenten (ernst van feiten en in kader van opsporing en het voorkomen van nieuwe

strafbare feiten). Zij zouden een aanscherping op dit punt niet meer dan logisch vinden, in elk geval met betrekking tot artikel 248e (grooming).

Artikel II, onderdeel C

Artikel 125m

De leden van de CDA-fractie vragen wat de sanctionering is wanneer de geheimhoudingsverplichting wordt geschonden door bijvoorbeeld webhostingbedrijven.

Artikel II, onderdeel D

Artikel 125p

Vierde lid

De leden van de CDA-fractie vragen (nogmaals)of het wel verstandig is ook een rechterlijke machtiging te vereisen bij het bevel tot ontoegankelijk maken van gegevens, juist gezien de spoedeisendheid waar de regering naar verwijst.

Artikel II, onderdeel G

Artikel 126nba

Eerste lid

De leden van de SP-fractie lezen dat voor de bevoegdheid om te kunnen hacken vereist is dat het geautomatiseerde werk bij de verdachte in gebruik is. Kan het ook gaan om werken waar door de verdachte gebruik van is gemaakt of is echt vereist dat de verdachte er nog steeds gebruik van maakt?
Deze leden constateren dat de officier van justitie moet onderbouwen waarom het nodig is dat onderzoek in een geautomatiseerd werk plaatsvindt. Alternatieven moeten daarbij zijn onderzocht, maar wordt ook onderbouwd waarom een alternatief niet ingezet kan worden? Wordt er bovendien aangegeven hoe groot de kans is dat de privacy van niet-verdachten wordt geschonden en dus inzage kan worden verkregen in meer gegevens dan nodig voor het opsporingsonderzoek? Zo nee, waarom niet? Deze leden achten dit noodzakelijk voor de Centrale toetsingscommissie en de rechter-commissaris om een deugdelijke belangenafweging te kunnen maken. Worden er voorts strengere eisen gesteld aan stelselmatige observatie dan eenmalig onderzoek doen in een geautomatiseerd werk? Zo nee, waarom niet? Zo ja, op welke manier?

De leden van de CDA-fractie delen volledig de bezorgdheid die de nationale politie heeft ten aanzien van de keuze om enkel in te grijpen bij systemen die bij de verdachte in gebruik zijn. Is het in het kader van een effectieve opsporing, en dus in de geest van onderhavig wetsvoorstel, niet van belang een stap voor te kunnen zijn op de digitale crimineel dan wel maximaal een stap achter te lopen? Houdt het wetsvoorstel wel voldoende rekening met criminelen die bewust verschillende apparaten gebruiken als dekmantel voor politie en justitie? Het gebruik van een apparaat van een partner of huisgenoot zal inderdaad voor de politie nog wel te voorzien zijn, maar hoe zit het met een verdachte die afwisselend gebruik maakt van verschillende computer in bijvoorbeeld internetcafés en bibliotheken? Speelt het wetsvoorstel hiermee wel voldoende in op het uitlenen en uitwisselen van telefoons in vriendengroepen en familie-

kringen (die kunnen fungeren als bende)? Graag vernemen deze leden hierop een reactie en desgewenst aanpassing van het wetsvoorstel.

Artikel II, onderdeel U

Artikel 126ee

De leden van de SP-fractie vinden het belangrijk dat eisen worden gesteld aan de software. Zij maken zich alleen zorgen over de controle voorafgaand aan de inzet en tijdens de inzet. Hoe wordt dit gewaarborgd en wie zal deze controle op zich nemen? Wordt dat gedaan door een onafhankelijke instantie zoals bijvoorbeeld de Autoriteit Persoonsgegevens? Zo nee, waarom niet?

Artikel II, onderdeel X

Artikel 552a

De leden van de SP-fractie lezen dat de regering het minder wenselijk vindt om te voorzien in een schadevergoedingsprocedure indien na beklag is gebleken dat ontoegankelijkmaking niet rechtmatig was. Waarom is dit minder wenselijk? De betrokkene heeft schade geleden door overheidshandelen en wordt gedwongen om in een langdurige en dure civiele procedure zijn of haar schadevergoeding te verhalen, terwijl reeds is komen vast te staan dat in strijd met de wet is gehandeld. Net als de Rvdr pleiten deze leden dus voor een afzonderlijke schadevergoedingsprocedure.

De voorzitter van de commissie,
Ypma

De griffier van de commissie,
Nava

Van: 10.2.e
Verzonden: vrijdag 11 maart 2016 10:20
Aan: 10.2.e 10.2.e 10.2.e 10.2.e 10.2.e
d
10.2.e 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: Voorbereiding KMO 16/3 - Operationeel portfolio

Hoi 10.2.e (en portefeuille-adviseurs),

Zoals bij 10.2.e al aangekondigd hierbij de stukken voor het KMO voor komende woensdag over het operationeel portfolio. Ik heb de stukken nog maar net binnengekregen, dus het is kort dag.

10.2.e afgesproken is dat jij de input voor de annotatie coördineert, samenvoegt en aanlevert.
Ik stuur de stukken bij deze ook naar de portefeuilleadviseurs omdat ik aanneem dat zij hierin ook een aandeel hebben.

Deadline input annotatie is weer dinsdag 10.00 uur.
Maandag graag z.s.m. even contact of dit gaat lukken. Ik ben dan de hele dag op de Lookant.

Groet en (toch;-) fijn weekend!

10.2.e

Senior beleidsadviseur
Politie | Landelijke Eenheid | Staf i.o.
afdeling Bestuursondersteuning
Hoofdstraat 54, 3972 LB Driebergen
Bezoekadres: Lookant 2
Postbus 100, 3970 AC Driebergen

Van: 10.2.e
Verzonden: vrijdag 11 maart 2016 11:11
Aan: 10.2.e
CC: 10.2.e ; 10.2.e 10.2.e
Onderwerp: FW: Voorbereiding KMO 16/3 - Operationeel portfolio
Bijlagen: 20160316, 05a. OPLEGNOTA KMO - Operationeel portfolio 2016.docx; 20160316, 05b. Bijlage 1 Uitvoeren specifieke doelgroep (randvoorwaarden geborgd).pdf; 20160316, 05c. Bijlage 2 Uitvoeren generieke doelgroep Scenario 1 + 2.pdf; 20160316, 05d. Bijlage 3 Niet uitvoeren generieke en specifieke doelgroep (randvoorwaarden niet geborgd.pdf; 20160316, 05e. Bijlage 4 Niet uitvoeren wet- en regelgeving zonder harde datum inwerkingtreding.pdf; 20160316, 05f. Bijlage 5 Niet uitvoeren Geen prioriteit.pdf

Hoi 10.2.e,

ik ontvang deze stukken net en heb ze snel doorgenomen.

Begrijp/lees ik nu goed dat CCIII niet in operationeel portfolio zit? En dat we zijn doorgeschoven naar niet uitvoeren in 2016 conform bijlage 4? In de oplegnota wordt dit geadviseerd om de volgende reden:

- 53 opgaven omdat van de onderliggende wet- en regelgeving de datum inwerkingtreding niet hard is *(bijlage 4)* en ondersteun de principiële lijn richting de departementen dat wet- en regelgeving in principe niet in het lopende jaar wordt geïmplementeerd.

Implementatie dit jaar gaat inderdaad lastig worden, maar er dienen voorbereidingen getroffen te worden om klaar te zijn op het moment dat de wet in werking treedt? Kun jij aangegeven wat dit voorstel betekent voor CCIII en de mogeljke consequenties voor bijvoorbeeld de inrichting van het lab en de werkzaamheden die daar plaatsvinden? We zijn net bezig om een gewijzigd PSD op te stellen voor de herziening van de IV-portfolio. Wat betekent dit voor dit proces..

Ik hoor graag je reactie!
Met groet,
10.2.e

OPLEGNOTA KORPSLEIDINGOVERLEG (KMO)

Agendapunt: 5 **Datum:** 16 maart 2016

Onderwerp: Operationeel Portfolio 2016

Aangeboden door c.q. akkoord van (cf. portefeuilleverdeling KL)

☐ **Korpschef: -** ☐ **Directeur korpsstaf: -**
Lid KL:Bik x☐ **Directeur Operatiën: Peije de Meij**
☐ **Programmamanager: -**
☐

Steller: Peije de Meij
Behandelend adviseur staf KL: 10.2.e 10.2.e

x Besluitvormend	☐ **Opinievormend**	☐ **Ter kennisname**

x Openbaar stuk	☐ **Vertrouwelijk stuk**

Gevraagd besluit

Het KMO wordt gevraagd in te stemmen met het volgende:

- Kennis te nemen van de inhoud van het operationeel portfolio 2016 dat bestaat uit:
  - Implementatieopgaven voor de eenheden
  - Voorbereiding implementatie door bedrijfsvoering (implementatie eenheden in 2016 of later)

- Akkoord te gaan met het uitvoeren in 2016 van 30 opgaven voor een specifieke doelgroep *(bijlage 1)*

- Akkoord te gaan met het uitvoeren in 2016 van 26 óf 16 opgaven voor een generieke doelgroep, maak daarbij een keuze tussen scenario 1 of 2 *(bijlage 2):*
  - Scenario 1: het uitvoeren alle 26 opgaven
  - Scenario 2: het uitvoeren van een beperkter aantal van 16 opgaven (i.v.m. het beperkte absorptievermogen wordt dit scenario dringend geadviseerd)

- Te besluiten tot het niet uitvoeren in 2016 van:
  - 32 opgaven met generieke en specifieke doelgroepen omdat de randvoorwaarden niet zijn geborgd. Waar nodig kunnen deze opgaven in de bijstelling van het portfolio 2016 (juli 2016) opnieuw worden gewogen *(bijlage 3).*
    - Maak uitzondering op deze regel voor de opgaven LMO en Raadsman bij Verhoor gezien politiek bestuurlijk context, deze kunnen ook buiten de bijstelling aan de portfolio worden toegevoegd, indien randvoorwaarden zijn geborgd.
  - 53 opgaven omdat van de onderliggende wet- en regelgeving de datum inwerkingtreding niet hard is *(bijlage 4)* en ondersteun de principiële lijn richting de departementen dat wet- en regelgeving in principe niet in het lopende jaar wordt geïmplementeerd.
  - 16 opgaven omdat er geen prioriteit door de portefeuillehouder is toegekend *(bijlage 5).* Voor twee opgaven geldt dat alle randvoorwaarden zijn geborgd, hierin kunnen eenheden een eigen keuze maken (dit betreft: operationele regie BOA's'en Best of three worlds)

Voortraject / afstemming

Met wie is afgestemd	Datum	Akkoord doorgeleiding en/of uitkomst bespreking
☐ KLO		
x KMO	9 maart 2016	De KMO vertegenwoordiging de Jong, Heijsman, Huijzer, Paauw en Vissers hebben deze besluitvorming voorbereid.

☐ BBVO		
x Beleidsdirecties	Voortdurend	Impact op de verschillende beleidsdirecties voortdurend afgestemd (IV-portfolio is afgestemd, resultaten PenM-onderzoek niet beschikbaar)
x Portefeuillehouder	Voortdurend	Portefeuillehouders betrokken geweest bij prioritering
☐ Departement		N.v.t.
x PDC	Voortdurend	Haalbaarheidstoets PDC voor zover mogelijk in tijd
X Directeur S&B	Voortdurend	Afstemming mbt Uitvoeringsplan

Samenvatting notitie/voorstel

In opbouw naar het operationeel portfolio 2016
Voor u ligt het Operationeel Portfolio 2016 dat, ondanks de korte voorbereidingstijd met een integrale afstemming tot stand is gekomen en een grote stap voorwaarts betekent in de ontwikkeling en integraliteit van de vak- en beleidsontwikkeling in ons korps. Het thema van de herijking is meer realisme, dat is ook terug te vinden in dit portfolio. Het portfolio wordt als bouwsteen gebruikt voor het Uitvoeringsplan.
Na het KMO van 16 december jl, waarin het eerste beeld van het aantal opgaven en de weegcriteria werden toegelicht, gaf u aan behoefte te hebben aan een strategisch kader en inzage in de weegcriteria. In twee bijeenkomsten is inhoud gegeven aan dit proces door een vertegenwoordiging van KMO-leden (de Jong, Heijsman, Huijzer, Paauw, Vissers). De opgaven zijn door u in de rol van portefeuillehouder aan de hand van nieuwe criteria gewogen en geprioriteerd op:

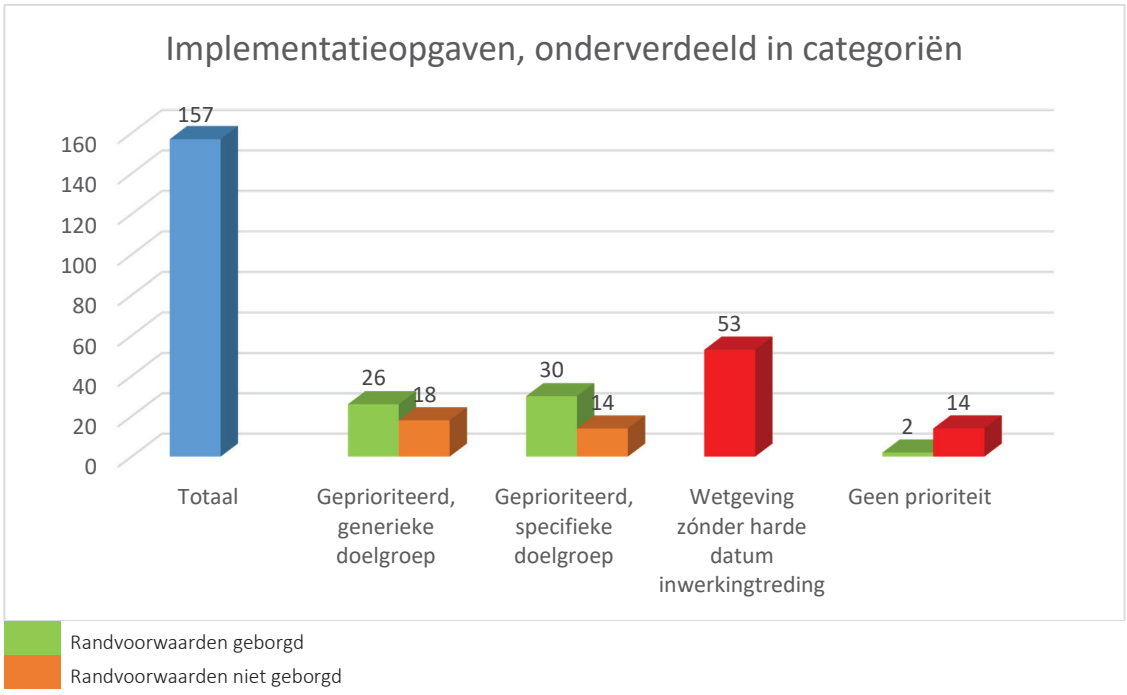
- Specifieke doelgroep
- Nee, tenzij.

De geprioriteerde onderwerpen zijn voorgelegd aan het PDC en de operatiën voor de haalbaarheid en uitvoerbaarheid.

De opgaven bestaan uit de volgende categorieën:

- Opgaven voor een generieke doelgroep in de operatiën (waarvan de randvoorwaarden wel/niet zijn geborgd)
- Opgaven voor een specifieke doelgroep in de operatiën (waarvan de randvoorwaarden wel/niet zijn geborgd)
- Opgaven wet- en regelgeving waar geen harde datum van inwerkingtreding aan ten grondslag ligt.
- Opgaven die door de portefeuillehouder zijn gedeprioriteerd voor 2016.

In onderstaand schema en bijlagen wordt dit nader toegelicht.



Het KMO wordt gevraagd akkoord te gaan met het uitvoeren van (een deel van) de generieke en de specifieke opgaven waarvan de randvoorwaarden zijn geborgd. Geadviseerd wordt de overige opgaven te

faseren naar ‘na 2016’. Dit advies levert een daling van het aantal opgaven op van 157 naar 56 of mogelijk zelfs naar 46 opgaven voor dit jaar (verschil tussen scenario 1 en 2).

Een vastgesteld portfolio 2016, en dan …
De opgaven in het portfolio worden dit jaar geïmplementeerd door de eenheden of voorbereid door de bedrijfsvoering. De context waarin dit moet gebeuren is complex door o.a. de veranderopgave die er nog naast loopt, de betaalbaarheid van het korps en de externe vraagstukken zoals migratie en terreur die veel van ons vragen.

Een aantal afspraken en instrumenten zijn nodig om tot een goede uitvoering van het portfolio te komen:
- Implementatiekalender:
  Er wordt een implementatiekalender ontwikkeld met de afdelingen Politieprofessie zodat zij inzicht en overzicht houden gedurende het jaar. Hierbij zal oog zijn voor de verschillende behoeftes en mogelijkheden van eenheden. Daar waar dat mogelijk is zullen implementatietrajecten worden gecombineerd, zodat minder implementatiecapaciteit nodig is en wordt nader overleg gevoerd over differentiëren van de doorlooptijd als er teveel opgaven in een bepaalde periode zijn.
- Inzet PDC:
  Op basis van de beschikbare informatie van de portefeuilles heeft het PDC op hoofdlijnen aangegeven wat mogelijk is. De exacte ondersteuning vanuit het PDC dient in overleg tussen de portefeuille en het PDC te worden bepaald. Net als de eenheden moet ook het PDC in werking worden gebracht, vanuit de herijking wordt hier prioriteit aan gegeven.
- Monitoring:
  De opgaven in de portfolio zullen periodiek worden gemonitord dit jaar. Niet alleen omdat het operationeel portfolio als bouwsteen wordt gebruikt voor het Uitvoeringsplan, maar ook voor de interne betrouwbaarheid en transparantie. De wijze van monitoring wordt op korte termijn uitgewerkt met Control en de hoofden Politieprofessie.
- Bijstelling van het operationeel portfolio in juli 2016:
  In het KMO van 6 juli zal er een review op het portfolio 2016 plaatsvinden.
- Aanvragen Tijdelijke Voorzieningen:
  In oktober 2015 is reeds de uitvraag gedaan voor tijdelijke voorzieningen (programma’s en projecten) in 2016. Onder voorbehoud van betaalbaarheid worden de aangevraagde voorzieningen, die te relateren zijn aan de opgaven uit het portfolio toegekend. Daar waar het voorzieningen betreft waarin beleidsontwikkeling plaatsvindt (geen implementatie) worden ook deze toegekend mits geen extra ontwikkelcapaciteit bij het PDC wordt gevraagd. De definitieve terugkoppeling naar de portefeuillehouders zal na het KMO van 16 maart 2016 plaatsvinden. Nieuwe aanvragen kunnen via reguliere werkwijze bij de afdeling programmamanagement worden aangevraagd.

Afhankelijk van het gekozen scenario staan 111 of 101 onderwerpen NIET in de portfolio. Op een deel van de onderwerpen gaat de beleidsontwikkeling door, maar er vindt geen implementatie plaats. Dit heeft consequenties:
- De portefeuillehouder informeert de betrokkenen, zowel intern als extern. Tevens dient het portfolio te worden besproken met de COR. De consequenties van het portfolio dienen te worden besproken met DG POL i.v.m. eerder gemaakte afspraken en gedane toezeggingen door de Minister aan de Tweede Kamer.
- Daar waar randvoorwaarden waren gereserveerd, maar de opgave niet in de portfolio wordt opgenomen, vervallen deze voor 2016. Deze resources komen dan ten goede aan het realiseren van de ontwikkelingen in de portfolio. Denk hierbij ook aan (advies)capaciteit binnen de portefeuille, beleidsdirecties en uitvoeringscapaciteit van het PDC. Dit kan voor collega’s teleurstellend zijn en tot onbegrip leiden. Begeleiding hierbij en sturing hierop is noodzakelijk om een ongewenste onderstroom te voorkomen.
- Daar waar de beleidsontwikkeling nog doorgaat op onderwerpen dient rekening te worden gehouden met het risico op een stuwmeer aan opgaven.

Consequenties (afgestemd met relevante betrokkenen)

X Personeel/ HRM		
X Financieel		
X Informatievoorziening		
X Facility Management		
☐ Communicatie		
☐ Juridisch		
☐ Politiek-bestuurlijk		

X Operatie		
X Uitvoeringstoets PDC		
☐ Realisatie NP		
☐ Personele reorganisatie		
☐ Administratieve lasten		

Vervolgtraject

Overleg		Overleg	
☐ KMO	☐ bespreking/opinievorming ☐ ter integrale toetsing/impactanalyse ☐ ter implementatie ☐ ter kennisgeving	x☐ COR (WOR)	X ter informatie ☐ voor instemming ☐ voor advies
☐ SDO	☐ ter integrale toetsing/impactanalyse ☐ ter implementatie ☐ ter kennisgeving	☐ Vakbonden	☐ formeel, via CGOP ☐ informeel via overleg KL-vakbonden
☐ overleg met de minister	☐ ter besluitvorming ☐ ter bespreking/opinievorming ☐ ter kennisgeving	☐ Programma-raad	☐ ter bespreking/opinievorming ☐ ter kennisgeving
☐ Overleg met DG Pol	☐ ter besluitvorming ☐ ter bespreking/opinievorming ☐ ter kennisgeving	☐ met ….	☐ ter bespreking/opinievorming ☐ ter kennisgeving ☐ ....
☐ Projectmana-gersoverleg	☐ ter bespreking/opinievorming ☐ ter implementatie ☐ ter kennisgeving	☐ met ….	☐ ter bespreking/opinievorming ☐ ter kennisgeving ☐ ....

Communicatie

☐ Verantwoordelijke:	
☐ Strategische boodschap:	

Uitvoering / implementatie / monitoring

☐ Verantwoordelijk:	Peije de Meij
☐ Voortgangsrapportage:	Monitoring en implementatie kalender

Documenten

Titel (hoofd)document en bijlagen

- 5

Domein	Portefeuilles	Implementatieopgaven	Toelichting PDC	Korte toelichting inhoud implementatieopgave	Soort verplichting

Niet onder reikwijdte

	Cybercrime	Borging LMIO + doorontwikkeling Landelijk Servicecentrum e-Crime	Planvorming is going concern en kan in overleg worden gedaan.	Op dit moment wordt mn. LMIO geborgd. Dit betreft tijdelijke handmatige invoer van meldingen tot realiseren van een technische oplossing, personele inrichting en het realiseren van een webservice voor digitale aangifte. Voor de langere termijn wordt een bredere voorziening ontwikkeld waarmee meldingen en aangiften op het gebied van e-crime, mn. cybercrime en fraude kunnen worden ontvangen, geregistreerd, geanalyseerd en evt. opgewerkt tot projectvoorstel. Dit leidt tot betere dienstverlening aan burgers en bedrijven en meer overzicht en inzicht en daarmee betere sturingsmogelijkheden op de aanpak. Het realiseren van de mogelijkheid van internetaangifte is ook een belangrijke doelstelling. In 2016 ligt de nadruk op: laatste activiteiten voor borgen LMIO 7-12 uitbreiding naar 7-12 en het in afstemming met de PDC en pf Fraude en Dienstverlening ontwikkelen van een integraal plan van aanpak. Ook is er een afhankelijkheid naar het realiseren van de webservice voor digitale aangiften (=is geen onderdeel van de pf) Niet meegenomen in inrichting; wordt als pilot uitgevoerd DLOC, maatschappelijke verplichting 250.000 aangiften, gekoppeld aan horizontale fraude veiligheidsagenda. 7-12 Alleen voor de planvorming is ondersteuning van het PDC dit jaar noodzakelijk. Financiering voor 2016: Borging LMIO en maken plan van aanpak is rond.	Herijking, borging LMIO is toezegging TK
		In werking brengen Digitaal Opsporen (incl. instroom Cybercrime experts en Hansken)	Realisatie 2 transferia, instroom cyber + faciliteiten voor instroom (in afstemming te bepalen)	Het in samenhang tot stand brengen van organisatorische, personele en technische maatregelen die nodig zijn om een landelijk gestandaardiseerde inrichting en werking van het digitale werkveld tot stand te brengen. Betreft o.a. het realiseren van zijinstroom en het in samenhang daarmee realiseren van de benodigde randvoorwaarden op het gebied van Huisvesting (FM), IV voorzieningen, en opleidingen (HRM). Cybercrime vraagt om actueel blijven in modus operandi etc. . Vanwege digitalisering van criminaliteit is digitaal opsporen steeds belangrijker. Sluit aan bij het in werking brengen van de organisatie op het gebied van digitaal opsporen met specifieke aandacht voor organisatie, mensen en middelen.	Afspraak Minister, Herijking, Gemeenschappelijke Veiligheidsagenda

Niet onder reikwijdte

Bijlage 2: Uitvoeren generieke doelgroep (randvoorwaarden geborgd), scenario 1 + 2

Domein	Portefeuilles	Implementatieopgaven	Scenario 1 (alles uitvoeren)	Scenario 2 (beperkt)	Toelichting PDC	Korte toelichting inhoud implementatieopgave	Soort verplichting
Niet onder reikwijdte							


Niet onder reikwijdte

Bijlage 3: Niet uitvoeren generieke en specifieke doelgroep (randvoorwaarden niet geborgd)

Domein	Portefeuilles	Implementatieopgaven	Toelichting PDC	Korte toelichting inhoud implementatieopgave	Soort verplichting
Niet onder reikwijdte					

Niet onder reikwijdte

Bijlage 4: Niet uitvoeren wet- en regelgeving zonder harde datum van inwerkingtreding

Domein	Portefeuilles	Implementatieopgaven

Niet onder reikwijdte

Niet onder reikwijdte

	Cybercrime	Implementatie Wet Computer Criminaliteit III							

Niet onder reikwijdte

Niet onder reikwijdte
0328

Bijlage 5: Niet uitvoeren Geen prioriteit

Domein	Portefeuilles	Implementatieopgaven	Korte toelichting inhoud implementatieopgave	Soort verplichting
Niet onder reikwijdte				

Niet onder reikwijdte

Van: Philips, Inge (I.C.)
Verzonden: vrijdag 11 maart 2016 11:16
Aan: 10.2.e 10.2.e
CC: 10.2.e ; 10.2.e
Onderwerp: Re: Voorbereiding KMO 16/3 - Operationeel portfolio

9
. Groet Inge

Groet,

10.2.e
Plv Diensthoofd
Politie - Landelijke Recherche

Van: 10.2.e
Verzonden: vrijdag 11 maart 2016 17:28
Aan: 10.2.e Philips, Inge (I.C.)
CC: 10.2.e ; 10.2.e
Onderwerp: RE: Voorbereiding KMO 16/3 - Operationeel portfolio

Hoi 10.2.e , Inge,

Ik lees het inderdaad ook zo. Misschien goed nog even naar het proces te kijken, zoals dat ook staat in de oplegnota.Daaruit kunnen ook de beïnvloedingsmogelijkheden afgeleid worden.

Na het KMO van 16 december jl, waarin het eerste beeld van het aantal opgaven en de weegcriteria werden toegelicht, gaf het KMO zelf aan behoefte te hebben aan een strategisch kader en inzage in de weegcriteria. 5 leden van het KMO hebben zich toen opgeworpen om zich verantwoordelijk te maken voor het bepalen van de weegcriteria en de prioritering op basis daarvan (de Jong, Heijsman, Huijzer, Paauw, Vissers). In twee bijeenkomsten is inhoud gegeven aan dit proces door die vertegenwoordiging van KMO-leden. Vervolgens is aan de eenheidschefs in de rol van pfh gevraag de opgaven te prioriteren.

In de afgelopen week heb ik in afstemming met 10.2.e en Theo vd Plas nog een slag gemaakt op de input vanuit de pf D&C voor dit proces en daarin ook het belang van de voorbereiding CCIII en beschikbaarheid van IV uren meegegeven (in afstemming met 9

Echter concludeer ik dat alle wetsvoorstellen waarvan nu geen harde datum bekend is door de KMO trekkers op dezelfde manier behandeld worden: niet uitvoeren.
Voor een groot aantal wetsvoorstellen is dit denk ik best een goede strategie om wat tegendruk te geven richting V&J en rust te krijgen in de organisatie, met name voor de wetsvoorstellen die niet direct een grote meerwaarde hebben
voor de politie. Echter niet voor allemaal, waaronder CCIII.

Aangezien het KMO zelf trekker is van het proces en het voorstel besproken wordt in het KMO stel ik voor goede argumentatie aan te leveren voor de annotatie van Theo, zodat hij dat daar kan adresseren (actie 9 i en 10.2.e . Ik zal ook Peije de Meij informeren op basis hiervan, omdat die ook in het KMO aanwezig is.

Ik kom nog met een voorzet voor de annotatie.

Groet,

10.2.e

Van: Philips, Inge (I.C.)
Verzonden: vrijdag 11 maart 2016 17:38
Aan: 10.2.e 10.2.e
CC: 10.2.e 10.2.e
Onderwerp: RE: Voorbereiding KMO 16/3 - Operationeel portfolio

Mooi, die argumentatie hebben we nog liggen van de vorige keer. Wat mij betreft niets aan veranderd. 10.2.e knip en plak jij die in een bericht voor Theo? GRoet en fijn weekend aan allen!

Inge

Van: 10.2.e
Verzonden: maandag 14 maart 2016 14:22
Aan: 10.2.e 10.2.e
CC: 10.2.e 10.2.e Philips, Inge (I.C.); 10.2.e
Onderwerp: Input voor KMO annotatie operationeel portfolio-CCIII

Hallo 10.2.e

Hierbij zoals afgesproken de argumenten voor de annotatie van Theo voor het KMO ivm. de deprioritering van CCIII in het voorstel operationeel portfolio:

- De wetsvoorstellen zonder definitieve datum inwerkingtreding hebben een verschillende status en belang voor de politie
- De voorbereiding van alle wetsvoorstellen zonder datum in werking treding allemaal stil zetten is daarom te kort door de bocht.
- Het wetsvoorstel Computercriminaliteit III ligt al in de Kamer (schriftelijke vragen zijn al ingediend) en is operationeel van groot belang voor de aanpak van cybercrime. De politie zit hier al jaren op te wachten. Er wordt nu uitgegaan van datum in werking treding 01-01-2017.
- Cybercrime is geprioriteerd in de Gemeenschappelijke Veiligheidsagenda en in de Herijking
- Met name de nieuwe bevoegdheid “Binnendringen in een geautomatiseerd werk” is qua werkwijze volledig nieuw en vergt voldoende voorbereidingstijd met ondersteuning van de PDC (m.n. IV) om te komen tot een zorgvuldige uitvoering. Dus ook los van datum in werking treding
- De voorbereiding van de implementatie raakt een beperkte groep 7-12 Er is geen operationele belasting van de eenheden.
- De voorbereiding van de implementatie loopt al volop met (beperkte) IV ondersteuning en er zijn al een aantal mensen voor vrijgemaakt. Er is in 2015 ook al 1,5 mln uitgegeven waaronder een investering in een testomgeving.
- Voor 2016 ligt er een begroting van 2,7 miljoen voorzien vanuit het bestedingsplan 2016 bijz. bijdrage Digitalisering en Cybercrime vanuit het Ministerie V&J (De posten bestaan uit: 500.000 euro opleiding, 500.000 euro externe inhuur voor het bouwen van het lab, 200.000 euro inrichting beveiligingsmaatregelen, 1.500.000 middelen en licentiegeld.)
Het niet besteden van de gelden van de bijzondere bijdrage D&C ligt politiek bestuurlijk zeer gevoelig. Zeker nu 12-14
- Het doorzetten van de ontwikkeling op CCIII is van strategisch belang in relatie tot versterken opsporing in zijn algemeenheid en de ontwikkeling van Digitale opsporing in het bijzonder.

Met vriendelijke groet,

10.2.e
10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën | 9
Nieuwe Uitleg 1, 2514 BP, Den Haag

From: 10.2.e
Sent: Monday, March 14, 2016 02:53 PM W. Europe Standard Time
To: Meij, Peije de (P.)
Subject: Input voor KMO operationeel portfolio

Hallo Peije,

Komend KMO staat het operationeel portfolio op de agenda zoals je weet. De keuze is daarbij gemaakt om alle wetgevingsvoorstellen waarvoor nog geen definitieve implementatiedatum is vastgesteld te deprioriteren. Dat pakt heel naar uit voor het wetsvoorstel CCIII. Daarvoor lopen al allerlei voorbereidingen om dit operationeel mogelijk te maken. Hier is voldoende tijd voor nodig met ondersteuning PDC om een zorgvuldig proces in te richten. Er is ook al veel geld voor opgenomen in het bestedingsplan D&C van komend jaar. Bij stilleggen is er een risico dat dan onderuitputting ontstaat en dat terwijl we 12-14 !

12-14

Argumenten voor door laten gaan van CCIII voorbereiding van de implementatie:
- De wetsvoorstellen zonder definitieve datum inwerkingtreding hebben een verschillende status en belang voor de politie
- De voorbereiding van alle wetsvoorstellen zonder datum in werking treding allemaal stil zetten is daarom te kort door de bocht.
- Het wetsvoorstel Computercriminaliteit III ligt al in de Kamer (schriftelijke vragen zijn al ingediend) en is operationeel van groot belang voor de aanpak van cybercrime. De politie zit hier al jaren op te wachten. Er wordt nu uitgegaan van datum in werking treding 01-01-2017.
- Cybercrime is geprioriteerd in de Gemeenschappelijke Veiligheidsagenda en in de Herijking
- Met name de nieuwe bevoegdheid “Binnendringen in een geautomatiseerd werk” is qua werkwijze volledig nieuw en vergt voldoende voorbereidingstijd met ondersteuning van de PDC (m.n. IV) om te komen tot een zorgvuldige uitvoering. Dus ook los van datum in werking treding
- De voorbereiding van de implementatie raakt een beperkte groep 7-12 . Er is geen operationele belasting van de eenheden.
- De voorbereiding van de implementatie loopt al volop met (beperkte) IV ondersteuning en er zijn al een aantal mensen voor vrijgemaakt. Er is in 2015 ook al 1,5 mln uitgegeven waaronder een investering in een testomgeving.
- Voor 2016 ligt er een begroting van 2,7 miljoen voorzien vanuit het bestedingsplan 2016 bijz. bijdrage Digitalisering en Cybercrime vanuit het Ministerie V&J (De posten bestaan uit: 500.000 euro opleiding, 500.000 euro externe inhuur voor het bouwen van het lab, 200.000 euro inrichting beveiligingsmaatregelen, 1.500.000 middelen en licentiegeld.)
Het niet besteden van de gelden van de bijzondere bijdrage D&C ligt politiek bestuurlijk zeer gevoelig. Zeker nu 12-14 !
- Het doorzetten van de ontwikkeling op CCIII is van strategisch belang in relatie tot versterken opsporing in zijn algemeenheid en de ontwikkeling van Digitale opsporing in het bijzonder.

Groet,

10.2.e

10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën | 9
Nieuwe Uitleg 1, 2514 BP, Den Haag

Van: 10.2.e
Verzonden: maandag 14 maart 2016 21:46
Aan: 10.2.e 10.2.e
CC: 10.2.e Philips, Inge (I.C.); 10.2.e 10.2.e
Onderwerp: RE: Input voor KMO annotatie operationeel portfolio-CCIII

Beste 10.2.e ,

wellicht als aanvulling hierop nog de volgende punten:
Het gaat NIET alleen over cybercrcrime.
Het gaat niet allen over 7-12 het gaat ook eenheden operationeel belasten (zijn we mee bezig) en ook Partners!
12-14

Kijk maar even hoe en of dit er nog in verwerkt kan worden.

groet, 10.2.e

Van: Meij, Peije de (P.)
Verzonden: maandag 14 maart 2016 22:27
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Input voor KMO operationeel portfolio

Dag 10.2.e ,

Ik begrijp je zorgen. De voorliggende keuzes zijn inderdaad pijnlijk en niet zonder consequenties. 12-14 Ik stuur je bericht met mijn reactie naar 10.2.e en 10.2.e om te toetsen of mijn redenering klopt.

Groet, 10.2.e

Van: 10.2.e
Verzonden: Monday, March 14, 2016 11:43 PM
Aan: Meij, Peije de (P.)
Cc:10.2.e 10.2.e [KNP]
Onderwerp: RE: Input voor KMO operationeel portfolio

Hallo Peije,

Dank voor je reactie. 12-14

Probleem is:
- dat wij deze bevoegdheid als politie echt heel hard nodig hebben om cybercrime aan te kunnen pakken
- dat het wetgevingstraject al ver is gevorderd en er gepland is op in werking treding 01-01-2017. Dit is niet nieuw en steeds met ons afgestemd zodat we ons goed zouden kunnen voorbereiden voor die tijd. Het wetsvoorstel ligt al bij de TK. We hebben een ronde tafel gehad en de schriftelijke vragen zijn binnen. Zoals het er op basis daarvan uit ziet is er een kamermeerderheid. Het loopt dus volop.
- en het belangrijkste: de voorbereiding grotendeels een IV project, waarvoor IV capaciteit nodig is om dit zo in te richten dat het past bij de IV standaarden. Er zitten ook uren in het IV portfolio, maar die raken we kwijt als dit onderwerp in het operationeel portfolio wordt geschrapt. Voorbereiden en doorontwikkelen zonder IV is geen optie.
Het project komt dan stil te liggen met genoemde consequenties.

Nog even wat achtergrond om te schetsen waar het om gaat:
Er moet een nieuwe infrastructuur gebouwd worden om te kunnen binnendringen in een geautomatiseerd werk. Een nieuwe bevoegdheid waar we echt nog heel veel voor moeten doen om dit goed en zorgvuldig uit te kunnen voeren, rekening houdend met goede functiescheiding, goede logging om voor de rechter forensisch bewijs te leveren van onze acties etc.
Er is ook al geruime tijd een projectleider van de dienst ICT betrokken bij het project, want de voorbereiding is in volle gang. Het staat op het IV portfolio (wel met te weinig uren om de voortgang te maken die wenselijk is, maar er zijn uren) en er is geld beschikbaar. Als nu in het operationeel portfolio de stecker eruit wordt getrokken gaan de uren uit het portfolio naar andere activiteiten en kunnen we niet verder met voorbereiden.

12-14

Ik vind het vervelend dat ik dit aan de orde moet stellen, maar vind het wel mijn rol, want ik zie echt grote risico's en wil je waarschuwen voor de consequenties.

Groet,

10.2.e

Van: 10.2.e]
Verzonden: dinsdag 15 maart 2016 05:58
Aan: 10.2.e Meij, Peije de (P.)
CC: 10.2.e
Onderwerp: Re: Input voor KMO operationeel portfolio

Goedemorgen,

De tussentijdse balanceersessie in juli geeft hier voldoende mogelijkheden voor.

Groet,

10.2.e

From 10.2.e @politie.nl>
Subject **RE: Input voor KMO operationeel portfolio**
To 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>
Date 15 maart 2016 14:37:50 CET

Goedemiddag allen,

In een zwart-wit redenatie moet het stoppen, echter …

CCIII kunnen we scharen bij een aantal andere wetgeving waarvan de voorbereiding wel door zou moeten gaan, omdat hier een lange voorbereidingstijd aan vooraf gaat. Niet onder reikwijdte

Ik stel voor dat aan het KMT mee te geven.

10.2.e
Adviseur

Politie | Directie Operatiën

Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag
M 06 10.2.e

Werkdagen: maandag t/m donderdag

Van: 10.2.e
Verzonden: woensdag 30 maart 2016 16:31
Aan: 10.2.e 10.2.e
CC: 10.2.e
Onderwerp: CCIII vragen

Hallo collega's,

V&J gaat de binnengekomen vragen CCIII clusteren en alvast een voorzet voor beantwoording doen, waarna we over ongeveer twee weken gevraagd zullen worden hierop te reflecteren. Mogelijk weer in enkele thema sessies zoals eerder ook zijn georganiseerd. Zodra ik hierover meer hoor laat ik het weten. Mijn voorstel is dat jullie dan meekijken wie er voor welk thema aan tafel moeten zitten van 7-12 .

Groet,
10.2.e

10.2.e
Adviseur
Politie | Staf Korpsleiding | Directie Operatiën
Nieuwe Uitleg 1, 2514 BP, Den Haag
M 06 10.2.e
E 10.2.e @politie.nl
Werkdagen: ma, di, do, vrij

From: 10.2.e
Sent: Wednesday, March 30, 2016 04:32 PM W. Europe Standard Time
To: 10.2.e 10.2.e
Cc: Philips, Inge (I.C.)
Subject: RE: CCIII vragen

10.2.e dank voor het bericht, lijkt me een prima aanpak, gr 10.2.e

Van: 10.2.e
Verzonden: woensdag 30 maart 2016 16:36
Aan: 10.2.e
Onderwerp: Re: CCIII vragen

Weet jij of 11 april nog steeds het gesprek met 9 gepland staat? En of 9 al gepland is?

Met vriendelijke groet,

10.2.e

Staf Korpsleiding Politie
Directie Operatien

Verzonden vanaf mijn Blackberry

Van: 10.2.e
Verzonden: woensdag 30 maart 2016 16:44
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>
Onderwerp: RE: CCIII vragen

Ja hoor, alles is gepland voor 11 april. 10.2.e en ik zijn met een aantal medewerkers aan het voorbereiden.
9 komt ook.
We hadden het er vandaag over en volgens ons was je op de hoogte, maar zelf verhinderd(?).
Volgende week 6 april leggen we het concept-programma voor aan Inge. Het is nogal eenvoudig hoor.
In ieder geval zit er een presentatie in over het waarom van de wet en de presentatie van de kick-off over het LAB.
Die laatste zitten dan weer functiescheiding, transparantie, controle e.d. in verwerkt (de wettelijke eisen).
Inge is uiteraard de (dag)voorzitter voor de sessie.
We zenden het programma uiteraard ook gr 10.2.e naar jou.

Van: 10.2.e
Verzonden: woensdag 30 maart 2016 18:28
Aan: 10.2.e
Onderwerp: RE: CCIII vragen

Hoi,

Ik wist van 11 april, maar dacht dat het alleen een gesprek met Inge zou zijn. Niet een programma.
Zou het de bedoeling zijn dat ik aanwezig was? Ik zou wel kunnen denk ik.
Ik hoor graag het programma, dan kan ik dat aan V&J doorgeven zodat de Stas geïnformeerd kan worden.

Groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 31 maart 2016 10:26
Aan: 10.2.e
CC: 10.2.e
Onderwerp: RE: CCIII vragen

ok, dan waren wij abuis.
Je bent in ieder geval hartelijk welkom.
10.2.e zal je op de hoogte houden, het is maandagochtend 11 april alhier, maar ik weet de tijden niet precies, gr 10.2.e

From: 10.2.e @politie.nl>
Subject: **RE: CCIII vragen**
To: 10.2.e @klpd.politie.nl>, 10.2.e @politie.nl>
Date: 31 maart 2016 16:44:25 CEST

Hoi 10.2.e

van 10 tot 12 uur op 11 apirl komen Kees Verhoeven en Ockje Tellegen langs voor een werkbezoek om nader geinformeerd te worden over CCIII. Bedoeling is om ze eerst een presentatie te laten geven door 9 over het waarom van deze bevoegdheid. Schijnbaar heeft hij dat al eens eerder gedaan voor iemand van de SP en is dat goed bevallen. Daarna laten we 10.2.e de presentatie geven (iets uitgebreider) die ook tijdens de kick-off is gegeven op 2 maart. Dit om een beeld te geven over functiescheiding, logging, toezicht etc. Daarna is er nog wat ruimte om met Inge nader van gedachten te wisselen.

Je bent uiteraard van harte welkom! Kijk maar even of het past in je agenda.

Groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 7 april 2016 16:42
Aan: Plas, Theo van der (T.G.)
CC: Philips, Inge (I.C.); 10.2.e 10.2.e
Onderwerp: Werkbezoek Verhoeven en Tellegen aan CCIII
Bijlagen: Agenda Werkbezoek.doc

Beste Theo,

aanstaande maandag komen Kees Verhoeven (D66) en Ockje Tellegen (VVD) op uitnodiging van Inge en met medewerking van 10.2.e op werkbezoek bij de Landelijke Eenheid om bijgepraat te worden over CCIII. Vanuit het departement is hiervoor ook toestemming verleend.

Het werkbezoek vindt plaats van 10 tot 12 uur in zaal F1. Ik weet niet of je in de gelegendheid bent om even aan te schuiven, maar je bent uiteraard van harte welkom. Ik heb het programma voor de volledigheid even bijgevoegd.

Met vriendelijke groet,
10.2.e

10.2.e

9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg

Postbus 100, 3970 AC Driebergen-Rijsenburg

M 10.2.e

Email : 10.2.e @politie.nl

Werkdagen: maandag, dinsdag, donderdag en vrijdag

Agenda

Organisatieonderdeel Project CCIII

Behandeld door 10.2.e
E-mail 10.2.e @politie.nl

Genodigden
Dhr. K. Verhoeven (D'66), Mevr. O. Tellegen (VVD), Dhr. B. Colenbrander (D'66), Mevr. C. de Fey (D'66), Dhr. M. van Vliet (D'66), Mevr. F. Otten (VVD), Mevr. I.Philips (Politie), 10.2.e (Politie, 9), 10.2.e (Politie, Kwartiermaker CCIII), 10.2.e (Politie, 9), 10.2.e (Politie, Directie Operatiën) en 10.2.e (Politie, 9

Overleg **Werkbezoek Dhr. Verhoeven en Mevr. Tellegen CCIII**
Datum 11 april 2016
Tijdstip 10.00 - 12.00 uur
Locatie Hoofdstraat 54, Driebergen, Vergaderzaal F1

1. **Welkom door dagvoorzitter Mevr. I. Philips, plv. Hoofd Landelijke Recherche**
2. **Presentatie over nut en noodzaak CCIII**
3. **Presentatie over heimelijk binnendringen in een geautomatiseerd werk op afstand**
4. **Vragen en discussie**
5. **Sluiting**

Van: 10.2.e
Verzonden: donderdag 7 april 2016 16:56
Aan: 10.2.e 10.2.e '
CC: Philips, Inge (I.C.); 10.2.e ; 10.2.e 10.2.e 10.2.e
Onderwerp: Programma werkbezoek CCIII Maandag 11 april 2016 10 - 12 uur LE Driebergen
Bijlagen: Agenda Werkbezoek.doc

Geachte heer Colenbrander, mevrouw Otten,

bijgaand treft u aan kort programma voor het werkbezoek CCIII aanstaande maandag bij de Landelijke Eenheid.

Ik heb alle namen die ik heb ontvangen doorgegeven aan de beveiliging, zodat u zich daar kunt melden en na ontvangst van een bezoekerspas kunt doorlopen naar de vergaderzaal F1. Houdt u er rekening mee dat de procedure bij de beveiliging enige tijd in beslag kan nemen.

U zult bij de vergaderzaal worden ontvangen door mevr. Philips.

Mocht u met de auto komen houdt u er dan rekening mee dat er zeer beperkt parkeerruimte is bij de Landelijke Eenheid.

Voor vragen ben ik uiteraard bereikbaar.

Wij kijken uit naar een prettige bijeenkomst.
Met vriendelijke groet,
10.2.e

10.2.e

9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg

Postbus 100, 3970 AC Driebergen-Rijsenburg

M 06 10.2.e

Email : 10.2.e @politie.nl

Werkdagen: maandag, dinsdag, donderdag en vrijdag

Agenda

POLITIE

Organisatieonderdeel Project CCIII

Is gelijk aan doc 384

Van: 10.2.e
Verzonden: dinsdag 10 mei 2016 11:16
Aan: 10.2.e 10.2.e 10.2.e @politieacademie.nl'; 10.2.e 10.2.e
'e10.2.e @mindef.nl'; 10.2.e @mindef.nl'; '10.2.e @belastingdienst.nl'; 10.2.e
10.2.e 10.2.e 10 10.2.e ; 10.2.e 10.2.e 10.2.e
CC: 10.2.e 10.2.e
Onderwerp: Input voor beantwoording vragen CCIII

<< Bestand: Technische vragen Tweede Kamer mbt CCIII om te bespreken met experts politie en OM.docx >> <<
Bestand: Algemene en juridische en beleidsvragen CCIII.docx >>

Beste allemaal,

Vorige week heb ik van 10.2.e van het Ministerie van VenJ de lijsten met vragen ontvangen die moeten
worden beantwoord vanuit de politie voor de behandeling van de wet CCIII in de Tweede Kamer. De twee vragenlijsten voeg ik nu al ter info bij. Ik zal deze nog bewerken om een clustering aan te brengen in de vragen.

Het ministerie is van plan om twee expertsessies te beleggen om gezamenlijk met ons de antwoorden te maken op de gestelde vragen. Het gaat hier om een meer technische sessie en een meer beleidsmatige sessie. Wanneer deze sessies gaan plaatsvinden is nog niet bekend.

Aan mij is gevraagd om aan 10.2.e door te geven wie voor deze bijeenkomsten uitgenodigd moeten worden. Ik zit aan jullie te denken…

Graag hoor ik of bereid bent om mee te helpen met het beantwoorden van de vragen. Ik zal intern op korte termijn een bijeenkomst beleggen om alvast gezamenlijk de vragen te beantwoorden, zodat we een concept al de expertsessies in kunnen gaan.

Het een en ander zal waarschijnlijk op korte termijn plaats vinden. Ik weet dat de agenda's vol zitten, maar ik wil jullie toch met klem verzoeken om hiervoor tijd vrij te maken. Alleen door een goede, gezamenlijke voorbereiding kunnen we er voor zorgen dat de wet uiteindelijk door de Kamer heen komt!

Met vriendelijke groet,

10.2.e

Van: 10.2.e
Verzonden: woensdag 18 mei 2016 15:27
Aan: 10.2.e 10.2.e 10.2.e @politieacademie.nl'; 10.2.e 10.2.e
10.2.e @mindef.nl'; 10.2.e @mindef.nl'; 10.2.e @belastingdienst.nl'; 10.2.e 10.2.e
10.2.e ; 10.2.e ; 10.2.e '; 10.2.e 10.2.e 10.2.e
Dick (D.)
Onderwerp: RE: Input voor beantwoording vragen CCIII

Beste allemaal,

<< Bestand: Thematisch gebundelde Technische vragen Tweede Kamer mbt CCIII om te bespreken met experts politie en OM.docx >>

Ondertussen heb ik van het departement bericht ontvangen dat zij op 31 mei een hele dag naar Driebergen komen om met ons in gesprek te gaan over de beantwoording van de vragen. Niet iedereen hoeft er de hele dag te zijn,
maar ik hoor graag of je in de gelegenheid bent om op die dag in ieder geval een moment te vinden om mee te denken met de beantwoording van de vragen.

Ik heb ondertussen de vragen zo goed en zo kwaad als mogelijk geprobeerd te clusteren. Ik hoop dat dat helpt. Zoals afgesproken zou ik het prijs stellen indien jullie al wat voorwerk kunnen doen en mij vanuit jullie alvast wat antwoorden mijn kant op te sturen. Ik zal die dan verwerken zodat we gezamenlijk, volgende week, er nog een slag over kunnen maken.

Ik schiet voor volgende week een vergaderverzoek er in. Ik weet dat niet iedereen aanwezig zal kunnen zijn, maar
laten we proberen zoveel mogelijk op 1 lijn te zitten voor wat betreft de beantwoording van de vragen.

Met groet,
10.2.e

Vragen Tweede Kamer gecombineerd.

KWETSBAARHEDEN ALGEMEEN

(13 D66) Voornoemde leden vragen de regering die brief gelijktijdig met de nota naar aanleiding van het verslag aan de Kamer te doen toekomen.

Antwoord vanuit het MinVenJ.

(17 D66) Deze leden vragen de regering in te gaan op de tegenstrijdigheid van deze beleidskeuze om cybercriminelen te bestrijden door de kwetsbaarheden, die zij gebruiken om hun criminelen activiteiten te ontplooien, niet proberen te dichten, maar juist open te houden en zelf te misbruiken.

Kwetsbaarheden zijn er en deze worden gebruikt, niet misbruikt. De kwetsbaarheden worden niet bewust opengehouden. Het dichten van kwetsbaarheden is voor de industrie, niet voor de overheid. De maker van de software is de enige die de kwetsbaarheid kan herstellen.

(18 D66) Voorts vragen de aan het woord zijnde leden de regering in te gaan op de mogelijke situatie dat de Nederlandse regering de nu nog schimmige markt in onbekende kwetsbaarheden, zogeheten «zero days», legitimeert en stimuleert door software te kopen van bijvoorbeeld een HackingTeam. Acht de regering het mogelijk dat hackers door de legitimering van de markt in «zero days» eerder geneigd zullen zijn om «zero days» te verkopen aan HackingTeam-achtige bedrijven of overheden?

De regering doet geen zaken met criminelen. Er zullen software paketten gekocht worden van gerenommeerde partijen. Legitimering van de markt betekent niet automatisch dat het zoeken naar en verkopen van zero-days strafbaar is. Kwetsbaarheden worden niet alleen door criminelen gebruikt, maar ook voor legitieme doeleinden. Zero days zijn een kwetsbaarheid, een exploit benut deze kwetsbaarheid. Er zijn meerdere kwetsbaarheden nodig om de exploit te laten werken.

(21 D66) Hoe verhoudt het eventueel misbruiken van fouten in software zich tot de brief van 4 januari 2016 van de regering over encryptie? Is de regering van plan fouten in encryptiesoftware te misbruiken om gegevens te ontsleutelen?

De overheid is voor een sterke encryptie. Door deze sterke encryptie is er wel nadrukkelijk de behoefte om de bevoegdheid van CCIII te hebben. Door de bevoegdheden van CCIII blijft het mogelijk om bij de leesbare data komen, zo niet dan is het veelal onmogelijk om de gegevens te ontsleutelen.

(166 D66) Is de regering op de hoogte van de zogeheten ASML-hack, waar een fout in de software van een VPN-dienst leidde tot economische schade voor het bedrijf? Hoe kijkt de regering aan tegen de economische consequenties van het gebruiken in plaats van dichten van dergelijke kwetsbaarheden?

Antwoord via MinVenJ.

MELDEN EN KWETSBAARHEDEN

(56 PvdD) Met het voorliggende wetsvoorstel zouden dit soort bugs niet gemeld en oplost worden, maar juist gebruikt worden door de opsporingsdiensten. Echter, als de politie een computer kan kraken, dan kan een kwaadwillende hacker dat ook. Vindt de regering het acceptabel dat de veiligheid van miljoenen apparaten aangetast wordt, alles in dienst van de hackbevoegdheid van de politie? Kan de regering uiteenzetten welke afweging is gemaakt tussen de het belang van de veiligheid van burgers tegenover de opsporingsbehoeften van de politie? Waar is de prioriteit gelegd? Graag ontvangen zij een reactie hierop van de regering.

Als het wetsvoorstel niet wordt doorgevoerd, zullen criminelen alsnog gebruik maken van de bestaande kwetsbaarheden. Dit wetsvoorstel zorgt er slechts voor dat de overheid de criminaliteit in het digitale domein kan blijven opsporen en bestrijden. Het trekken van een verband tussen de kwetsbaarheden van software en de bevoegdheden van dit wetsvoorstel is onterecht. De kwetsbaarheden ontstaan niet door dit wetsvoorstel, die zijn er al en worden uitgebuit door criminele organisaties. De wereldwijde schade door cybercriminaliteit, waaronder economische spionage is in 2015 al beraamd op meer dan $340 miljard. Bron: Deloitte.

(193 CU) Hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd?

Het niet melden van kwetsbaarheden zal een afweging zijn in het onderzoeksbelang. Deze afweging wordt gemaakt in nauwe samenspraak tussen zowel OM als Politie. Door de veelheid van partijen werkzaam in het digitale domein zal een kwetsbaarheid veelal snel gemeld worden bij de diverse CERT organisaties. In Nederland heeft naast de diverse CERT's het NCSC deze ontvangende en coördinatie rol.

TECHNIEK EN KWETSBAARHEDEN

(71 D66) Klopt het dat DDoS-aanvallen uitgevoerd worden door gebruik te maken van Botnets, die zijn opgezet door gebruik te maken van fouten in software van computers, mobieltjes, tablets en andere apparaten? Klopt het dat de regering door middel van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruik maakt van fouten in de software? Klopt het dat de fouten in de software die gebruikt worden door de politie om een geautomatiseerd werk binnen te dringen dezelfde fouten zouden kunnen zijn als de fouten die criminelen gebruiken om Botnets op te zetten? Ziet de regering de tegenstrijdigheid van deze benadering?

Ja, DDos aanvallen kunnen gebruik maken van Botnets.

Ja, de opsporingsinstanties zouden inderdaad o.a. gebruik kunnen maken van kwetsbaarheden in software om haar bevoegdheden in te zetten.

Ja, afhankelijk van de kwetsbaarheden kunnen zowel de overheid als criminelen hier gebruik van maken zodra zij hiervan op de hoogte zijn. Niet alle kwetsbaarheden zijn geschikt om botnets op in te zetten.

Nee, er is geen tegenstrijdigheid in de benadering, criminelen maken gebruik van kwetsbaarheden die zij vinden, de opsporingsinstanties kunnen dat ook doen. Als de buitendeur van een huis

openstaat, kan iemand er langs lopen of naar binnen gaan om iets te stelen, de politie kan binnentreden door via een geopende deur te gaan of in te breken.

(72 D66) Is het niet beter om ervoor te zorgen dat fouten gedicht worden zodat het überhaupt moeilijker wordt om Botnets op te zetten? Deelt de regering de mening dat dat een grotere impact zal hebben op het aantal DDoS-aanvallen?

Ja, het is inderdaad beter om er voor te zorgen dat fouten gedicht worden.

Nee, de regering deelt deze mening niet. DDOS aanvallen kunnen onafhankelijk van kwetsbaarheden worden uitgevoerd.

TECHNIEK ALGEMEEN

(121 D66) Kan de regering toelichten wat voor soort routers zullen worden binnengedrongen? Gaat het hier vooral om thuisnetwerken of Wi-Fi-hotspots of gaat het ook om zogenaamde enterprise routers die netwerken van internetaanbieders (ISP's) met elkaar verbinden?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(122 D66) Wordt bij het binnendringen van de routers ook de software, de zogeheten firmware, aangepast? Welke software wordt er voor het binnendringen gebruikt? Wat wordt er gedaan met de datapakketjes die de router moet doorgeven? Worden er aanpassingen gedaan aan het routingprotocol? Worden de datapakketjes ingezien door middel van «deep-packet-inspection» of wordt alleen de «header» gelezen?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(139 PvdA) Zijn er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen? Zo ja, welke mogelijk- heden zijn dat? Kan de politie zelf zwakten op afstand in een systeem aanbrengen? In welke mate zijn systeemzwakten van belang voor de politie om een geautomatiseerd systeem binnen te dringen? Kunnen via het lek dat de politie zelf creëert of waar het gebruik van maakt ook anderen dat systeem binnendringen? Waarom zouden «exploits» als kwetsbaarheid wel snel opgelost kunnen worden en de andere manieren die de politie gebruikt om een systeem binnen te dringen niet onschadelijk kunnen worden gemaakt?

Met opmerkingen g]: Vraag dep wat wordt hiermee bedoeld?

Ja, er zijn andere mogelijkheden. Social engineering is daar een voorbeeld van. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

Ja, de politie kan op afstand zelf kwetsbaarheden in een systeem aanbrengen, mits er op voorhand al een initiële kwetsbaarheid aanwezig is. Het gebruik van het woord systeemzwaktes is suggestief, we hebben het hier over kwetsbaarheden in het systeem. Soms heb je kwetsbaarheden in het systeem nodig om binnen te kunnen dringen. Het is niet uitgesloten dat er ook anderen van de kwetsbaarheden gebruik kunnen maken. Zonder in te gaan op methoden en technieken zijn er ook

andere kwetsbaarheden die opgelost kunnen worden. Als hier met het oplossen van kwetsbaarheden bedoeld worden het minder kwetsbaar maken van het systeem.

De politie zal op basis van de wet bepaalde methodes toepassen en conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105.

(165 D66)Wat bedoelt de regering met verhullingstechnieken? Bedoelt de regering dat het kwetsbaarheden in bijvoorbeeld VPN-diensten wil gebruiken?

Antwoord via MinVenJ.

(182 D66) Kan de regering nader toelichting wat zij bedoelt met «zoveel mogelijk»? Is de regering van plan om bij het binnendringen van routers de firmware aan te passen? Op wat voor manier wordt de firmware aangepast bij het beëindigen van het onderzoek? Wordt in een dergelijk geval de laatste versie van de firmware geïnstalleerd, ook als dit betekent dat de politie daarna niet meer de router kan binnendringen?

De politie zal op basis van de wet bepaalde methodes toepassen en conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105.

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

Er zal continu registratie en logging worden uitgevoerd van de werkzaamheden die worden verricht. Conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105. De gehele actie is gecoördineerd, de verkenning, het binnendringen, het observeren, het exfiltreren. Hierin wordt nauw samengewerkt tussen Politie en OM. Achteraf vindt er een rechterlijke toets plaats om te bezien of werkzaamheden volgens de wet zijn uitgevoerd.

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

Met opmerkingen 9 Vraag dep om nadere toelichting

Ieder systeem dat verbonden is met het internet kan in potentie gehackt worden. De politie zal er voor zorgen dat alles in het werk wordt gesteld om niet gehackt te worden. Het "binnendringen" zal gebeuren vanuit een omgeving die niet in verbinding staat met andere politiesystemen.

(161 D66) Deze leden lezen dat in de fase van het onderzoek van het geautomatiseerd werk eventueel een technische hulpmiddel wordt geplaatst. Kan de regering aangeven in welke gevallen het niet nodig is een technisch hulpmiddel te plaatsen en toch een geautomatiseerd werk binnengedrongen kan worden?

Het is mogelijk om zonder een technisch hulpmiddel te plaatsen binnen te dringen in een geautomatiseerd werk. Iedere situatie is echter anders. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(162 D66) Kan de regering aangeven op wat voor manier, zonder de hackbevoegdheid te gebruiken, vastgesteld kan worden welke programma's zijn geïnstalleerd en welke bestandsmappen aanwezig zijn op het geautomatiseerd werk?

Twee voorbeelden zijn het in beslag nemen van een geautomatiseerd werk of social engineering. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(245 SP) Hoe weet men van tevoren waar men moet zijn? Men weet toch niet altijd waar gegevens opgeslagen staan? Wat wordt gedaan met gegevens die niet relevant zijn voor de opsporing?

Om hier achter te komen hebben de opsporingsinstanties de bevoegdheid van dit wetsvoorstel nodig. Gegevens die niet onder het bevel vallen komen niet ter beschikking van het tactisch opsporingsteam. Dit wordt door middel van functiescheiding georganiseerd.

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

Dat is aan de fabrikant van de apparatuur.

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

Dubbel.

(138 PvdA) Wat gebeurt er met verdachte informatie die al tijdens de verkennende fase in een geautomatiseerd werk gevonden wordt? Stel bijvoorbeeld dat er een map met de naam «kinderporno» gevonden wordt, hoe moet de opsporings- ambtenaar er dan in deze verkennende fase mee om gaan?

Afhankelijk van de situatie zal er worden opgetreden als bij kennisname van een misdrijf in de fysieke wereld.

(163 D66) Klopt het dat in de praktijk al in de verkennende fase routers gehackt moeten worden om al deze informatie van geautomatiseerde werken te verzamelen? Wat gebeurt er met de informatie van geautomatiseerde werken van niet-verdachten? Kan de regering aangeven welke software gebruikt wordt om de benodigde informatie te verzamelen in de verkennende fase?

Ja, dat is een mogelijkheid nadat er een bevel is gegeven. Informatie van niet-verdachten wordt afgehandeld conform functiescheiding en inhoud van het bevel. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

MELDEN

(141 PvdA) Hoe verhoudt de bevoegdheid om op afstand heimelijk een geautomatiseerd werk te onderzoeken zich tot de plicht om datalekken te melden? Is ook de politie aan die meldplicht gehouden?

De meldplicht over datalekken gaat over het verliezen van eigen informatie. De Wet datalekken is een wijziging van de WBP. Politiegegevens worden verwerkt onder de WPG en vallen derhalve niet onder deze wet. Er bestaat geen meldplicht datalekken voor hackers.

(146 SP) Betekent dit niet ook dat het van belang kan zijn voor de overheid om deze lekken niet te dichten? In hoeverre wordt een softwarefabrikant, eindgebruiker of het Nationaal Cyber Security Centrum (NCSC) op de hoogte gesteld van een kwetsbaarheid als deze is geconstateerd door opsporings- instanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan?

Kwetsbaarheden zijn er en deze worden gebruikt. De kwetsbaarheden worden niet bewust opengehouden. Het dichten van kwetsbaarheden is voor de industrie, niet voor de overheid. De maker van de software is de enige die de kwetsbaarheid kan herstellen.

(147 SP) Worden deze aan hen gemeld zodat deze kunnen worden opgelost?

Het melden van kwetsbaarheden zal een afweging zijn in het onderzoeksbelang. Deze afweging wordt gemaakt in nauwe samenspraak tussen zowel OM als Politie. Door de veelheid van partijen werkzaam in het digitale domein zal een kwetsbaarheid veelal snel gemeld worden bij de diverse CERT organisaties. In Nederland heeft naast de diverse CERT's het NCSC deze ontvangende en coördinatie rol.

(148 SP) Deze leden merken op dat de regering stelt dat de politie geen baat heeft bij instandhouding van onbeveiligde systemen vanwege de maatschappelijke kosten. Kan de regering dit nader toelichten? Kunnen politie en Openbaar Ministerie (OM) ook heimelijk binnendringen zonder gebruik te maken van «zero days»? Of zijn er per definitie kwetsbaarheden nodig?

De overheid is voorstander van veilige systemen. Er kan ook zonder zero days worden binnengedrongen, echter kwetsbaarheden zijn wel altijd nodig.

(177 D66) Klopt het dat het zeer onwaarschijnlijk is dat de politie de fouten die de aan te kopen software gebruikt om een geautomatiseerd werk binnen te dringen zal melden bij de fabrikant zodat ze gedicht kunnen worden? Dit betekent toch dat de politie een belang heeft bij de instandhouding van onveilige software? Deelt de regering de mening dat het actueel houden van programma's geen soelaas biedt tegen het gebruiken van onbekende kwetsbaarheden zoals de politie beoogt te doen?

Zie standpunt regering zero days brief. Antwoord via MinVenJ.

PRIVACY

(142 PvdA) In hoeverre kan het doel van de bescherming van de cybersecurity, daaronder de integriteit en veiligheid van het internet begrepen, botsen met het doel van het voorkomen van cybercrime waaronder het onderzoeken van geautomatiseerde werken?

Met opmerkingen Nog bespreken me departement.

Er is altijd een trade off tussen privacy en cybersecurity. Antwoord via MinVenJ.

ALGEMEEN

(169 D66) Kan de regering nader toelichten wat zij met «in beginsel» bedoelt? Bestaat de mogelijk dat de regering bedrijven zal dwingen of vragen om kwetsbaarheden in software in te bouwen?

Antwoord via MinVenJ.

(170 D66) Kan de regering bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten?

Dit kunnen wij bevestigen.

(171 D66) Hoe denkt de politie te voorkomen dat derden daar gebruik van kunnen maken en in welke mate denkt de politie daar succesvol in te kunnen zijn?

Niet van toepassing. Zie beantwoording vraag 170.

(175 D66) Voorts lezen de leden van de D66-fractie dat de politie waar mogelijk zal proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Is de regering het met de leden eens dat dit vrijwel onmogelijk is? Kan de regering concrete voorbeelden geven waarin dit wel mogelijk is?

Voorkomen dat anderen gebruik maken van kwetsbaarheden is door de politie niet te voorkomen. De praktijk zal uitwijzen in hoeverre dit mogelijk is.

(176 D66) Klopt het dat de politie afhankelijk zal zijn van zowel onbekend als bekende fouten in software?

De politie is inderdaad afhankelijk van kwetsbaarheden.

(178 D66) Deelt de regering de mening dat de politie niet zowel een belang kan hebben bij onveilige software en tegelijk een belang bij het veiliger maken van software?

Nee, deze mening delen we niet. In het kader van de functiescheiding zal er gebruik worden gemaakt van kwetsbaarheden door bevoegd personeel.

(250 D66) Indien de regering niet kan uitsluiten dat door het gebruik van technische kwetsbaarheden de achterdeur ook open komt te staan voor kwaadwillende derden die dezelfde achterdeur willen gebruiken, hoe meent zij dan dat de burger kan vertrouwen op de integriteit van een computersysteem?

De integriteit van een computersysteem kan door de overheid niet worden gegarandeerd.

(29 SP) De aan het woord zijnde leden vragen of het klopt dat het op dit moment niet mogelijk is gegevens te achterhalen die zijn opgeslagen in de Cloud. Kunnen praktijkvoorbeelden gegeven worden van opsporingsonderzoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen?

In sommige gevallen is dit wel mogelijk, met name als de cloudomgeving zich in NL bevindt. Er zijn tal van voorbeelden waarin de cloudprovider niet wenste mee te werken aan een bevoegd gegeven bevel in NL.(Voorbeeld via THTC?)

(292 SP) Ook willen de leden van de SP-fractie weten hoe wordt gecontroleerd of de software buiten de grenzen van de bevoegdheid kan worden ingezet, zoals Bits of Freedom opmerkt. Wat zijn de ervaringen van de Duitse autoriteiten hiermee, maar ook waar het gaat om aanvallen van derden?

Met opmerkingen g Antwoord via departement.

De inzet van de bevoegdheid wordt uitvoerig vooraf en achteraf getoetst. Logging en auditing van de gebruikte middelen vindt continu plaats. Door de functiescheiding zijn er maar weinig personen die toegang hebben. De opsporingsinstanties zullen altijd volgens protocollen werken.

***(D66)* Ook stelt de regering dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden. Kan de regering deze techniek nader toelichten?**

Antwoord via MinVenJ. Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(164 D66) Voorts stelt de regering dat er informatie verzameld wordt uit open bronnen. Kan de regering aangeven welke open bronnen bedoeld worden? Welke bijzondere opsporingsbevoegdheden kunnen ingezet worden om inloggegevens te achterhalen?

Informatie wordt inderdaad verzameld uit open bronnen zoals gedefinieerd in het cybercrimeverdrag artikel 32. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

PROPORTIONALITEIT

(172 D66) Hoe beschouwt de regering in dat licht de proportionaliteit van haar voorstel om gebruik te gaan maken van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten?

De bevoegdheid zal altijd proportioneel gebruikt worden. Misbruik door derden is inderdaad nooit uit te sluiten. Bij bepaalde categorieën systemen en verdachten zullen technische kwetsbaarheden de enige mogelijkheid blijken te zijn om binnen te dringen.

(1 SP) De vraag is in hoeverre de nieuwe bevoegdheid om heimelijk een geautomatiseerd werk binnen te dringen in het leven wordt geroepen omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is of omdat er echt misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid. Zo ja, is ook onderzocht of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is? Graag ontvangen deze leden een uitgebreide toelichting hierop.

Er blijven inderdaad misdrijven onopgelost door het ontbreken van deze bevoegdheid. De steeds verdergaande digitalisering geven criminelen in toenemende mate mogelijkheden om zich te onttrekken aan de traditionele opsporingsmethoden. Als voorbeeld kan genoemd worden dat de communicatie tussen criminelen onderling is in toenemende mate niet meer inzichtelijk. Er is nog geen onderzoek gedaan naar mogelijkheden waar de privacy beter gewaarborgd is.

(23 PvdA) Zo vragen de leden van de PvdA-fractie in hoeverre bij het gebruik van de nieuwe bevoegdheid niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben. Hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn?

De bestaande bevoegdheden zijn vaak makkelijker in te zetten dan het binnendringen. Daarbij wordt iedere inzet getoetst waarbij voor het meest geschikte middel gekozen wordt rekening houden met subsidiariteit en proportionaliteit.

(24 PvdA) Hoe wordt gewaarborgd dat de bevoegdheid tot het doen van het op afstand en heimelijk onderzoeken in een geautomatiseerd werk het ultimum remedium is in de reeks van bestaande bevoegdheden? Maakt de rechter-commissaris hierin een afweging? Waarom is het «niet uitge- sloten» dat er in plaats van het op afstand heimelijk binnendringen in een geautomatiseerd werk gekozen wordt voor een van de andere opsporings- bevoegdheden? Waarom wordt niet standaard eerst uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie?

Zie bovenstaand antwoord. Antwoord via MinVenJ.

(32 SP) Deze leden begrijpen dat inmiddels ook gebruik wordt gemaakt van internettaps, waardoor communicatiegegevens, die via internet gedeeld worden, afgetapt kunnen worden. Waarom is deze mogelijkheid blijkbaar onvoldoende zodat opsporingsambtenaren de bevoegdheid krijgen op afstand te kunnen hacken? Om welke opsporingsambtenaren gaat het en in welke situaties is het noodzakelijk?

Zie hiervoor het WODC rapport "het gebruik van de telefoon- en internettap in de opsporing" uit 2012. Data is tegenwoordig veelal geencrypt en veelal wordt gebruik gemaakt van verschillende communicatie kanalen die niet onder de tap staan.

NUT EN NOODZAAK

(34 D66) Kan de regering ingaan op de noodzaak en naast enkele concrete gevallen ook een meer overstijgende algemene noodzaak formuleren voor de toevoeging van deze bevoegdheid? Kan het ook op een andere minder ingrijpende wijze plaatsvinden?

Er is een groep criminelen en systemen waar de opsporing met behulp van traditionele opsporingsmethoden geen vat op kan krijgen. Het is een extra tool in de toolbox van de Politie. Waarmee het spectrum van tools wordt uitgebreid en waardoor de Politie voor sommige zaken een meer passende tool heeft.

(43 D66) Voorts vragen de leden van de D66-fractie de regering in te gaan op de voordelen van ICT-technologieën die het voor de politie de afgelopen jaren juist makkelijker hebben gemaakt om criminelen op te pakken, zoals beter beschikbare informatie via telefoons en iPads, het gebruik van drones, «gunshot-detection-systems», het monitoren van tweets en andere social media, het voorspellen van misdaad op basis van «big-data» of GPS-systemen. Kan de regering toelichten in hoeverre de technologische ontwikkelingen het werk van de politie de afgelopen jaren per saldo makkelijker of moeilijker hebben gemaakt? Kan de regering haar antwoord met statistieken onderbouwen?

Zie hiervoor het onlangs verschenen rapport over de kwaliteit van de recherche. Dit maakt duidelijk welke positie de politie op dit moment inneemt in het digitale domein.

(45 D66) Kan de regering toelichten hoe de reeds bestaande mogelijkheden een verdere uitbreiding van de bevoegdheid tot het heimelijk toegang verschaffen noodzakelijk maakt zoals het wetsvoorstel pretendeert? In hoeverre kan hier louter worden volstaan met het toevoegen van enkele strikte waarborgen voor toepassing in plaats van nog verder uitbreiden van de bevoegdheden?

De wereld verandert / digitaliseert, dan moet de opsporing mee veranderen. Het internet is ook niet meer te doorzoeken met slim googlen, de hoeveelheid data is te groot, slimme software is noodzakelijk. Bij een DDos aanval zullen we geen vingerafdrukken of voetsporen meer vinden. Nieuwe criminaliteit vraagt om nieuwe criminaliteitsbestrijding (zie 34 D66)

(60 PvdD) Deze leden zetten vraagtekens bij de bredere inzet van het wetsvoorstel als efficiencymiddel. Wat is de implicatie van de financiële paragraaf, waarin staat dat er kosten kunnen worden bespaard met de inzet van de bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen? Is het uitgesloten dat de hackbevoegdheid ook in andere domeinen kan worden toegepast? Deelt de regering de mening dat efficiency nooit een drijfveer zou mogen zijn als het gaat om de veiligheid, de grondrechten en de privacy van burgers?

Antwoord via MinVenJ.

(167 D66) Kan de regering nader toelichten waarom hacken via «socialengineering» of «phishing» niet voldoende is om de problemen geschetst in het hoofdstuk over de noodzaak van dit wetsvoorstel te overkomen?

De politie wil gebruik maken van alle potentiële kwetsbaarheden en zich dus niet laten beperken tot social engineering of phishing. Als de crimineel erg cyberbewust is, zal hij niet te engineeren of phishen zijn.

46 D66) De aan het woord zijnde leden vragen waaruit blijkt dat de bestaande bevoegdheden in toenemende mate te kort schieten. Welke wezenlijke problemen en gebleken knelpunten zijn er?

Er is een groep criminelen en systemen waar de opsporing met behulp van traditionele opsporingsmethoden geen vat op kan krijgen. Het is een extra tool in de toolbox van de Politie. Waarmee het spectrum van tools wordt uitgebreid en waardoor de Politie voor sommige zaken een meer passende tool heeft.

TECHNIEK EN TOETSING

(27 SP) De aan het woord zijnde leden vragen hoe men weet waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig zijn. Hoe groot is het risico dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing? Hoe wordt dit risico zoveel mogelijk weggenomen? Er kunnen bijvoorbeeld ongelooflijk veel gegevens verzameld worden bij toegang tot bijvoorbeeld de Cloud. Hiervoor zijn waarborgen ingebouwd, zoals toetsing door de rechter- commissaris naar de proportionaliteit, maar hoe wordt voorkomen dat ongericht gegevens wordt verzameld? Men weet immers niet altijd van tevoren waar welke gegevens vandaan gehaald moeten worden en welke gegevens nodig zijn. Hoe ziet de regering dit praktisch voor zich? De leden van de SP-fractie begrijpen, zoals de regering stelt, dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn. Soms is het werk waar de gegevens op staan niet bekend en is het tijdrovend en privacy schendend om deze te achterhalen. Betekent dit dat het plaatsen van software niet altijd mogelijk is?

Zie hiervoor het antwoord op eerdere vragen.

(154 CDA) Immers, hoe kan van tevoren worden vastgesteld wel programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturings- systeem is, wie er allemaal gebruik van maakt, etc.? Zijn dit niet juist allemaal onderdelen die door toepassing van de bevoegdheid inzichtelijk moeten worden voor politie en justitie?

Sommige informatie is vooraf te verkrijgen andere is pas na binnentreden beschikbaar. Er wordt op slimme manieren met behulp van diverse technieken gezocht naar belastende informatie.

TOETSING

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

GEHEIMHOUDERS

(31 SP) De leden van de SP-fractie merken op dat er een verplichting komt tot vernietiging van de gegevens die onder het geheimhoudingsplicht vallen. Maar wie bepaalt welke gegevens om die redenen kunnen worden vernietigd en om welke gegevens het gaat? Bovendien zijn de gegevens op dat moment reeds ingezien. Hoe wordt daarmee omgegaan? Heeft de betreffende opsporingsambtenaar dan een afgeleide geheimhoudingsplicht?

Het tactisch opsporingsteam zal gegevens die onder de geheimhoudingsplicht nooit onder ogen krijgen door de door de functiescheiding tussen het tactische en technische team. Het technisch team krijgt als eerste de informatie onder ogen, die wist de gegevens (alles op gelogde wijze) voordat iemand die zou kunnen acteren op de informatie ergens van weet.

(67 CDA) Met betrekking tot dit besluit vragen zij of wordt gecontroleerd of door advocaten opgegeven nummers inderdaad nummers van advocaten betreffen en niet een dekmantel vormen

voor contact met andere personen. Zo nee, waarom niet? Hoe kan gegarandeerd worden dat het verschoningsrecht op dit punt niet wordt misbruikt?

Dat heet niets met deze wet te maken. Antwoord via MinVenJ.

(73 D66) Kan de regering toelichten hoe dit in de praktijk werkt? Stel dat er een «keylogger» wordt geïnstalleerd op een smartphone. Hoe wordt in dat geval de «logging» stil gezet zodra de verdachte een whatsapp bericht verstuurd naar zijn advocaat? Kan de regering toelichten hoe omgegaan wordt met een concept e-mailbericht van een verdachte aan een advocaat?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

FUNCTIESCHEIDING

(77 D66) Kan de regering in dit kader toelichten waar precies de overgang ligt tussen technisch optreden en tactisch optreden ten aanzien van geautomatiseerde werken?

Zodra er een bevel is afgegeven door de OvJ en RC om binnen te dringen gaat het technisch team aan het werk. De werkzaamheden van het technisch team zijn afhankelijk van de vraag vanuit het tactisch opsporingsteam. De beide teams werken onafhankelijk van elkaar. Waar de precieze overgang ligt tussen de beide teams is een onderdeel van het werkproces.

(116 CDA) Tegelijkertijd vragen zij of de regering de mening deelt dat in de praktijk juist van belang is dat deze teams goed met elkaar communiceren en geen verdere belemmeringen op dit punt worden opgelegd, ook niet in lagere regelgeving.

Communicatie is altijd een belangrijk onderdeel van een opsporingsonderzoek. Het is wel zaak om alleen te communiceren over die onderwerpen die een goede uitvoering van het onderzoek niet in de weg staan.

Van: 10.2.e
Verzonden: woensdag 25 mei 2016 11:33
Aan: 10.2.e .); 10.2.e 10.2.e @politieacademie.nl';
10.2.e 10.2.e 10.2.e @mindef.nl';
10.2.e @mindef.nl'; 10.2.e @belastingdienst.nl'; 10.2.e
10.2.e 10.2.e 10.2.e 10.2.e
10.2.e 10.2.e 10.2.e 10.2.e
CC: 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: Antwoorden nav bijeenkomst 24 mei tbv bespreking departement 31 mei

Beste allemaal,

Gistermiddag hebben we een goede bijeenkomst gehad waarin we zo goed als alle vragen hebben weten te behandelen. Dank voor jullie input!

Ik heb dit alles nu verwerkt in bijgevoegd document. Willen jullie er nog een keer doorheen lopen en kijken of alles in lijn is met hetgeen we gisteren hebben besproken.
10.2.e en 10.2.e zijn bezig met een algemeen verhaal. Dit wil ik hier bijvoegen en dan als 1 geheel ter voorbereiding op 31 mei rondsturen naar iedereen (incl. departement). Hopelijk geeft dat dan wat richting aan het overleg.

Indien mogelijk ontvang ik graag jullie opmerkingen uiterlijk morgen, zodat ik het morgenavond kan verzenden. Ik ben zelf namelijk vrijdag en maandag niet aanwezig helaas.

Nogmaals dank voor het goede en vele werk dat al verzet is.

Met vriendelijke groet,
10.2.e

Vragen Tweede Kamer gecombineerd.

KWETSBAARHEDEN ALGEMEEN

(13 D66) Voornoemde leden vragen de regering die brief gelijktijdig met de nota naar aanleiding van het verslag aan de Kamer te doen toekomen.

Antwoord vanuit het MinVenJ.

(17 D66) Deze leden vragen de regering in te gaan op de tegenstrijdigheid van deze beleidskeuze om cybercriminelen te bestrijden door de kwetsbaarheden, die zij gebruiken om hun criminelen activiteiten te ontplooien, niet proberen te dichten, maar juist open te houden en zelf te misbruiken.

Kwetsbaarheden zijn er en deze worden gebruikt, niet misbruikt. De kwetsbaarheden worden niet bewust opengehouden. Het dichten van kwetsbaarheden is voor de industrie, niet voor de overheid. De maker van de software is de enige die de kwetsbaarheid kan herstellen.

(18 D66) Voorts vragen de aan het woord zijnde leden de regering in te gaan op de mogelijke situatie dat de Nederlandse regering de nu nog schimmige markt in onbekende kwetsbaarheden, zogeheten «zero days», legitimeert en stimuleert door software te kopen van bijvoorbeeld een HackingTeam. Acht de regering het mogelijk dat hackers door de legitimering van de markt in «zero days» eerder geneigd zullen zijn om «zero days» te verkopen aan HackingTeam-achtige bedrijven of overheden?

De regering doet geen zaken met criminelen. Er zullen software paketten gekocht worden van gerenommeerde partijen. Legitimering van de markt betekent niet automatisch dat het zoeken naar en verkopen van zero-days strafbaar is. Kwetsbaarheden worden niet alleen door criminelen gebruikt, maar ook voor legitieme doeleinden. Zero days zijn een kwetsbaarheid, een exploit benut deze kwetsbaarheid. Er zijn meerdere kwetsbaarheden nodig om de exploit te laten werken.

(21 D66) Hoe verhoudt het eventueel misbruiken van fouten in software zich tot de brief van 4 januari 2016 van de regering over encryptie? Is de regering van plan fouten in encryptiesoftware te misbruiken om gegevens te ontsleutelen?

De overheid is voor een sterke encryptie. Door deze sterke encryptie is er wel nadrukkelijk de behoefte om de bevoegdheid van CCIII te hebben. Door de bevoegdheden van CCIII blijft het mogelijk om bij de leesbare data komen, zo niet dan is het veelal onmogelijk om de gegevens te ontsleutelen.

(166 D66) Is de regering op de hoogte van de zogeheten ASML-hack, waar een fout in de software van een VPN-dienst leidde tot economische schade voor het bedrijf? Hoe kijkt de regering aan tegen de economische consequenties van het gebruiken in plaats van dichten van dergelijke kwetsbaarheden?

Antwoord via MinVenJ.

MELDEN EN KWETSBAARHEDEN

(56 PvdD) Met het voorliggende wetsvoorstel zouden dit soort bugs niet gemeld en oplost worden, maar juist gebruikt worden door de opsporingsdiensten. Echter, als de politie een computer kan kraken, dan kan een kwaadwillende hacker dat ook. Vindt de regering het acceptabel dat de veiligheid van miljoenen apparaten aangetast wordt, alles in dienst van de hackbevoegdheid van de politie? Kan de regering uiteenzetten welke afweging is gemaakt tussen de het belang van de veiligheid van burgers tegenover de opsporingsbehoeften van de politie? Waar is de prioriteit gelegd? Graag ontvangen zij een reactie hierop van de regering.

Als het wetsvoorstel niet wordt doorgevoerd, zullen criminelen alsnog gebruik maken van de bestaande kwetsbaarheden. Dit wetsvoorstel zorgt er slechts voor dat de overheid de criminaliteit in het digitale domein kan blijven opsporen en bestrijden. Het trekken van een verband tussen de kwetsbaarheden van software en de bevoegdheden van dit wetsvoorstel is onterecht. De kwetsbaarheden ontstaan niet door dit wetsvoorstel, die zijn er al en worden uitgebuit door criminele organisaties. De wereldwijde schade door cybercriminaliteit, waaronder economische spionage is in 2015 al beraamd op meer dan $340 miljard. Bron: Deloitte.

(193 CU) Hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd?

Het niet melden van kwetsbaarheden zal een afweging zijn in het onderzoeksbelang. Deze afweging wordt gemaakt in nauwe samenspraak tussen zowel OM als Politie. Door de veelheid van partijen werkzaam in het digitale domein zal een kwetsbaarheid veelal snel gemeld worden bij de diverse CERT organisaties. In Nederland heeft naast de diverse CERT's het NCSC deze ontvangende en coördinatie rol.

TECHNIEK EN KWETSBAARHEDEN

(71 D66) Klopt het dat DDoS-aanvallen uitgevoerd worden door gebruik te maken van Botnets, die zijn opgezet door gebruik te maken van fouten in software van computers, mobieltjes, tablets en andere apparaten? Klopt het dat de regering door middel van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruik maakt van fouten in de software? Klopt het dat de fouten in de software die gebruikt worden door de politie om een geautomatiseerd werk binnen te dringen dezelfde fouten zouden kunnen zijn als de fouten die criminelen gebruiken om Botnets op te zetten? Ziet de regering de tegenstrijdigheid van deze benadering?

Ja, DDos aanvallen kunnen gebruik maken van Botnets.

Ja, de opsporingsinstanties zouden inderdaad o.a. gebruik kunnen maken van kwetsbaarheden in software om haar bevoegdheden in te zetten.

Ja, afhankelijk van de kwetsbaarheden kunnen zowel de overheid als criminelen hier gebruik van maken zodra zij hiervan op de hoogte zijn. Niet alle kwetsbaarheden zijn geschikt om botnets op in te zetten.

Nee, er is geen tegenstrijdigheid in de benadering, criminelen maken gebruik van kwetsbaarheden die zij vinden, de opsporingsinstanties kunnen dat ook doen. Als de buitendeur van een huis

openstaat, kan iemand er langs lopen of naar binnen gaan om iets te stelen, de politie kan binnentreden door via een geopende deur te gaan of in te breken.

(72 D66) Is het niet beter om ervoor te zorgen dat fouten gedicht worden zodat het überhaupt moeilijker wordt om Botnets op te zetten? Deelt de regering de mening dat dat een grotere impact zal hebben op het aantal DDoS-aanvallen?

Ja, het is inderdaad beter om er voor te zorgen dat fouten gedicht worden.

Nee, de regering deelt deze mening niet. DDOS aanvallen kunnen onafhankelijk van kwetsbaarheden worden uitgevoerd.

TECHNIEK ALGEMEEN

(121 D66) Kan de regering toelichten wat voor soort routers zullen worden binnengedrongen? Gaat het hier vooral om thuisnetwerken of Wi-Fi-hotspots of gaat het ook om zogenaamde enterprise routers die netwerken van internetaanbieders (ISP's) met elkaar verbinden?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(122 D66) Wordt bij het binnendringen van de routers ook de software, de zogeheten firmware, aangepast? Welke software wordt er voor het binnendringen gebruikt? Wat wordt er gedaan met de datapakketjes die de router moet doorgeven? Worden er aanpassingen gedaan aan het routingprotocol? Worden de datapakketjes ingezien door middel van «deep-packet-inspection» of wordt alleen de «header» gelezen?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(139 PvdA) Zijn er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen? Zo ja, welke mogelijk- heden zijn dat? Kan de politie zelf zwakten op afstand in een systeem aanbrengen? In welke mate zijn systeemzwakten van belang voor de politie om een geautomatiseerd systeem binnen te dringen? Kunnen via het lek dat de politie zelf creëert of waar het gebruik van maakt ook anderen dat systeem binnendringen? Waarom zouden «exploits» als kwetsbaarheid wel snel opgelost kunnen worden en de andere manieren die de politie gebruikt om een systeem binnen te dringen niet onschadelijk kunnen worden gemaakt?

Met opmerkingen9 Vraag dep wat wordt hiermee bedoeld?

Ja, er zijn andere mogelijkheden. Social engineering is daar een voorbeeld van. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

Ja, de politie kan op afstand zelf kwetsbaarheden in een systeem aanbrengen, mits er op voorhand al een initiële kwetsbaarheid aanwezig is. Het gebruik van het woord systeemzwaktes is suggestief, we hebben het hier over kwetsbaarheden in het systeem. Soms heb je kwetsbaarheden in het systeem nodig om binnen te kunnen dringen. Het is niet uitgesloten dat er ook anderen van de kwetsbaarheden gebruik kunnen maken. Zonder in te gaan op methoden en technieken zijn er ook

andere kwetsbaarheden die opgelost kunnen worden. Als hier met het oplossen van kwetsbaarheden bedoeld worden het minder kwetsbaar maken van het systeem.

De politie zal op basis van de wet bepaalde methodes toepassen en conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105.

(165 D66)Wat bedoelt de regering met verhullingstechnieken? Bedoelt de regering dat het kwetsbaarheden in bijvoorbeeld VPN-diensten wil gebruiken?

Antwoord via MinVenJ.

(182 D66) Kan de regering nader toelichting wat zij bedoelt met «zoveel mogelijk»? Is de regering van plan om bij het binnendringen van routers de firmware aan te passen? Op wat voor manier wordt de firmware aangepast bij het beëindigen van het onderzoek? Wordt in een dergelijk geval de laatste versie van de firmware geïnstalleerd, ook als dit betekent dat de politie daarna niet meer de router kan binnendringen?

De politie zal op basis van de wet bepaalde methodes toepassen en conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105.

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

Er zal continu registratie en logging worden uitgevoerd van de werkzaamheden die worden verricht. Conform de wet zal het systeem zo veel mogelijk in de oorspronkelijke staat worden achtergelaten. Dit alles conform hetgeen is opgenomen in de Memorie van Toelichting op pagina 105. De gehele actie is gecoördineerd, de verkenning, het binnendringen, het observeren, het exfiltreren. Hierin wordt nauw samengewerkt tussen Politie en OM. Achteraf vindt er een rechterlijke toets plaats om te bezien of werkzaamheden volgens de wet zijn uitgevoerd.

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

Met opmerkingen 9 : Vraag dep om nadere toelichting

Ieder systeem dat verbonden is met het internet kan in potentie gehackt worden. De politie zal er voor zorgen dat alles in het werk wordt gesteld om niet gehackt te worden. Het "binnendringen" zal gebeuren vanuit een omgeving die niet in verbinding staat met andere politiesystemen.

(161 D66) Deze leden lezen dat in de fase van het onderzoek van het geautomatiseerd werk eventueel een technische hulpmiddel wordt geplaatst. Kan de regering aangeven in welke gevallen het niet nodig is een technisch hulpmiddel te plaatsen en toch een geautomatiseerd werk binnengedrongen kan worden?

Het is mogelijk om zonder een technisch hulpmiddel te plaatsen binnen te dringen in een geautomatiseerd werk. Iedere situatie is echter anders. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(162 D66) Kan de regering aangeven op wat voor manier, zonder de hackbevoegdheid te gebruiken, vastgesteld kan worden welke programma's zijn geïnstalleerd en welke bestandsmappen aanwezig zijn op het geautomatiseerd werk?

Twee voorbeelden zijn het in beslag nemen van een geautomatiseerd werk of social engineering. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(245 SP) Hoe weet men van tevoren waar men moet zijn? Men weet toch niet altijd waar gegevens opgeslagen staan? Wat wordt gedaan met gegevens die niet relevant zijn voor de opsporing?

Om hier achter te komen hebben de opsporingsinstanties de bevoegdheid van dit wetsvoorstel nodig. Gegevens die niet onder het bevel vallen komen niet ter beschikking van het tactisch opsporingsteam. Dit wordt door middel van functiescheiding georganiseerd.

(101 CDA) Hoe kan technisch worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software- applicaties op zijn smartphone worden geïnstalleerd?

Dat is aan de fabrikant van de apparatuur.

(189 D66) Op wat voor manier gaat de politie ervoor zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt? Kan de regering uitsluiten dat het bij verlies van controle van de server IP-«hijacking»-technieken moet toepassen om de controle terug te krijgen?

Dubbel.

(138 PvdA) Wat gebeurt er met verdachte informatie die al tijdens de verkennende fase in een geautomatiseerd werk gevonden wordt? Stel bijvoorbeeld dat er een map met de naam «kinderporno» gevonden wordt, hoe moet de opsporings- ambtenaar er dan in deze verkennende fase mee om gaan?

Afhankelijk van de situatie zal er worden opgetreden als bij kennisname van een misdrijf in de fysieke wereld.

(163 D66) Klopt het dat in de praktijk al in de verkennende fase routers gehackt moeten worden om al deze informatie van geautomatiseerde werken te verzamelen? Wat gebeurt er met de informatie van geautomatiseerde werken van niet-verdachten? Kan de regering aangeven welke software gebruikt wordt om de benodigde informatie te verzamelen in de verkennende fase?

Ja, dat is een mogelijkheid nadat er een bevel is gegeven. Informatie van niet-verdachten wordt afgehandeld conform functiescheiding en inhoud van het bevel. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

MELDEN

(141 PvdA) Hoe verhoudt de bevoegdheid om op afstand heimelijk een geautomatiseerd werk te onderzoeken zich tot de plicht om datalekken te melden? Is ook de politie aan die meldplicht gehouden?

De meldplicht over datalekken gaat over het verliezen van eigen informatie. De Wet datalekken is een wijziging van de WBP. Politiegegevens worden verwerkt onder de WPG en vallen derhalve niet onder deze wet. Er bestaat geen meldplicht datalekken voor hackers.

(146 SP) Betekent dit niet ook dat het van belang kan zijn voor de overheid om deze lekken niet te dichten? In hoeverre wordt een softwarefabrikant, eindgebruiker of het Nationaal Cyber Security Centrum (NCSC) op de hoogte gesteld van een kwetsbaarheid als deze is geconstateerd door opsporings- instanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan?

Kwetsbaarheden zijn er en deze worden gebruikt. De kwetsbaarheden worden niet bewust opengehouden. Het dichten van kwetsbaarheden is voor de industrie, niet voor de overheid. De maker van de software is de enige die de kwetsbaarheid kan herstellen.

(147 SP) Worden deze aan hen gemeld zodat deze kunnen worden opgelost?

Het melden van kwetsbaarheden zal een afweging zijn in het onderzoeksbelang. Deze afweging wordt gemaakt in nauwe samenspraak tussen zowel OM als Politie. Door de veelheid van partijen werkzaam in het digitale domein zal een kwetsbaarheid veelal snel gemeld worden bij de diverse CERT organisaties. In Nederland heeft naast de diverse CERT's het NCSC deze ontvangende en coördinatie rol.

(148 SP) Deze leden merken op dat de regering stelt dat de politie geen baat heeft bij instandhouding van onbeveiligde systemen vanwege de maatschappelijke kosten. Kan de regering dit nader toelichten? Kunnen politie en Openbaar Ministerie (OM) ook heimelijk binnendringen zonder gebruik te maken van «zero days»? Of zijn er per definitie kwetsbaarheden nodig?

De overheid is voorstander van veilige systemen. Er kan ook zonder zero days worden binnengedrongen, echter kwetsbaarheden zijn wel altijd nodig.

(177 D66) Klopt het dat het zeer onwaarschijnlijk is dat de politie de fouten die de aan te kopen software gebruikt om een geautomatiseerd werk binnen te dringen zal melden bij de fabrikant zodat ze gedicht kunnen worden? Dit betekent toch dat de politie een belang heeft bij de instandhouding van onveilige software? Deelt de regering de mening dat het actueel houden van programma's geen soelaas biedt tegen het gebruiken van onbekende kwetsbaarheden zoals de politie beoogt te doen?

Zie standpunt regering zero days brief. Antwoord via MinVenJ.

PRIVACY

(142 PvdA) In hoeverre kan het doel van de bescherming van de cybersecurity, daaronder de integriteit en veiligheid van het internet begrepen, botsen met het doel van het voorkomen van cybercrime waaronder het onderzoeken van geautomatiseerde werken?

Met opmerkingen Nog bespreken me departement.

Er is altijd een trade off tussen privacy en cybersecurity. Antwoord via MinVenJ.

ALGEMEEN

(169 D66) Kan de regering nader toelichten wat zij met «in beginsel» bedoelt? Bestaat de mogelijk dat de regering bedrijven zal dwingen of vragen om kwetsbaarheden in software in te bouwen?

Antwoord via MinVenJ.

(170 D66) Kan de regering bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten?

Dit kunnen wij bevestigen.

(171 D66) Hoe denkt de politie te voorkomen dat derden daar gebruik van kunnen maken en in welke mate denkt de politie daar succesvol in te kunnen zijn?

Niet van toepassing. Zie beantwoording vraag 170.

(175 D66) Voorts lezen de leden van de D66-fractie dat de politie waar mogelijk zal proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Is de regering het met de leden eens dat dit vrijwel onmogelijk is? Kan de regering concrete voorbeelden geven waarin dit wel mogelijk is?

Voorkomen dat anderen gebruik maken van kwetsbaarheden is door de politie niet te voorkomen. De praktijk zal uitwijzen in hoeverre dit mogelijk is.

(176 D66) Klopt het dat de politie afhankelijk zal zijn van zowel onbekend als bekende fouten in software?

De politie is inderdaad afhankelijk van kwetsbaarheden.

(178 D66) Deelt de regering de mening dat de politie niet zowel een belang kan hebben bij onveilige software en tegelijk een belang bij het veiliger maken van software?

Nee, deze mening delen we niet. In het kader van de functiescheiding zal er gebruik worden gemaakt van kwetsbaarheden door bevoegd personeel.

(250 D66) Indien de regering niet kan uitsluiten dat door het gebruik van technische kwetsbaarheden de achterdeur ook open komt te staan voor kwaadwillende derden die dezelfde achterdeur willen gebruiken, hoe meent zij dan dat de burger kan vertrouwen op de integriteit van een computersysteem?

De integriteit van een computersysteem kan door de overheid niet worden gegarandeerd.

(29 SP) De aan het woord zijnde leden vragen of het klopt dat het op dit moment niet mogelijk is gegevens te achterhalen die zijn opgeslagen in de Cloud. Kunnen praktijkvoorbeelden gegeven worden van opsporingsonderzoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen?

In sommige gevallen is dit wel mogelijk, met name als de cloudomgeving zich in NL bevindt. Er zijn tal van voorbeelden waarin de cloudprovider niet wenste mee te werken aan een bevoegd gegeven bevel in NL.(Voorbeeld via THTC?)

(292 SP) Ook willen de leden van de SP-fractie weten hoe wordt gecontroleerd of de software buiten de grenzen van de bevoegdheid kan worden ingezet, zoals Bits of Freedom opmerkt. Wat zijn de ervaringen van de Duitse autoriteiten hiermee, maar ook waar het gaat om aanvallen van derden?

Met opmerkingen g Antwoord via departement.

De inzet van de bevoegdheid wordt uitvoerig vooraf en achteraf getoetst. Logging en auditing van de gebruikte middelen vindt continu plaats. Door de functiescheiding zijn er maar weinig personen die toegang hebben. De opsporingsinstanties zullen altijd volgens protocollen werken.

***(D66)* Ook stelt de regering dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden. Kan de regering deze techniek nader toelichten?**

Antwoord via MinVenJ. Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

(164 D66) Voorts stelt de regering dat er informatie verzameld wordt uit open bronnen. Kan de regering aangeven welke open bronnen bedoeld worden? Welke bijzondere opsporingsbevoegdheden kunnen ingezet worden om inloggegevens te achterhalen?

Informatie wordt inderdaad verzameld uit open bronnen zoals gedefinieerd in het cybercrimeverdrag artikel 32. Verder worden er geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

PROPORTIONALITEIT

(172 D66) Hoe beschouwt de regering in dat licht de proportionaliteit van haar voorstel om gebruik te gaan maken van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten?

De bevoegdheid zal altijd proportioneel gebruikt worden. Misbruik door derden is inderdaad nooit uit te sluiten. Bij bepaalde categorieën systemen en verdachten zullen technische kwetsbaarheden de enige mogelijkheid blijken te zijn om binnen te dringen.

(1 SP) De vraag is in hoeverre de nieuwe bevoegdheid om heimelijk een geautomatiseerd werk binnen te dringen in het leven wordt geroepen omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is of omdat er echt misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid. Zo ja, is ook onderzocht of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is? Graag ontvangen deze leden een uitgebreide toelichting hierop.

Er blijven inderdaad misdrijven onopgelost door het ontbreken van deze bevoegdheid. De steeds verdergaande digitalisering geven criminelen in toenemende mate mogelijkheden om zich te onttrekken aan de traditionele opsporingsmethoden. Als voorbeeld kan genoemd worden dat de communicatie tussen criminelen onderling is in toenemende mate niet meer inzichtelijk. Er is nog geen onderzoek gedaan naar mogelijkheden waar de privacy beter gewaarborgd is.

(23 PvdA) Zo vragen de leden van de PvdA-fractie in hoeverre bij het gebruik van de nieuwe bevoegdheid niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben. Hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn?

De bestaande bevoegdheden zijn vaak makkelijker in te zetten dan het binnendringen. Daarbij wordt iedere inzet getoetst waarbij voor het meest geschikte middel gekozen wordt rekening houden met subsidiariteit en proportionaliteit.

(24 PvdA) Hoe wordt gewaarborgd dat de bevoegdheid tot het doen van het op afstand en heimelijk onderzoeken in een geautomatiseerd werk het ultimum remedium is in de reeks van bestaande bevoegdheden? Maakt de rechter-commissaris hierin een afweging? Waarom is het «niet uitge- sloten» dat er in plaats van het op afstand heimelijk binnendringen in een geautomatiseerd werk gekozen wordt voor een van de andere opsporings- bevoegdheden? Waarom wordt niet standaard eerst uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie?

Zie bovenstaand antwoord. Antwoord via MinVenJ.

(32 SP) Deze leden begrijpen dat inmiddels ook gebruik wordt gemaakt van internettaps, waardoor communicatiegegevens, die via internet gedeeld worden, afgetapt kunnen worden. Waarom is deze mogelijkheid blijkbaar onvoldoende zodat opsporingsambtenaren de bevoegdheid krijgen op afstand te kunnen hacken? Om welke opsporingsambtenaren gaat het en in welke situaties is het noodzakelijk?

Zie hiervoor het WODC rapport "het gebruik van de telefoon- en internettap in de opsporing" uit 2012. Data is tegenwoordig veelal geencrypt en veelal wordt gebruik gemaakt van verschillende communicatie kanalen die niet onder de tap staan.

NUT EN NOODZAAK

(34 D66) Kan de regering ingaan op de noodzaak en naast enkele concrete gevallen ook een meer overstijgende algemene noodzaak formuleren voor de toevoeging van deze bevoegdheid? Kan het ook op een andere minder ingrijpende wijze plaatsvinden?

Er is een groep criminelen en systemen waar de opsporing met behulp van traditionele opsporingsmethoden geen vat op kan krijgen. Het is een extra tool in de toolbox van de Politie. Waarmee het spectrum van tools wordt uitgebreid en waardoor de Politie voor sommige zaken een meer passende tool heeft.

(43 D66) Voorts vragen de leden van de D66-fractie de regering in te gaan op de voordelen van ICT-technologieën die het voor de politie de afgelopen jaren juist makkelijker hebben gemaakt om criminelen op te pakken, zoals beter beschikbare informatie via telefoons en iPads, het gebruik van drones, «gunshot-detection-systems», het monitoren van tweets en andere social media, het voorspellen van misdaad op basis van «big-data» of GPS-systemen. Kan de regering toelichten in hoeverre de technologische ontwikkelingen het werk van de politie de afgelopen jaren per saldo makkelijker of moeilijker hebben gemaakt? Kan de regering haar antwoord met statistieken onderbouwen?

Zie hiervoor het onlangs verschenen rapport over de kwaliteit van de recherche. Dit maakt duidelijk welke positie de politie op dit moment inneemt in het digitale domein.

(45 D66) Kan de regering toelichten hoe de reeds bestaande mogelijkheden een verdere uitbreiding van de bevoegdheid tot het heimelijk toegang verschaffen noodzakelijk maakt zoals het wetsvoorstel pretendeert? In hoeverre kan hier louter worden volstaan met het toevoegen van enkele strikte waarborgen voor toepassing in plaats van nog verder uitbreiden van de bevoegdheden?

De wereld verandert / digitaliseert, dan moet de opsporing mee veranderen. Het internet is ook niet meer te doorzoeken met slim googlen, de hoeveelheid data is te groot, slimme software is noodzakelijk. Bij een DDos aanval zullen we geen vingerafdrukken of voetsporen meer vinden. Nieuwe criminaliteit vraagt om nieuwe criminaliteitsbestrijding (zie 34 D66)

(60 PvdD) Deze leden zetten vraagtekens bij de bredere inzet van het wetsvoorstel als efficiencymiddel. Wat is de implicatie van de financiële paragraaf, waarin staat dat er kosten kunnen worden bespaard met de inzet van de bevoegdheid, omdat die andere bevoegdheden zou kunnen vervangen? Is het uitgesloten dat de hackbevoegdheid ook in andere domeinen kan worden toegepast? Deelt de regering de mening dat efficiency nooit een drijfveer zou mogen zijn als het gaat om de veiligheid, de grondrechten en de privacy van burgers?

Antwoord via MinVenJ.

(167 D66) Kan de regering nader toelichten waarom hacken via «socialengineering» of «phishing» niet voldoende is om de problemen geschetst in het hoofdstuk over de noodzaak van dit wetsvoorstel te overkomen?

De politie wil gebruik maken van alle potentiële kwetsbaarheden en zich dus niet laten beperken tot social engineering of phishing. Als de crimineel erg cyberbewust is, zal hij niet te engineeren of phishen zijn.

46 D66) De aan het woord zijnde leden vragen waaruit blijkt dat de bestaande bevoegdheden in toenemende mate te kort schieten. Welke wezenlijke problemen en gebleken knelpunten zijn er?

Er is een groep criminelen en systemen waar de opsporing met behulp van traditionele opsporingsmethoden geen vat op kan krijgen. Het is een extra tool in de toolbox van de Politie. Waarmee het spectrum van tools wordt uitgebreid en waardoor de Politie voor sommige zaken een meer passende tool heeft.

TECHNIEK EN TOETSING

(27 SP) De aan het woord zijnde leden vragen hoe men weet waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig zijn. Hoe groot is het risico dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing? Hoe wordt dit risico zoveel mogelijk weggenomen? Er kunnen bijvoorbeeld ongelooflijk veel gegevens verzameld worden bij toegang tot bijvoorbeeld de Cloud. Hiervoor zijn waarborgen ingebouwd, zoals toetsing door de rechter- commissaris naar de proportionaliteit, maar hoe wordt voorkomen dat ongericht gegevens wordt verzameld? Men weet immers niet altijd van tevoren waar welke gegevens vandaan gehaald moeten worden en welke gegevens nodig zijn. Hoe ziet de regering dit praktisch voor zich? De leden van de SP-fractie begrijpen, zoals de regering stelt, dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn. Soms is het werk waar de gegevens op staan niet bekend en is het tijdrovend en privacy schendend om deze te achterhalen. Betekent dit dat het plaatsen van software niet altijd mogelijk is?

Zie hiervoor het antwoord op eerdere vragen.

(154 CDA) Immers, hoe kan van tevoren worden vastgesteld wel programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturings- systeem is, wie er allemaal gebruik van maakt, etc.? Zijn dit niet juist allemaal onderdelen die door toepassing van de bevoegdheid inzichtelijk moeten worden voor politie en justitie?

Sommige informatie is vooraf te verkrijgen andere is pas na binnentreden beschikbaar. Er wordt op slimme manieren met behulp van diverse technieken gezocht naar belastende informatie.

TOETSING

(184 D66) Hoe wordt er op toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

GEHEIMHOUDERS

(31 SP) De leden van de SP-fractie merken op dat er een verplichting komt tot vernietiging van de gegevens die onder het geheimhoudingsplicht vallen. Maar wie bepaalt welke gegevens om die redenen kunnen worden vernietigd en om welke gegevens het gaat? Bovendien zijn de gegevens op dat moment reeds ingezien. Hoe wordt daarmee omgegaan? Heeft de betreffende opsporingsambtenaar dan een afgeleide geheimhoudingsplicht?

Het tactisch opsporingsteam zal gegevens die onder de geheimhoudingsplicht nooit onder ogen krijgen door de door de functiescheiding tussen het tactische en technische team. Het technisch team krijgt als eerste de informatie onder ogen, die wist de gegevens (alles op gelogde wijze) voordat iemand die zou kunnen acteren op de informatie ergens van weet.

(67 CDA) Met betrekking tot dit besluit vragen zij of wordt gecontroleerd of door advocaten opgegeven nummers inderdaad nummers van advocaten betreffen en niet een dekmantel vormen

voor contact met andere personen. Zo nee, waarom niet? Hoe kan gegarandeerd worden dat het verschoningsrecht op dit punt niet wordt misbruikt?

Dat heet niets met deze wet te maken. Antwoord via MinVenJ.

(73 D66) Kan de regering toelichten hoe dit in de praktijk werkt? Stel dat er een «keylogger» wordt geïnstalleerd op een smartphone. Hoe wordt in dat geval de «logging» stil gezet zodra de verdachte een whatsapp bericht verstuurd naar zijn advocaat? Kan de regering toelichten hoe omgegaan wordt met een concept e-mailbericht van een verdachte aan een advocaat?

Er worden geen uitspraken gedaan over de methoden en technieken die opsporingsinstanties gebruikten om haar werkzaamheden goed te kunnen uitvoeren.

FUNCTIESCHEIDING

(77 D66) Kan de regering in dit kader toelichten waar precies de overgang ligt tussen technisch optreden en tactisch optreden ten aanzien van geautomatiseerde werken?

Zodra er een bevel is afgegeven door de OvJ en RC om binnen te dringen gaat het technisch team aan het werk. De werkzaamheden van het technisch team zijn afhankelijk van de vraag vanuit het tactisch opsporingsteam. De beide teams werken onafhankelijk van elkaar. Waar de precieze overgang ligt tussen de beide teams is een onderdeel van het werkproces.

(116 CDA) Tegelijkertijd vragen zij of de regering de mening deelt dat in de praktijk juist van belang is dat deze teams goed met elkaar communiceren en geen verdere belemmeringen op dit punt worden opgelegd, ook niet in lagere regelgeving.

Communicatie is altijd een belangrijk onderdeel van een opsporingsonderzoek. Het is wel zaak om alleen te communiceren over die onderwerpen die een goede uitvoering van het onderzoek niet in de weg staan.

Van: 10.2.e P. - BD/DRC/CV [mailto10.2.e @minvenj.nl]
Verzonden: woensdag 15 juni 2016 12:18
Aan: 10.2.e - BD/DCS/ACSB; 10.2.e - BD/DGPOL/PBT/PT; 10.2.e 10.2.e @minbzk.nl); 10.2.e @mindef.nl; 10.2.e @mindef.nl; 10.2.e @minbzk.nl; 10.2.e :10.2.e @om.nl)
CC: 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV
Onderwerp: E-mail verzenden: Conceptbrief kwetsbaarheden V15jun2016.docx
Urgentie: Hoog

Beste collega's,

Bij deze ontvangen jullie de conceptbrief over de omgang met kwetsbaarheden ter afstemming. Daarbij heb ik twee verzoeken:

- Graag verneem ik jullie schriftelijk commentaar uiterlijk 21 juni, zo veel mogelijk in track changes.
- Graag verneem ik tbv een overleg hierover op welke dagen jullie volgende week en de week daarna NIET kunnen en er ook geen vervanging beschikbaar is.

Met vriendelijke groet,

10.2.e

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Rechtspleging en Rechtshandhaving Directie Rechtshandhaving en Criminaliteitsbestrijding Turfmarkt 147 |
2511 DP | Den Haag Postbus 20301 | 2500 EH | Den Haag M 10.2.e 10.2.e @minvenj.nl

From: 10.2.e
Sent: Wednesday, June 15, 2016 01:42 PM W. Europe Standard Time
To: 10.2.e 10.2.e .); 10.2.e @politieacademie.nl'; 10.2.e 10.2.e 10.2.e @mindef.nl'; 10.2.e @mindef.nl';10.2.e @belastingdienst.nl'; 10.2.e 10.2.e 10.2.e 10.2.e '; 10.2.e 10.2.e ; 10.2.e 10.2.e
Cc: 10.2.e 10.2.e 10.2.e 10.2.e
Subject: FW: E-mail verzenden: Conceptbrief kwetsbaarheden V15jun2016.docx

Beste mensen,

Bijgaand treffen jullie aan een conceptbrief over de omgang met kwetsbaarheden. Ik stuur hem nu ongezien door. Ik ga er morgen/vrijdag even mee aan de slag.
Mochten jullie opmerkingen hebben, dan hoor ik dat graag voor 20 juni (ik weet het, wederom een zeer krappe deadline vanuit het departement), zodat ik10.2.e op 21 juni van commentaar kan voorzien.

Met groet,

10.2.e

Van: 10.2.e
Verzonden: donderdag 16 juni 2016 13:00
Aan: '10.2.e BD/DGPOL/PBT/PT'
CC: 10.2.e .); 10.2.e
Onderwerp: Vragen en antwoorden Verslag CC III DGPOL met opm9
Bijlagen: Vragen en antwoorden Verslag CC III DGPOL met opm9

Hoi 10.2.e

bijgaand mijn opmerkingen en tekstvoorstellen. Dit heb ik niet met 10.2.e afgestemd, dus mocht zij nog meer of andere opmerkingen hebben, dan hoor ik dat ook graag.

Met vriendelijke groet,
10.2.e

Vragen en antwoorden Verslag CC III DGPOL

(131 VVD) De aan het woord zijn leden merken op dat het heimelijk binnendringen op afstand in een geautomatiseerd werk gebeurt door deskundige (technische) opsporingsambtenaren. Wordt er in de Contourennota Rijksrecherche en het opleidingsaanbod bij de Politieacademie rekening gehouden met de steeds grotere vraag bij de politie naar deze specialisten? Geldt zowel voor de tactische als voor de technische opsporingsdiensten dezelfde screening?

Ten behoeve van de implementatie van dit wetsvoorstel, maar ook in verband met de prioriteit die de aanpak van cybercriminaliteit heeft (zie inderdaad ook de Contourennota Opsporing), wordt de vraag en noodzaak van deze specialisten onderkend. De aankomende jaren zal middels door- en zij-instroom van medewerkers zoveel mogelijk in deze vraag worden voorzien (in relatie tot het Inrichtingsplan Nationale Politie). Het opleidingsaanbod bij de Politieacademie biedt tal van (verplichte) opleidingen, modules en trainingen aan op het gebied van cybercrime en digitale expertise, zoals Recherchekundige Master Digitaal, digitale opsporing, internet en opsporing, forensic scripting etc.. Nieuwe instroom of doorstroom van medewerkers genereert afname van extra opleidingen. Dit wordt in de ramingen meegenomen. 12-14

??

(277 SP) In hoeverre zal hier in de gaten worden gehouden of uitvoerende organisaties, vooral politie en rechtspraak, genoeg middelen hebben om deze taken uit te voeren? Hoe is er rekening gehouden met de bezuinigingen op ICT bij de politie?

De politie ontvangt een bijzondere bijdrage van 13,8 mln. per jaar voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld en cybercrime, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie. In brede zin zijn de middelen, waaronder (extra inhuur van) capaciteit, van de IV organisatie voor het uitvoeren van operationele ICT vernieuwingen binnen de politie op dit moment beperkt. De IV-projecten op het gebied van cybercrime staan echter op het IV-portfolio en worden uitgevoerd. Wel brengt de financiële druk met zich mee dat projecten vertraging oplopen, omdat niet altijd de volledig gewenste uren beschikbaar zijn. Echter, bij de inwerkingtreding van het onderhavige wetsvoorstel zal de politie in staat zijn de bijbehorende bevoegdheden uit te voeren.

Met opmerkingen 12-14

(278 SP) Is er voldoende expertise bij de politie om deze extra bevoegdheden op te vangen? Zijn er bovendien genoeg middelen om alle experts op te leiden om niet alleen om te gaan met de bevoegdheid, maar ook met de techniek die erbij komt kijken?

Zoals hierboven ook al is opgemerkt is ten behoeve van de implementatie van dit wetsvoorstel, maar ook in verband met de prioriteit die de aanpak van cybercriminaliteit heeft, wordt de vraag en noodzaak van deze specialisten onderkend. De aankomende jaren zal middels door- en zij-instroom van medewerkers zoveel mogelijk in deze vraag worden voorzien (in relatie tot het Inrichtingsplan Nationale Politie). Het opleidingsaanbod bij de Politieacademie biedt tal van (verplichte) opleidingen, modules en trainingen aan op het gebied van cybercrime en digitale expertise, zoals Recherchekundige Master Digitaal, digitale opsporing, internet en opsporing, forensic scripting etc..
PM: nieuwe opleidingen of specialisten ivm CC III voorzien? Zie hiervoor het antwoord op vraag 131.

(280 SP) Deze leden vragen nogmaals aandacht voor de capaciteit bij de politie. Er wordt 2.000 fte weggehaald bij de politie. Hoeveel extra capaciteit kan dan worden ingezet bij uitvoering van bevoegdheden op grond van dit wetsvoorstel? Komt deze capaciteit van binnen de nationale politie? Zo ja, waar vandaan? Of worden er nieuwe mensen aangetrokken? Kan de regering haar antwoord toelichten?

De politie werkt toe naar een operationele doelsterkte van 49.802 fte conform het inrichtingsplan. De realisatie hiervan verloopt stapsgewijs. De bezetting en de prognose voor de doorstroom, uitstroom en (zij-) instroom in de periode 2017-2021 en de instroom van aspiranten in 2017-2019 is (in aantallen) opgenomen in de Korpsbegroting 2017-2021, als onderdeel van het beheerplan Politie. Met deze instroom wordt geanticipeerd op de (toekomstige) uitstroom en instroom. Naast initiële instroom, is er sprake van specifieke instroom in de opsporing op HBO niveau. Dit betreft instroom onder meer op het gebied van Cybercrime. De totale zij-instroom vormt onderdeel van de personeelsprognose die in de begroting is opgenomen.

(282 CDA) Met verwondering hebben de leden van de CDA-fractie kennisgenomen van het standpunt dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk moeten dekken binnen het reguliere budget zonder dat de regering daarbij aangeeft wat die precieze kosten zijn. Alleen voor de Raad voor de rechtspraak (Rvdr) is een verwachte inschatting gegeven (€ 500.000) en alleen al daarvan kunnen deze leden zich voorstellen dat het geen eenvoudige klus zal zijn voor de Rvdr om dit binnen de huidige financiële (beperkte) begroting in te passen. Hoe ziet de regering dit aspect?

De politie ontvangt een bijzondere bijdrage van 13,8 mln. per jaar voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld en cybercrime, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De personeels- en IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie. Dit past in het reeds voorziene sterkte- en IVbeleid van politie.

(283 CDA) Waarom heeft de regering deze impact- analyse niet aan de Kamer gezonden dan wel de resultaten hiervan verwerkt in onderhavig wetsvoorstel? Is zij alsnog bereid zo spoedig mogelijk na ontvangt van dit verslag deze impactanalyse aan de Kamer te zenden?

Met opmerkingen 12-14

De impactanalyse die de politie heeft uitgevoerd is voor zover relevant meegenomen en verwerkt in het wetsvoorstel. De impactanalyse is niet meegezonden omdat de impactanalyse daarnaast ten doel had de politie voor te bereiden op de implementatie van dit wetsvoorstel. De impactanalyse is gezien de inhoud ervan, gerubriceerd als zeer vertrouwelijk en kan daarom niet worden toegezonden aan Uw Kamer.

(284 CDA) Wat zijn precies de aanzienlijke consequenties waarover de nationale politie het heeft in haar advies van 12 december 2014? Wat betekent onderhavig wetsvoorstel niet alleen budgettair, maar ook qua aantal benodigde extra fte voor de uitvoering hiervan? In het bijzonder vragen deze leden of er voldoende capaciteit in de technische teams is aanwezig is.

De consequenties waarover de politie heeft zijn dat het naast de inrichting van een geheel nieuw werkproces ook de aanpassing van bestaande processen vergt, een andere manier van werven van nieuwe medewerkers met een hogere kennisintensiteit en met een hogere functiewaardering, een nieuwe manier van het verkrijgen van de benodigde kennis, een verhoging van expertise en kennisniveau binnen bestaande afdelingen alsmede de aanleg, inrichting en het beheer van nieuwe ICT-infrastructuren en -middelen.

De politie ontvangt een bijzondere bijdrage van 13,8 mln. per jaar voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld en cybercrime, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De personeels- en IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie. Dit past in het reeds voorziene sterkte- en IVbeleid van politie.

Met opmerkingen 9]: Zie mijn eerdere opmerking.

De vraag en noodzaak van de digitaal experts wordt onderkend. De aankomende jaren zal middels door- en zij-instroom van medewerkers zoveel mogelijk in deze vraag worden voorzien (in relatie tot het Inrichtingsplan Nationale Politie).

(285 CDA) Valt te verwachten dat er veel meer gebruik zal worden gemaakt van de voorgestelde bevoegdheden? Zo ja, past zij hierop de personele bezetting van technische en tactische teams dan ook aan? Deze leden vragen wat de stand van zaken is van het implementatieplan van de nationale politie, waarnaar wordt verwezen in het hierboven genoemde advies.

De politie is sinds 2015 bezig met de implementatie van dit wetsvoorstel. De politie zal volgens een groeimodel klein beginnen, waarna de impact vanuit de praktijk getoetst zal worden en eventueel bij gesteld kan worden indien nodig.

12-14

(286 CDA)) De leden van de CDA-fractie vragen of er nog meer impactanalyses zijn opgesteld, bijvoorbeeld ten aanzien van het OM. Indien dat het geval is, vragen zij de regering deze aan de Kamer te doen toekomen. Zo lezen zij ook dat er een «quick-scan online handelsfraude» is uitgevoerd. Ook deze zouden zij graag ontvangen in het kader van de behandeling van dit wetsvoorstel.

De impactanalyse van politie is gezien de inhoud ervan gerubriceerd als zeer vertrouwelijk en kan daarom niet worden toegezonden aan Uw Kamer.

Met opmerkingen 9]: 12-14

(287 D66) Voor de politie en het OM ontbreken de bedragen. Deze leden missen de financiële gevolgen die uit het wetsvoorstel zullen voortvloeien voor de politie. Indien het regering aangeeft dat gevolgen ten koste komen van het totaal beschikbare budget voor de politie, aan welke bedragen moet dan gedacht worden en wat betekenen de financiële gevolgen van het voorstel voor andere activiteiten van de politie die uit hetzelfde bestaande budget gefinancierd worden?

De mate van financiële impact wordt onder andere bepaald door de keuze van de inrichting van het proces. De politie ontvangt een bijzondere bijdrage van 13,8 mln. per jaar voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld en cybercrime, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De personeels- en IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie. Dit past in het reeds voorziene sterkte- en IVbeleid van politie.

Met opmerkingen 9]: Zie eerdere opmerking hierover.

(288 D66) Deze leden vragen de regering de Kamer een impactanalyse met kostenplaatje te doen toekomen gelijktijdig met nota naar aanleiding van het verslag zodat de Kamer ook daar kennis van kan nemen.

De impactanalyse van politie is gezien de inhoud ervan gerubriceerd als zeer vertrouwelijk en kan daarom niet worden toegezonden aan Uw Kamer.

(289 D66) De leden van de D66-fractie vragen om een reactie op het bericht van de politie dat zij de nieuwe online opsporingstaken niet kan gaan uitvoeren als er voor 40 miljoen euro moet worden bezuinigd op de ICT, zoals de regering wil. Het plaatsvervangend hoofd van de Landelijke Recherche noemt de twee ambities van de regering «volstrekt onverenigbaar» en zegt dat «de politiek heel veel vraagt van de politie en zich goed moet afvragen waar de prioriteit ligt.» Wat is uw reactie op deze noodklok van de recherche en hoe denkt u er in te voorzien dat de ICT-faciliteiten van de politie geschikt zijn om de nieuwe hackbevoegdheden te kunnen uitvoeren?

De politie ontvangt een bijzondere bijdrage van 13,8 mln. per jaar voor de verdere professionalisering van het alledaagse politiewerk in een gedigitaliseerde wereld en cybercrime, waaronder ook aanschaf en implementatie van tooling. De voorbereiding van de implementatie van CCIII wordt hier ook voor een groot deel uit bekostigd. De IV capaciteit en structurele kosten voor beheer en onderhoud worden hier echter niet uit bekostigd en komen ten laste van de algemene begroting van de politie. In brede zin zijn de middelen, waaronder (extra inhuur van) capaciteit, van de IV organisatie voor het uitvoeren van operationele ICT vernieuwingen binnen de politie op dit moment beperkt. De IV-projecten op het gebied van cybercrime staan echter op het IV-portfolio en worden uitgevoerd. Wel brengt de financiële druk met zich mee dat projecten vertraging oplopen, omdat niet altijd de volledig gewenste uren beschikbaar zijn. Echter, bij de inwerkingtreding van het onderhavige wetsvoorstel zal de politie in staat zijn de bijbehorende bevoegdheden uit te voeren.

Met opmerkingen 9 : Zie mijn eerdere opmerking.

From: 9
Sent: woensdag 29 juni 2016 07:47:23
To: 10.2.e BD/DGPOL/PMP/FMI
Subject: Inge Philips

http://www.nrc nl/nieuws/2016/06/28/op-ict-bezuinigen-en-online-opsporing-verwachten-dat-gaat-niet-samen

From: 10.2.e BD/DGPOL/PMP/FMI
Sent: woensdag 29 juni 2016 08:08:39
To: 10.2.e BD/DGPOL/PBT/PT
Subject: FW: Inge Philips

Ter info

Van: 10.2.e /DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: woensdag 29 juni 2016 10:24
Aan: 10.2.e
Onderwerp: FW: Inge Philips

Ter info

Groet 10.2.e
06 10.2.e

Van: 10.2.e
Verzonden: vrijdag 1 juli 2016 11:36
Aan: 10.2.e 10.2.e 10.2.e @politieacademie.nl'; 10.2.e ;10.2.e 10.2.e @mindef.nl'; 10.2.e @mindef.nl'; '10.2.e @belastingdienst.nl';10.2.e 10.2.e 10.2.e ; '10.2.e @politieacademie.nl';10.2.e 10.2.e 10.2.e 10.2.e
CC: 10.2.e ; Philips, Inge (I.C.); 10.2.e ; 10.2.e
Onderwerp: Kwetsbaarheden brief nieuwe versie

Beste mensen,

Afgelopen woensdag ben ik aanwezig geweest bij een overleg op het departement met mensen van het departement, AIVD, MIVD en NCSC. Resultaat daarvan is bijgevoegde brief. Ik heb deze gisteravond ontvangen. Verzoek van het departement is om uiterlijk maandag COB te reageren... Heel kort dag, maar ik hoop dat er toch een mogelijk is voor sommigen om hier naar te kijken...

Alvast bedankt voor jullie hulp en een goed weekend.

10.2.e

Van: 10.2.e
Verzonden: maandag 4 juli 2016 14:15
Aan: 10.2.e
CC: 10.2.e Philips, Inge (I.C.); 10.2.e ;10.2.e 10.2.e 10.2.e '10.2.e @politieacademie.nl'; 10.2.e 10.2.e .); 10.2.e @mindef.nl'; 10.2.e @mindef.nl'; '10.2.e @belastingdienst.nl'; 10.2.e 10.2.e 10.2.e 10.2.e @politieacademie.nl'; 10.2.e 10.2.e 10.2.e
Onderwerp: RE: Kwetsbaarheden brief nieuwe versie

10.2.e

Bij deze mijn opmerkingen:

7-12-14

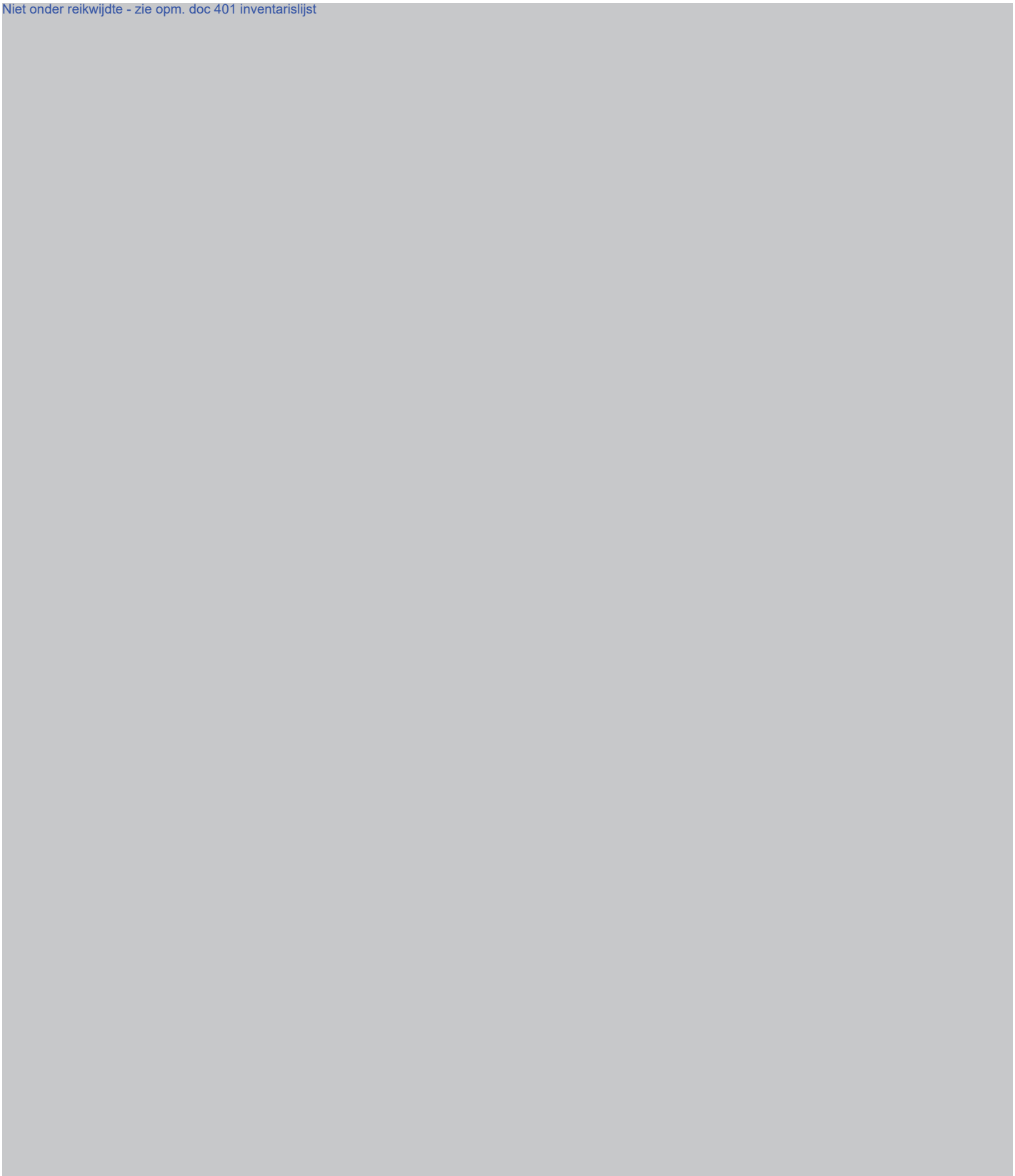
Dan nog een stijl opmerking:
Op pagina 3 wordt het NCSC genoemd. De eerste keer alleen als acroniem en de tweede keer met de volle naam.
Het is logischer als dat andersom is.

Tot zover mijn opmerkingen,

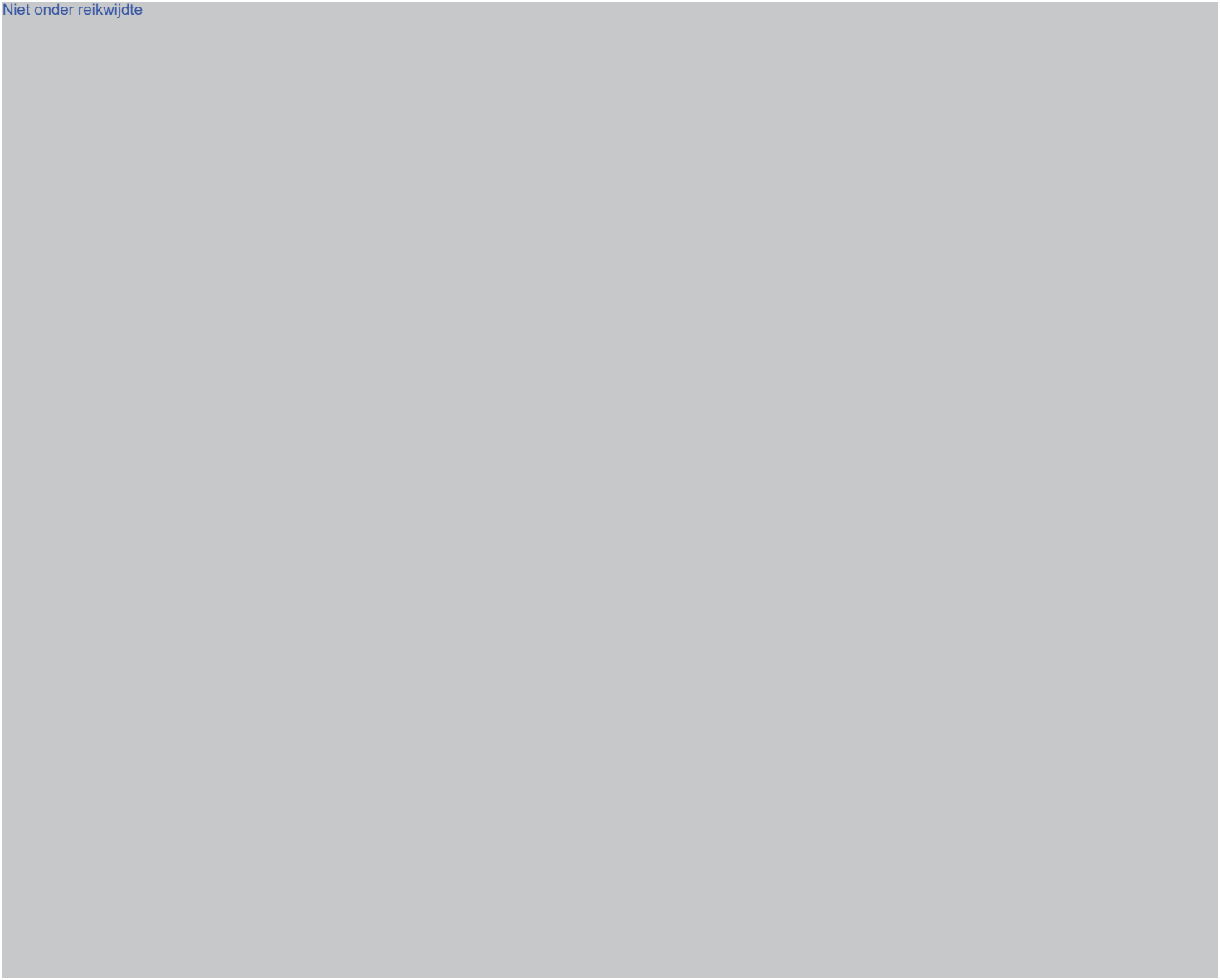
Grz,
10.2.e

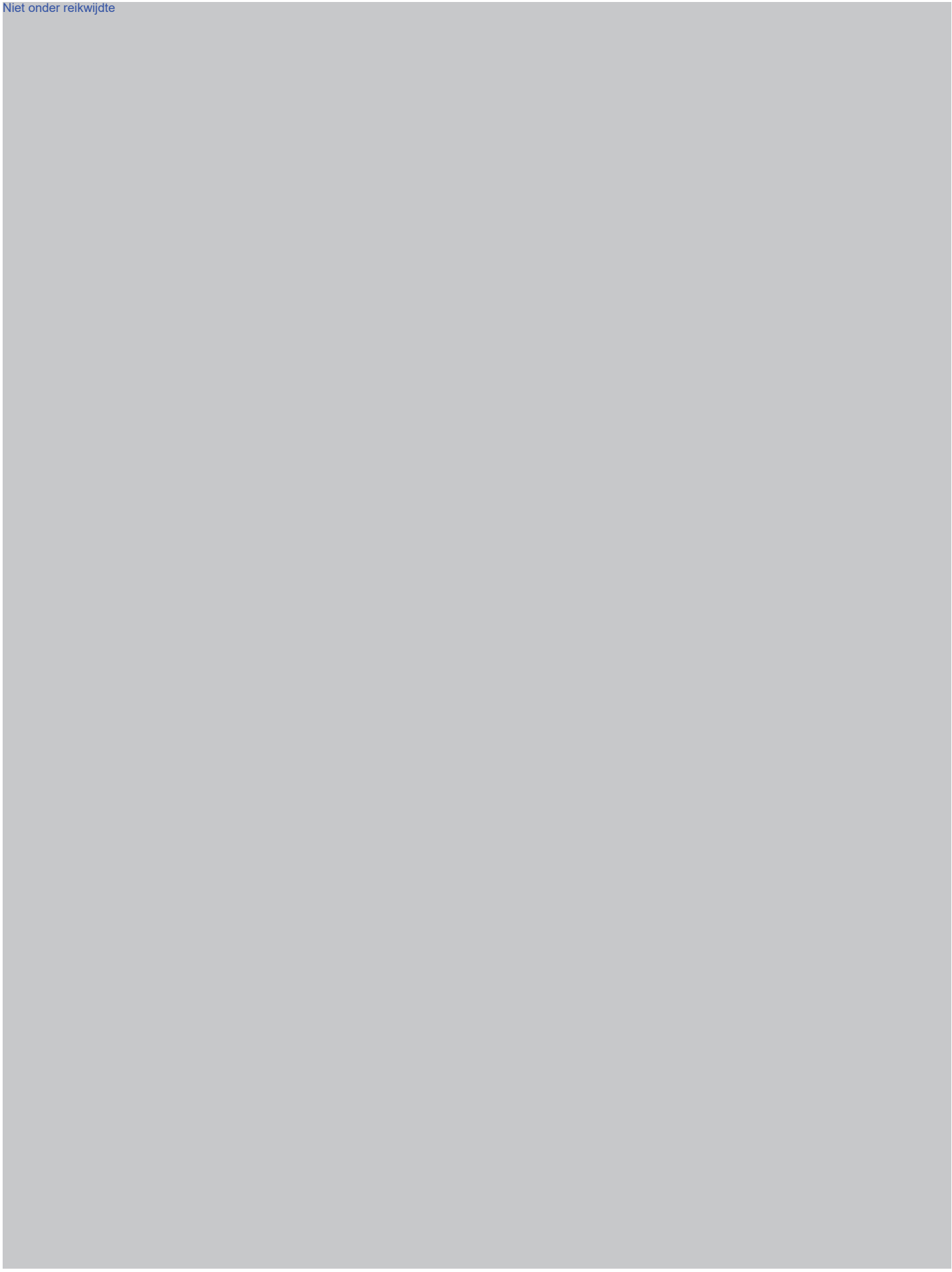

Niet onder reikwijdte - zie opm. doc 401 inventarislijst


Niet onder reikwijdte - zie opm. doc 401 inventarislijst

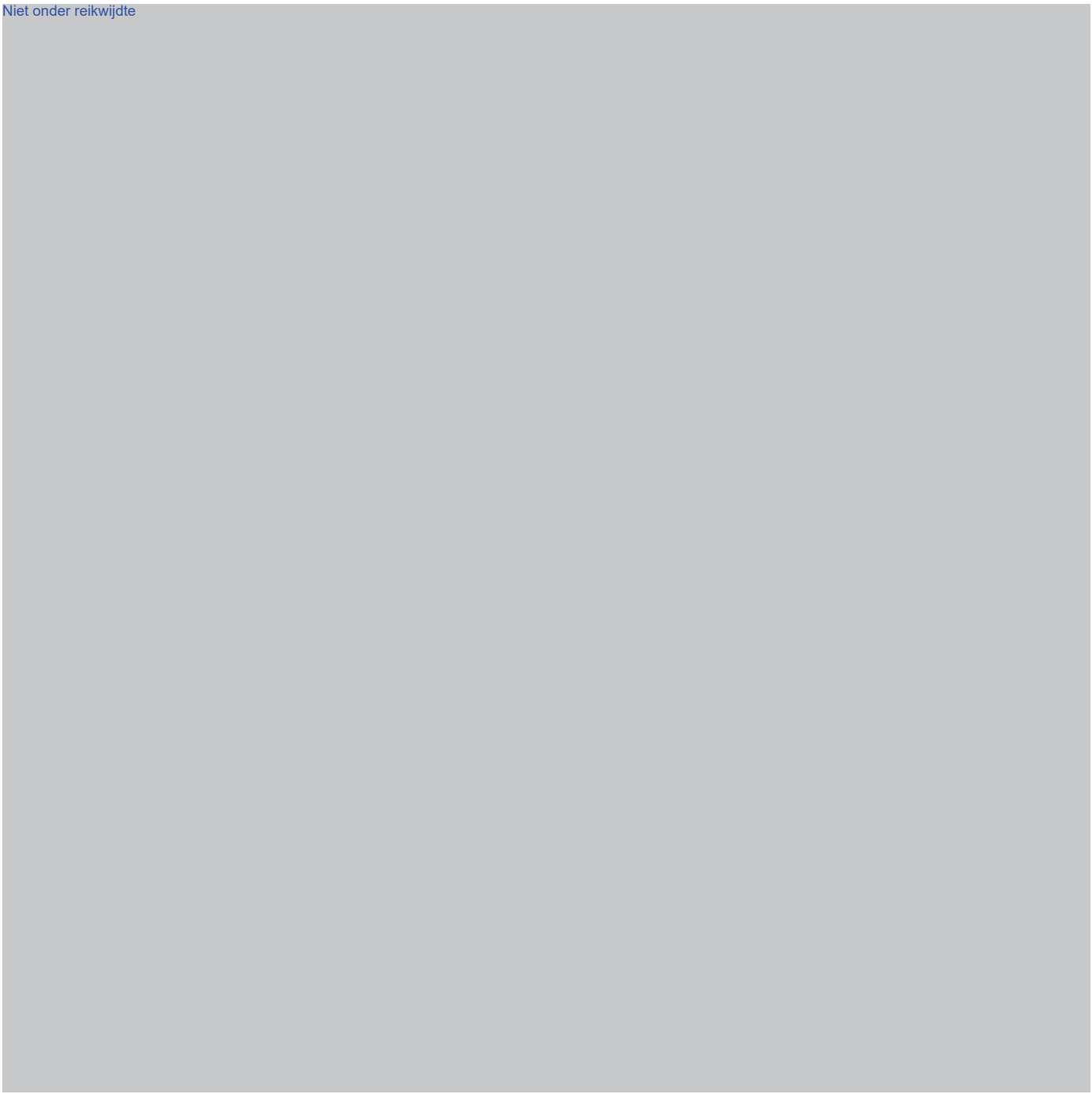

Niet onder reikwijdte - zie opm. doc 401 inventarislijst


Niet onder reikwijdte - zie opm. doc 401 inventarislijst


Niet onder reikwijdte


Niet onder reikwijdte


Niet onder reikwijdte


Niet onder reikwijdte

Van: 10.2.e
Verzonden: woensdag 10 augustus 2016 17:05
Aan: 10.2.e
CC: 10.2.e); 10.2.e 10.2.e 10.2.e
Onderwerp: FW:
Bijlagen: 20151117101022301.pdf

Beste 10.2. ,

Ingevolge ons gesprek van gisteren doe ik je een aantal documenten toekomen rondom het thema "Online Handelsfraude". Het rapport is toegelicht en besproken in de Stuurgroep CCIII en officieel aangeboden aan de portefeuillehouder Patricia Zorko door onze vz/opdrachtgever Inge Philips, voorzien van advies om de rapportage mee te nemen in het project Landelijk Centrum eCrime. Ofschoon Patricia het daar mee eens was (ik had het al besproken bij presentatie CCIII in Kerngroep, Inge is toen ziek naar huis gegaan), is er bij mijn weten, ook niet na rappél, antwoord op gekomen Dat moet nog wel, want dan heeft project CCIII décharge op dit punt.
Als jij dat laatste zou kunnen bevorderen, zeer graag!

PS We hebben 10.2.e recentelijk nog gesporken bij een afrondende bijeenkomst, maar 10.2.e heeft onderstaande actie kennelijk niet ingezet of het heeft niet tot resultaat geleid. 9 werkt nu bij ZSM, gr 9
De rest volgt nog, zo heb ik onder andere 10.2.e het geheel toegezonden en toegelicht.
Dat jij niet bent meegenomen in het circuit is wel verklaarbaar, want toendertijd moesten we het regelen met 10.2. , 10.2.e en 10.2.e

9

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg Postbus 100, 3970 AC Driebergen-Rijsenburg M 06 10.2.e Email :10.2.e @politie.nl

Organisatieonderdeel I

POLITIE

Behandeld door
Functie
Postadres

Bezoekadres

Telefoon
E-mail

Retouradres(zichtbaar in venster van envelop)

10.2.e
politiechef Eenheid Noord Holland

Ons kenmerk Ons kenmerk
Uw kenmerk Uw kenmerk
In afschrift aan In afschrift aan
Datum
Bijlage(n) 0
Pagina 1

Onderwerp Bijdrage 10.2.e voor de implementatie van de Wet Computer Criminaliteit III

Geachte mevrouw 10.2.e

In 2015 is het project Computer Criminaliteit III (CCIII) onder mijn leiding gestart met de voorbereiding van de politie op de implementatie van de Wet CCIII.Het project wordt uitgevoerd binnen de portefeuille Digitalisering en Cybercrime. Binnen de KL is Ruud Bik verantwoordelijk als domeinhouder Opsporing.

Een belangrijk onderdeel van het project is de impactanalyse van de gevolgen van de invoering van de wet op het gebied van "Online Handelsfraude". Op mijn verzoek heeft uw eenheid een bijdrage aan het project geleverd door de inzet van 9

Zij heeft gedurende de eerste helft van 2015 onderzoek gedaan en op 15 oktober 2015 de impactanalyse opgeleverd, welke zij op 28 oktober 2015 heeft gepresenteerd in de Stuurgroep CCIII. Zowel de inhoud van de impactanalyse als de presentatie en toelichting door 9 zijn door de Stuurgroep zeer positief ontvangen. U vindt hieronder de reactie van de Stuurgroep zoals deze is verwoord in de besluitenlijst van de Stuurgroep:

- 10.2.e verzorgt een presentatie van haar studie naar het deelonderwerp CCIII, "Online Handelsfraude". De Stuurgroepleden zijn unaniem positief over de kwaliteit en inhoud van de analyse, alsmede de heldere en overzichtelijke presentatie. Aan 10.2.e wordt mee gegeven dat het onderzoek helder en goed onderbouwd is. Vanuit de Stuurgroep krijgt 9 de complimenten voor haar geleverde prestatie.

Gelet op de presentatie en de conclusies van de impactanalyse is het mijn voornemen om de portefeuillehouder Digitalisering en Cybercrime te vragen deze impactnalyse aan de bieden aan de projectleider van het Landelijk Servicecentrum eCrime (LSCeC) met het advies om deze analyse uitdrukkelijk te betrekken bij de beleidsontwikkeling en uitvoering van het project LSCeC. De portefeuillehouder heeft tijdens de Kerngroep Digitalisering en Cybercrime reeds ingestemd met dit voornemen.

Ik wil mijn dank overbrengen aan uw Eenheid voor de medewerking. Daarnaast wil ik een speciaal woord van dank en de complimenten overbrengen aan 10.2.e voor haar inzet en resultaat. Uit persoonlijke waarneming en informatie van 9 weet ik dat zij veel en gedegen werk heeft verzet en dat zij regelmatig een eigen koers heeft moeten varen bij tegenwind en weerstand. Zij heeft aangetoond te staan voor haar visie en onderzoeksresultaten en hoewel zij persoonlijk opzag tegen de presentatie, heeft zij dit boven eigen verwachting op een rustige wijze uitstekend gedaan.

Datum
Onderwerp Bijdrage 10.2.e voor de implementatie van de Wet Computer Criminaliteit III
Pagina 2/2

POLITIE

Ik verzoek u bovenstaande over te brengen aan 10.2.e en haar, als je dat opportuun acht, in aanmerking te laten komen voor een blijk van waardering en/of persoonlijke beloning. Indien noodzakelijk of gewenst kunnen eventuele kosten worden gedekt vanuit het project CCIII.

Met vriendelijke groet

9

Inge Philips
Voorzitter Stuurgroep CCIII

Van: 10.2.e
Verzonden: woensdag 10 augustus 2016 17:07
Aan: 10.2.e
CC: 10.2.e
Onderwerp: FW: impactanalyse
Bijlagen: Bijlage 6.a - impactanalyse incl sjabloon.doc

Ten vervolge op informatiepakket, gr 10.2.e

Impactanalyse

Impactanalyse van invoering van de wet Computer Criminaliteit III op het gebied van online handelsfraude

Auteur: 10.2.e

In opdracht van: I. Philips

Projectleider: 10.2.e

Status: Definitief

Versie 1.1

1 oktober 2015

Rubricering: Politie Intern (Groen)

Toelichting voor gebruik van rubricering.

Deze code is verplicht voor ICT documenten.
Deze informatie is naar eigen inzicht te **verwijderen**. (klik in de tabel/plaatje en delete)

Rubricering	Hieronder valt informatie	Toelichting
Politie Intern (GROEN)	• die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden • waarvan toegang door niet-gerechtigden kan en/of zal leiden tot nadeel aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie	Onder nadeel wordt verstaan de schending van privacy van personen, doordat naam, adres en/of andere gevoelige gegevens openbaar worden, danwel het bekend worden van gegevens, waardoor de uitvoering van de politietaak kan worden aangetast en waarvan de gevolgen lastig zijn te herstellen
Politie Zeer Vertrouwelijk (GEEL)	• die betrekking heeft op de politie en door de politie uitgevoerde werkzaamheden • waarvan toegang door niet-gerechtigden kan en/of zal leiden tot schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie. • waarvan inzage door nietgerechtigden, kan leiden tot schadelijke gevolgen voor onderzoek naar de zware en georganiseerde criminaliteit	Onder schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de dienstverlening en/of taken van de politie, de ketenpartners en/of in het partnerdomein van de politie zodanig in gevaar komen, dat de gevolgen daarvan nauwelijks herstelbaar zullen zijn
Politie Geheim (ROOD)	• die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden en • waarvan toegang door niet-gerechtigden kan en/of zal leiden tot ernstige schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie. • waarvan inzage door niet gerechtigden kan leiden tot het toebrengen van ernstige schade aan de opsporing van, en de opsporingsmethodieken inzake ernstige inbreuken op de rechtsorde, of ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten	Onder ernstige schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn
Politie Zeer Geheim (PAARS)	• die betrekking heeft op de politie en de door de politie uitgevoerde werkzaamheden en • waarvan toegang door niet-gerechtigden kan en/of zal leiden tot zeer ernstige schade aan het korps, andere politieorganisaties, de ketenpartners, de dienstverlening en/of het partnerdomein van de politie • waarvan inzage door niet gerechtigden zeer ernstige schadelijke gevolgen heeft voor het onderzoek naar georganiseerde zware criminaliteit, of zeer ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten.	Onder zeer ernst ige schade kan onder meer verstaan worden de openbaarmaking van gegevens, waardoor de uitoefening van de taken van de politie zodanig in gevaar komen, dat deze onherstelbaar zullen zijn en mensenlevens in het geding zijn (infiltranten, informanten en beschermde getuigen).

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde Wijzigingen
1.0	01-07-2015		
1.1	01-10-2015		

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

Review commentaar

Versie	Wanneer	Wie	Functie

Inhoudsopgave

1. Inleiding

Met deze impactanalyse wordt getracht een verdieping te bewerkstelligen op de QuickScan van 10 september 2014 over de impact van het wetsvoorstel computercriminaliteit III waar wetgeving op het gebied van online handelsfraude in 2013 aan het wetsvoorstel is toegevoegd. De eenheden kunnen, indien nodig, deze impactanalyse gebruiken bij de implementatie. De onderzoekstermijn loopt van 1 januari 2015 tot en met 30 juni 2015.

Om de onderzoeksvraag: 'Wat is de impact van de invoering van de wijzigingen in de CCIII wetgeving op het gebied van online handelsfraude binnen de politie?' te kunnen beantwoorden zal allereerst een definitiebepaling worden gegeven van de term online handelsfraude. Daarna volgt een uiteenzetting van de beoordeling van de aanpassingen binnen de specifieke CCIII wetgeving. Vervolgens worden de werkprocessen beschreven waarbij een onderscheidt is gemaakt tussen Advies & intake, LMIO en Opsporing. In elke van deze werkprocessen wordt de geldende werkwijze tot en met 1 juli 2015 besproken, de mogelijke impact van de aanpassingen in de CCIII- wetgeving en de implementatie.

In deze impactanalyse wordt naar aanleiding van bevindingen een beschrijving gegeven van de huidige processen en eventuele wijzigingen na invoering van de nieuwe wetgeving op het gebied van onder andere Personeel, Informatie, Organisatie, Financiën, Administratie, Communicatie en Huisvesting. Tevens wordt beschreven wie de belanghebbenden en gebruikers zijn van de nieuwe wetgeving. Daarbij worden randvoorwaarden en afhankelijkheden, raakvlakken ten opzichte van andere projecten, mogelijke risico's, resources en de realisatie van producten zoveel als mogelijk weergegeven indien dit binnen de scope van het onderzoek valt. Activiteiten die voortvloeien uit deze impactanalyse kunnen worden opgenomen in een Project Initiatie Document die mogelijk later opgesteld zal worden.

Om tot deze bevindingen te komen is gekozen voor het bevragen van respondenten die direct betrokken zijn bij het werkproces van 'Online Handelsfraude' of indirect hiermee te maken hebben. Hierbij valt te denken aan [9] de opsporing op het niveau van zowel het wijkteam als de Districtsrecherche, Service & Intake, gegevensbeheer, informatiemanagement, Dienst Verlening Concept en functioneel beheer van diverse eenheden. Tevens is bij diverse respondenten om benodigde documentatie of toegang tot gegevens gevraagd. Er is als achtergrondinformatie voornamelijk gebruik gemaakt van de documenten die zijn opgeslagen in de bestandsmap op de schijf van het LMIO. Ook is er een zoekslag gemaakt op internet en de intranetsite van de politie voor aanvullende informatie.

2. Definitiebepaling online handelsfraude

Om een goed inzicht te krijgen over welke mogelijke problematiek we het nu hebben is allereerst een definitiebepaling van toepassing voor de term ‘online handelsfraude’. De definitie, zoals gebruikt wordt in het document ’antwoorden op Kamervragen over het Jaarverslag 2013’ (2014) zal als leidraad worden gebruikt.

Met de term handelsfraude wordt daar gedoeld “ op vormen van internetoplichting, waarbij goederen of diensten op internet worden aangeboden zonder dat deze na betaling worden geleverd”.

3. Wetgeving

Om te beoordelen wat de impact van de invoering van het nieuwe wetsvoorstel is op het gebied van online handelsfraude, is besloten om de aanpassingen in de CCIII wetgeving nader te bestuderen en te bekijken welke onderdelen van de wet mogelijk van toepassing kunnen zijn in de bestrijding van de online handelsfraude.

Uit nadere bestudering van de voorgestelde wetswijzigingen in het document 'Wijziging van het Wetboek van strafrecht en het wetboek van strafvordering in verband met de verbetering en versterking van de opsporing en vervolgens van computercriminaliteit (computercriminaliteit III)' (2013) blijkt dat de aanvulling op het artikel 326 Sr, met art 326d Sr, wellicht de grootste invloed op het proces van online handelsfraude heeft.

Artikel 326 Sr; Oplichting wordt uitgebreid met de volgende wetstekst:

Art 326d: Hij, die een beroep of een gewoonte maakt van het door middel van een geautomatiseerd werk te koop aanbieden van goederen of aanbieden van diensten met het oogmerk om die goederen of diensten na betaling niet te leveren wordt, indien betaling is gevolgd, gestraft met gevangenisstraf van ten hoogte vier jaren of een geldboete van de vijfde categorie.

De overige wetsartikelen die worden aangepast hebben volgens diverse respondenten weinig tot geen invloed op het werkproces binnen de online handelsfraude. De uitspraak van 11 maart 2015 over de wet bewaargegevens telecommunicatie is voor deze impactanalyse buiten beschouwing gelaten ondanks dat meerdere respondenten hier problemen mee voorzien bij het behandelen van de onderzoeken naar 'online handelsfraude'.

4. Werkproces

Binnen het scala van diverse vormen van cybercrime heeft de online handelsfraude de afgelopen jaren een vlucht genomen. De schadeposten groeien en de burger verwacht een antwoord van de politie (Holst, 2014). In 2010 is gestart met een pilotproject van het Landelijk Meldpunt Internet Oplichting. Ten tijde van de pilot, in de jaren 2010-2014, is het LMIO uitgegroeid tot een afdeling van formaat die op jaarbasis een geschat aantal van 50.000 meldingen van online handelsfraude ontvangt (Holst, mei 2014).

De landelijke prioriteit ‘verbeteren van intake en registratie’ van 2010-2014 wordt de komende jaren wederom als prioriteit gezien en cybercrime blijft in de jaren 2015-2018 ook een bestuurlijke prioriteit (Holst, 2014). Het Landelijk Service Centrum E-Crime, verder LSCEC te noemen, is in de mogelijkheid om invulling te geven aan de uitvoering van deze prioriteit en zal dan ook in nauwe samenwerking met het LMIO en DLOC/OIV een werkproces bepalen. Uiteraard dient hierbij wel rekening gehouden te worden met de uitwerking van het Dienst Verlening Concept (2012) van politie en de overige richtlijnen en toewijzingskaders die er binnen de Nationale Politie gesteld zijn.

Vanwege deze prioriteiten is men in de afgelopen jaren tot de conclusie gekomen dat het werkproces van het LMIO op bepaalde punten aangepast dient te worden zodat deze volledig conform de eisen van de Nationale Politie aan de geldende wet- en regelgeving voldoet. Het beëindigen van het contract met YourRequest, die tot voor kort de web-hosting van www.mijnpolitie.nl deed, is inmiddels in gang gezet. Per 1 mei 2015 is dit proces onder www.politie.nl ondergebracht waarbij het van belang is dat dezelfde dienstverlening (of beter) gecontinueerd kan worden (Holst, mei 2014). De lezer wordt dan ook verzocht om tijdens het lezen van deze impactanalyse rekening te houden met eventuele wijzigingen of aanpassingen die zich in het werkproces hebben voorgedaan of zich mogelijk in de toekomst nog voor gaan doen.

Om de impact van de wetgeving te bepalen, zullen de diverse werkprocessen op het gebied van online handelsfraude nader beschreven worden. Allereerst zal de advisering aan de burger en de intake worden besproken. De burger kan op diverse wijzen om advies vragen en aangifte doen bij de politie indien er sprake is van online handelsfraude. Hieruit voortvloeiend zal de rol en het werkproces van de medewerkers van het Regionaal Service Centrum (RSC), de Intake & Service (I&S) en de Dienst Landelijk Operationeel Centrum (DLOC/OIV) besproken worden. Er zal een onderverdeling worden gemaakt in de beschrijving van de huidige werkprocessen, de verwachte wijzigingen in de werkprocessen naar aanleiding van de aanpassing in de CCIII wetgeving en de mogelijke implementatie van deze wijzigingen inclusief eventuele aanbevelingen of verbeterpunten.

Vervolgens zal, volgens eenzelfde indeling het werkproces binnen het LMIO beschreven worden. Aangezien de huidige werkprocessen aan verandering onderhevig zijn, zal getracht worden een zo recent mogelijke opgave te doen van de werkzaamheden en bijbehorende werkprocessen. Na het werkproces van het LMIO besproken te hebben, volgt een beschrijving van het werkproces door de Opsporing. Tijdens het beschrijven van de diverse werkprocessen zal tevens ruimte worden gecreëerd voor mogelijke aanbevelingen of kritische kanttekeningen.

4.1 Advies & Intake

De basis van de werkzaamheden bij de afdelingen Intake & Service van de politie ligt, meestal, bij de advisering van burgers, het maken van een melding en/ of het helpen bij het doen van aangifte. Zo ook op het gebied van online handelsfraude. Het CBS heeft over het jaar 2013 berekend dat er in totaal in zo rond de 450.000 benadeelden van online handelsfraude waren en dat dit aantal de komende jaren alleen maar zal stijgen (Kloosterman, 2014).

4.1.1 Huidig werkproces

Indien burgers vragen hebben of advies willen, maken zij over het algemeen gebruik van de diensten van de medewerkers van een Regionaal Service Centrum (RSC) via 0900-8844 of van de mensen van de frontoffice op de bureau' s. De medewerkers van het RSC geven voornamelijk telefonisch advies omtrent een casus en zijn over het algemeen (nog) niet bekend met het opnemen van telefonische of 3D-aangiftes. Via een uitvraagprocedure proberen de medewerkers van het RSC te achterhalen wat de vraag van de burger is zodat zij deze van een advies kunnen voorzien. Indien een burger aangifte wil doen dan kunnen de medewerkers van het RSC deze op een willekeurig bureau in de eenheid inplannen zodat de medewerkers van Intake & Service deze aangifte op kunnen nemen of verwijzen naar de mogelijkheid om digitaal aangifte te doen.

Omdat de medewerkers van het RSC, tot voor kort, in hun opleiding niet in grote mate geconfronteerd worden met specifieke (strafrechtelijke) wet- en regelgeving kunnen ze gebruik maken van een uitvraagprotocol. In het geval van online handelsfraude is het merendeel van de medewerkers op het RSC op de hoogte van het feit dat mensen ook digitaal aangifte kunnen doen en verwezen ze daarbij de burger in eerste instantie naar de site www.mijnpolitie.nl. Vanwege gewijzigde procedures verwijst men sinds 1 mei 2015 naar de site www.politie.nl. De advisering voor de wijze voor het doen van aangifte verschilt echter wel per eenheid en per medewerker ondanks dat het LMIO heeft aangegeven dat de digitale mogelijkheid voor het doen van aangifte de voorkeur heeft.

De medewerkers van de Intake & Service op de bureau' s zijn, net als de collega's van het RSC in staat om adviezen aan burgers te verstrekken. Tevens zijn de medewerkers Intake & Service naast dat ze in het bezit zijn van de BOA specifiek opgeleid voor het opnemen van de aangiftes. Hierbij gaat het zowel om de lichtere aangiftes als om de complexere gevallen van bijvoorbeeld mishandeling, belaging of online handelsfraude. De medewerkers van Intake & Service zijn over het algemeen goed op de hoogte van de betreffende wet- en regelgeving en kunnen bij wijzigingen daarin goed anticiperen. Tevens geven respondenten aan dat de procedure m.b.t. het doen van aangifte van online handelsfraude bekend is en zijn de adviezen daarop aangepast ondanks dat de voorkeur in verwijzingsmogelijkheid per eenheid nog wel verschilt.

Uiteindelijk zal, met behulp van de inzet van het Click, Call, Face principe, in de toekomst ervoor gezorgd moeten worden dat er in toenemende mate op aangestuurd wordt dat het grootste gedeelte van de aangiftes online handelsfraude digitaal en op uniforme wijze bij de politie binnen komen.

PERSOONLIJKE AANGIFTE

Indien een burger aangifte wil doen omdat deze persoon slachtoffer is van 'online handelsfraude' dan zijn daar een aantal manieren voor, te weten, persoonlijk aangifte doen aan een bureau van politie, aangifte doen via een 3D- loket of aangifte doen via internet. Zoals eerder vermeld verschilt de voorkeur van verwijzen per eenheid. Waar de ene eenheid het, volgens respondenten, prettiger vind om te adviseren de burger aan een bureau de aangifte te laten doen vind de andere eenheid het prettiger om de burger te verwijzen naar de mogelijkheid om digitaal aangifte te doen. Een ding is volgens de privacyfunctionarissen duidelijk, de burger bepaalt te allen tijde of en op welke wijze deze de aangifte wil doen.

Indien een burger, ondanks tegenstrijdige adviezen of een gebrek aan (strafbare) feiten in de casus, erop staat om aangifte te doen dan is het protocol, volgens de privacyfunctionarissen, dat de aangifte, al dan niet direct, opgenomen wordt. Indien de aangifte niet direct opgenomen kan worden of de burger niet digitaal aangifte wil doen dan dient er een afspraak met de betreffende burger gemaakt te worden voor het doen van aangifte op een ander tijdstip of andere locatie. Het weigeren van het opnemen van een aangifte is, volgens een privacyfunctionaris en diverse respondenten werkzaam bij Intake & Service, uit den boze en strijdig met de geldende wet- en regelgeving, gestelde afspraken en protocollen. Bij het maken van alleen een melding is wel enige ruimte in beoordeling mogelijk.

Bij het opnemen van de aangifte op een bureau of in een 3D- Loket wordt bij ‘online handelsfraude’ meestal gebruik gemaakt van de maatschappelijke klasse F600 (oplichting) in BVH en wordt dit, tot op heden, niet nader gespecificeerd door middel van een projectcode. Voor het opnemen van een aangifte m.b.t. oplichting aan het bureau of via het 3D-loket staat 90 minuten ingepland. In het werkproces tussen het opnemen van een aangifte op een bureau of een 3D- loket zit nauwelijks verschil behalve dan de afdelingscode voor wat betreft de coördinatie.

De 3D- loketten zijn binnen de politie in opkomst en binnen een aantal eenheden worden pilot -projecten gedraaid met het verwerken van aangiftes binnen 3D-loketten. Op strategische plaatsen binnen een eenheid zijn loketten geplaatst die toegankelijk zijn voor burgers voor het doen van aangifte. Op een centrale locatie zit een medewerker van Intake & Service of het RSC die de toegang tot en het contact met de persoon in het 3D-loket bedient. Via deze weg is het mogelijk om aangifte te doen van ‘online handelsfraude’. Uit politiegegevens van de regio Noord- Holland blijkt dat op dit moment, in deze eenheid, nog minimaal gebruik wordt gemaakt van de mogelijkheid tot het doen van aangifte van online handelsfraude via het 3D-loket. Concrete cijfers van het doen van aangifte aan de bureau’ s binnen de eenheden kunnen via Cognos in de diverse eenheden opgevraagd worden, echter omdat de aangiftes online handelsfraude in de diverse eenheden zich op dit moment nog niet specifiek onderscheiden van overige aangiftes van oplichting is dit binnen het gestelde tijdsbestek niet te achterhalen.

DIGITALE AANGIFTE

Een burger heeft ook de mogelijkheid om via www.politie.nl digitaal, conform de uitgangspunten van het Dienstverleningsconcept, de aangifte te doen (Elenbaas, 2015). Het Click, Call, Face principe zal in de toekomst ervoor zorgen dat er in toenemende mate op aangestuurd wordt dat het grootste gedeelte van de aangiftes omtrent online handelsfraude via deze weg bij de politie binnen komen. Vanaf 1 mei 2015 is de site www.mijnpolitie.nl niet meer beschikbaar zijn voor de burger. Vanaf 1 mei 2015 wordt met www.politie.nl getracht om eenzelfde procedure van digitale dienstverlening te behouden zodat de kwaliteit van de dienstverlening gewaarborgd kan worden, echter, een tussenfase tussen de twee systemen valt niet te vermijden zoals in het stuk van Elenbaas (2015) aangegeven wordt.

Via de site www.politie.nl maakt de burger een melding van online handelsfraude met de intentie om aangifte te doen. In de tussenperiode komt deze melding binnen in de mailbox van het team Operationele Informatie Verwerking (OIV) van de afdeling Dienst Landelijke Operationeel Centrum (DLOC) van de Landelijke Eenheid. Een werkvoorbereider baseert op basis van kwaliteit en inhoud of de melding van een burger, die de intentie heeft om aangifte te doen, in BVH ingevoerd gaat worden. De exacte vorm en capaciteit van de afdeling die deze front-office diensten gaat vervullen, dient nog echter te worden vastgesteld maar op basis van een gemiddeld aantal van 50.000 digitale meldingen die op jaarbasis binnen komen zullen 4 a 5 fte zeker gewenst zijn (Elenbaas, 2015). Een respondent benadrukt dat hij, ondanks dat hij ervan uitgaat dat hier afspraken over zijn gesteld, moeite heeft met deze werkwijze omdat deze tegenstrijdig is met het intakeproces bij de bureaus en de RSC ’s. Volgens de betreffende respondent blijft het, ondanks dat de praktijk soms anders uitwijst, discutabel om als medewerker van politie te bepalen of een aangifte opgenomen wordt als een burger wel de intentie heeft om aangifte te doen. Gezien de grote aantallen van de meldingen snapt de respondent de overweging echter wel.

De automatische koppeling tussen het digitaal invoeren van een aangifte online handelsfraude is op dit moment wettelijk gezien volgens Elenbaas (2015) nog niet mogelijk. Vermoedelijk ligt hieraan ten grondslag dat de burger een aangifte zou doen van online handelsfraude met een bekende dader omdat er in veel gevallen een naam en bankrekeningnummer bekend zou zijn. Diverse respondenten trekken in twijfel of er in deze fase al bepaald kan worden of er sprake is van een bekende dader en daarmede iemand die als verdachte aangemerkt kan worden of eerder van een persoon die als ‘rol in onderzoek’ betiteld kan worden en verwijzen in dit geval naar pagina 20 van het handboek van BVH waar de landelijke afspraken m.b.t. oplossingsindicatie zijn gesteld. Wellicht dat deze afspraken kunnen bijdragen aan een mogelijkheid om de automatische koppeling tot stand te kunnen brengen tussen het digitaal doen

van aangifte van ‘internetoplichting’ van de burger en de systemen van politie zodat handmatige invoerwerkzaamheden, zoals nu het geval is, in de toekomst voorkomen kunnen worden. Indien dit geen uitkomst biedt dan zal er gewacht dienen te worden op de invoering van de wettelijke mogelijkheid om van dit soort feiten digitaal aangifte te doen. Tot die tijd zullen de burgers, die de intentie hebben om aangifte van online handelsfraude te doen, officieel een melding maken.

Tijdens dit werkproces worden de automatische meldingen richting de netwerkpartners zoals Marktplaats en de banken op eenzelfde wijze in stand gehouden als bij het proces ten tijde van het gebruik van YourRequest. Indien de aangifte in de BVH omgeving van de Landelijke Eenheid is ingevoerd dan wordt deze via de systemen 7-11-12 zichtbaar voor het LMIO.

Het LMIO verzorgt de analyse en bepaalt in overleg met het OM over het al dan niet starten van een voorbereidend strafrechtelijk onderzoek. De medewerker van DLOC die de aangifte in BVH invoert koppelt daar tevens een projectcode aan zodat duidelijk zichtbaar is dat de ingevoerde oplichtingszaak een online handelsfraude betreft. Door middel van het gebruik van deze projectcodes zoals OHF: internetoplichting , WWF: webwinkelfraude en OIF: voor overige internet gerelateerde fraude is er een duidelijk onderscheid zichtbaar en kunnen de aangiftes die digitaal worden ingediend beter worden geregistreerd.

Het zou de volgens de respondenten van gegevensbeheer de voorkeur hebben om deze indeling van projectcodes ook in de overige eenheden te gebruiken echter het LMIO vreest dat er vanwege het gebrek aan kennis en inzicht bij de gebruikers verkeerde combinaties van incidenten en bijbehorende projectcodes optreedt waardoor het cijferbeeld diffuus zou worden.

COÖRDINATIE

Indien een burger bij een bureau in een eenheid aangifte heeft gedaan van online handelsfraude dan wordt deze aangifte door een coördinerende afdeling in het wijkteam beoordeeld. Omdat een aangifte ingevoerd wordt in het BVH van de betreffende eenheid waar aangifte wordt gedaan, maakt deze registratie automatisch een link met het leidende programma voor de coördinatie van zaken, BOSZ. Het blijkt dat het LMIO in het verleden de betreffende coördinerende afdelingen binnen de eenheden heeft verzocht om contact met hun op te nemen om te kunnen bepalen of de betreffende aangifte aansluit bij een van hun dossiers/ onderzoeken. De achterliggende gedachte is dat op deze wijze het mogelijk dubbel uitvoeren van onderzoek ondervangen kan worden. Respondenten geven echter aan dat dit in de praktijk nauwelijks gebeurt en zelfs dat deze werkwijze niet bekend is.

Indien er een aangifte van online handelsfraude aan het bureau wordt gedaan dan krijgt een verbalisant op het wijkteam of een Basisteam Recherche- afdeling vaak de aangifte toebedeeld om het onderzoek te draaien. Als de betreffende collega in dat geval niet zelf de politiesystemen bevraagt om mogelijk verbanden met andere zaken te leggen dan kan het zijn dat de verbalisant de individuele casus onderzoekt.

Omdat op het basisteamniveau tegenwoordig veranderde procedures zijn, betekent dit dat een casus van online handelsfraude niet altijd een zaaksofficier krijgt en dus via ZSM afgehandeld wordt. In het hoofdstuk over Opsporing zal hier verder op in worden gegaan.

4.1.2. Impact van de nieuwe CCIII wetgeving

Om te kunnen bepalen wat de mogelijke impact zal zijn van de toevoeging van de artikelen van de CCIII wetgeving op het adviserings- en intakeproces van de politie, en met name de invloed van artikel 326d, is deze wetgeving voorgelegd aan diverse respondenten. Aan hen is gevraagd of zij verwachten dat deze wet een mogelijke impact gaat hebben op het werkproces en of zij een omschrijving kunnen geven van de mogelijke impact indien dit volgens hun het geval is. Tevens is aan hen gevraagd hoe zij denken dat deze

aanpassing in de wetgeving het beste kenbaar gemaakt kan worden onder de medewerkers van Intake & Service, het RSC, de coördinatoren en wellicht ook de wijkteams.

Om goed te kunnen bepalen welke impact de invoer van de CCIII wetgeving heeft op de afdelingen die belast zijn met de advisering en intake van de aangiftes omtrent online handelsfraude is het van belang om een beter cijfermatig inzicht te verkrijgen evenals inzicht in de specifieke opbouw van de betreffende afdelingen, die met deze werkzaamheden zijn belast. Allereerst zal er een inzage in de cijfers worden geboden gevolgd door een uiteenzetting van de mogelijke wijzigingen op de afdelingen zelf en mogelijke manieren om de wijzigingen te implementeren.

CIJFERS

Omdat er in de eenheden geen specifiek cijfermatig inzicht vanuit COGNOS is in de behandeling en afhandeling van het aantal onderzoeken omtrent online handelsfraude is aan het LMIO gevraagd om een overzicht te presenteren.

Het LMIO kan o.a. een globaal overzicht over het jaar 2013 verschaffen waarin men aan kan geven hoeveel dossiers er vanuit een eenheid gestart worden m.b.t. online handelsfraude maar ook vanuit het LMIO zelf. Laatstgenoemde zal echter later beschreven worden. De onderstaande cijfers staan ook in de QuickScan (2014) vernoemd. Bij de interpretatie van deze gegevens dient er rekening mee te worden gehouden met het feit dat een dossier, dat vanuit een eenheid wordt gestart, kan bestaan uit een (1) enkele of meerdere aangiftes en geen indicatie geeft voor het totaal aantal opgenomen en verwerkte aangiftes ‘online handelsfraude’ binnen een eenheid.

Tabel 1: Dossiers online handelsfraude per eenheid in 2013

Eenheid	Dossiers vanuit de Eenheid
1. Noord Nederland	6
2. Oost- Nederland	22
3. Midden- Nederland	7
4. Noord Holland	4
5. Amsterdam	5
6. Haaglanden	14
7. Rotterdam	7
8. Zeeland & West-Brabant	5
9. Noord- Oost Brabant	9
10. Limburg	4
11. Totaal	83

(bron; QuickScan 2014)

Diverse respondenten geven aan dat men ervaart dat er steeds vaker aan bureau’ s om advies wordt gevraagd en aangifte word gedaan van online handelsfraude, concrete cijfers over de advisering zijn er niet. Tevens ervaart men een toename in het aantal aangiftes van mogelijke katvangers die aangifte komen doen van diefstal van hun bankpas inclusief pincode. Laatstgenoemde valt officieel niet onder de online handelsfraude maar is wel een aspect waar in de beoordeling m.b.t. de impact ook rekening mee kan worden gehouden ondanks dat dit eigenlijk buiten de scope van het onderzoek valt.

Tevens is het op dit moment zo dat het LMIO aangeeft ongeveer 50.000 meldingen op jaarbasis binnen te krijgen. Het CBS heeft berekend dat er in Nederland 450.000 benadeelden zijn en dat deze aantallen alleen maar zullen stijgen. In de registratie ‘missen’ we dus grofweg 400.000 aangiftes.

Het ontbreken van aangiftes kan een aantal oorzaken hebben die niet zozeer binnen de politie hoeven te liggen. Men kan hierbij denken aan een verminderde aangiftebereidheid van burgers of een gebrek aan kennis bij burgers naar de mogelijkheden voor het doen van aangifte of een gebrek aan vertrouwen dat de politie hun zaak in onderzoek neemt.

Een aantal oorzaken dat binnen de politie gezocht kan worden is onder andere de wijze van het registreren van meldingen en cijfers omtrent online handelsfraude in de daarvoor aangewezen politiesystemen maar ook het verstrekken van het advies dat zaken van online handelsfraude civiel zijn en niet strafrechtelijk wat helaas, volgens sommige respondenten, nog steeds voorkomt.

Uit navraag bij diverse respondenten blijkt dat zij ervaren dat de medewerkers van Intake & Service op de bureau' s binnen de eenheden over het algemeen goed op de hoogte zijn van de betreffende wet- en regelgeving en zeer bekend zijn met het opnemen van aangiftes. Tevens vervullen de medewerkers aan de frontoffice een adviserende rol en plannen en verwerken regelmatig aangiftes waaronder die van internetoplichting. Gemiddeld hebben de medewerkers voor het opnemen van een aangifte in BVH oplichting 90 minuten de tijd.

Indien de wetgeving wordt aangepast conform hetgeen er vermeld wordt in de CCIII- wetgeving heeft dit volgens diverse respondenten wel invloed op het (proces van) adviseren van de burger. Op het gebied van online handelsfraude heeft artikel 326d de meeste invloed. Volgens respondenten vervaagt met de invoer van dat artikel de grens tussen civielrechtelijke zaken en strafrechtelijke zaken meer. Waar vroeger, indien er niet aan de bestanddelen van het artikel oplichting kon worden voldaan, de burger al snel werd verteld dat ze een civiele procedure op moesten starten omdat er strafrechtelijk geen mogelijkheden waren omdat oplichting (valse naam/hoedanigheid/ listige kunstgrepen etc.) niet kon worden bewezen, zullen met de nieuwe wetgeving burgers vanaf dat moment meestal het advies krijgen om aangifte te doen. De wettelijke bestandsdelen van het artikel 326d zijn volgens de respondenten makkelijker te bewijzen en beschrijven. Met name de omschrijving van de valse naam/hoedanigheid, listige kunstgrepen of samenweefsel van verdichtsels levert bij het reguliere artikel van oplichting, 326 Sr, problemen op.

De advisering op basis van het artikel 326d zal dus veranderen ten opzichte van de huidige situatie. Burgers zullen met de invoering van de nieuwe wetgeving vaker te horen krijgen dat zij aangifte kunnen doen en daarmee werkt de toevoeging van de wet dus drempelverlagend richting de burger. De wijze waarop de burger aangifte kan doen, blijkt per eenheid nogal te verschillen. Waar de ene eenheid de servicegerichtheid voornamelijk zoekt in het persoonlijke contact met de burger, zoekt een andere eenheid dit juist in de snelheid van het oppakken van zaken door middel van het doorverwijzen naar de digitale mogelijkheid om aangifte te doen. Een landelijke uniforme werkwijze omtrent het adviseren en doorverwijzen van burgers is er volgens de respondenten niet en kan verschillen per casus. Het LMIO pleit ervoor om zoveel mogelijk burgers naar de digitale manier van aangifte doen te verwijzen. Hierdoor komen de aangiftes binnen bij de medewerkers van het LSCEC die dit volgens de afgesproken werkwijzen verwerken in de BVH-omgeving van de Landelijke Eenheid. Met een potentieel hoger aantal digitale aangiftes komt daar dan ook in eerste instantie de werkdruk te liggen.

Bij de introductie van de nieuwe wetgeving, artikel 326d Sr, is het volgens een meerderheid van de respondenten mogelijk dat het aantal aangiftes omtrent 'online handelsfraude' toeneemt. Tot op heden krijgen burgers toch met enige regelmaat te horen dat ze geen aangifte kunnen doen omdat hun casus niet aan de wettelijke bestanddelen van oplichting voldoet. Met de nieuwe wetgeving is het bijna niet meer mogelijk om dit advies uit te brengen. Wel gaven de respondenten aan dat er, als gevolg van de wijziging van de wetgeving, wellicht meer aangiftes op het bureau of in het 3D-loket omtrent online handelsfraude binnen zouden kunnen komen wat er mogelijk voor zorgt dat de druk op de medewerkers van het RSC en de Intake & Service toeneemt. Op de vraag over welke aantallen we het dan hebben kon geen van de respondenten antwoord geven maar men verwacht uiteindelijk dat de totale impact hiervan te overzien is.

Enkele respondenten geven aan dat de Intake & Service ook steeds meer geconfronteerd wordt met aangiftes van potentiele katvangers. In het geval van online handelsfraude zijn katvangers personen die hun bankpas en pincode, veelal tegen betaling, af hebben gestaan aan een persoon die de betreffende rekening gebruikt om geld op te laten storten om het vervolgens op te nemen. Om aansprakelijkheid te voorkomen doen veel katvangers aangifte van diefstal van hun bankpas en pincode. Al deze aangiftes leveren eveneens een extra druk op bij de Intake & Service en uiteindelijk wellicht ook bij de opsporing.

Volgens diverse respondenten is de werkdruk bij de medewerkers Intake & Service op dit moment al redelijk hoog. De reorganisatie in combinatie met het ‘veranderende’ dienstverleningsconcept zorgen ervoor dat het aantal bureau’ s met openstellingen afneemt. Tevens is er sprake van een afname van het aantal medewerkers Intake & Service op de bureau’ s waardoor de druk bij de overgebleven medewerkers stijgt.

Met de huidige ontwikkelingen is het niet mogelijk om meer personeel voor de Intake & Service aan te trekken en lopen de afdelingen van Intake & Service op het bureau in sommige gevallen al over van de werkzaamheden. Mogelijk dat de eventuele stijging van het aantal aangiften aan het bureau of via een 3D- loket gaat leiden tot een wachttijd voor het doen van aangifte. Adviseren om zoveel mogelijk personen digitaal aangifte te laten doen is een optie om de druk bij de afdelingen Intake & Service en het RSC in de eenheden te doen laten afnemen. Of dit een gewenste situatie is in het kader van de servicegerichtheid voor sommige regio’s in het land is echter de vraag. Een (1) enkele respondent geeft aan dat het wellicht interessant is om de medewerkers van het RSC en Intake & Service meer bekend te maken met het LMIO zodat zij uiteindelijk beter inzicht krijgen in de werkprocessen van het LMIO. De respondent acht dit echter niet specifiek noodzakelijk voor de implementatie van de nieuwe wetgeving.

4.1.3: Implementatie

Indien de voorgestelde CCIII wetgeving geïmplementeerd dient te worden, is het van belang om op voorhand te inventariseren welke activiteiten ondernomen dienen te worden om dit uiteindelijk te kunnen realiseren. Voor de advisering & Intake zal het PIOFACH model aangehouden worden.

PERSONEEL

Respondenten geven aan dat de medewerkers van Intake & Service op de bureau’ s geen aanvullende opleidingen nodig hebben om de aanvulling van artikel 326d op een juiste wijze te kunnen toepassen. Over het algemeen zijn de medewerkers in het bezit van gedegen wetskennis en valt een relatief kleine aanpassing als dit goed te overzien. Respondenten geven aan dat men wel op de hoogte dient te worden gebracht als er sprake is van een wijziging in het werkproces van de systemen, o.a. BVH, waar zij in werken. Mogelijk dat dit soort wijzigingen via de BVH A-Z vermeld en verspreid kunnen worden.

In verband met de reorganisatie zal het aantal fte’s van de medewerkers van Intake & Service op de bureau’ s beperkter worden terwijl de werkzaamheden vermoedelijk niet af zullen nemen. Het toe te passen Click, Call, Face principe zal ervoor zorgen dat de afdeling Intake & Service op het bureau minder belast wordt met de aangiftes van lichtere vergrijpen. Deze lichtere vergrijpen zullen echter in toenemende mate door de medewerkers van het RSC opgepakt gaan worden. Er vind hier dus meer een verplaatsing van lasten plaats dan dat er sprake is van een verlichting van lasten.

De RSC’ s zullen na de reorganisatie vermoedelijk uit gaan breiden zodat het Dienst Verlening Concept ook daar tot uitvoer kan worden gebracht. Er zullen hiervoor medewerkers aangetrokken moeten worden die allen voorzien dienen te worden van de juiste opleidingen. Hierbij valt te denken aan opleidingen voor de BOA en wetskennis om aangiftes op te nemen, maar ook opleidingen die ervoor zorgen dat de medewerkers op een juiste wijze om kunnen gaan met de diverse systemen die binnen de politie gebruikt worden. Tevens dient men bij het RSC opgeleid te worden aangiftes die via het 3D- loket gedaan worden op te nemen. Het is mogelijk dat via deze wijze aangiftes van online handelsfraude worden gedaan.

Binnen de afdeling OIV/DLOC hebben de medewerkers vermoedelijk geen aanvullende opleidingen nodig. Door het LMIO is een omschrijving van de gewenste tekstbestanden voor de Fomutra en de Verklaring van de Aangever beschikbaar gesteld. Beide tekstbestanden blijken na beoordeling met name geschikt om artikel 326d primair ten laste te leggen.

INFORMATIE

Als de CCIII wetgeving doorgang gaat vinden dan dienen de systemen binnen de politie, en met name BVH, daarop aangepast te worden. Vanwege de mogelijke toevoeging van het wetsartikel 326d dient dit strafrechtelijke artikel aan incidentcodes in BVH gekoppeld te worden. Tevens is het daarbij mogelijk om de lijst van Modus Operandi (MO) aan te passen zodat de medewerkers bij het opnemen van een aangifte de van toepassing zijnde MO toe kunnen voegen.

Volgens een respondent van functioneel beheer zijn er binnen de Landelijke Eenheid medewerkers werkzaam die wetswijzigingen in kaart brengen zodat politiesystemen in een kort tijdsbestek daarop aangepast kunnen worden. Indien er goedkeuring is voor de aanpassing van de CCIII wetgeving is het, volgens de respondent, ook mogelijk om dit zelf aan een functioneel beheerder door te geven. BVH is een systeem dat eens per maand ge-update kan worden en de respondent die gespecialiseerd is op dit gebied ziet in de wetstoevoeging van artikel 326d op dit moment geen moeilijkheden waarom het niet binnen een korte termijn in BVH aangepast kan worden.

Met betrekking tot de invoering van de projectcodes in de overige eenheden zal een kosten- baten afweging gemaakt dienen te worden. Van het totaal aantal aangiftes dat binnenkomt, gaat 80% volgens het LMIO digitaal en komt 20% via het bureau binnen. Wellicht dat het zelfs mogelijk is dat LMIO via 7-11-12 aangiftes die niet digitaal binnen komen scant en de coördinerende rol die ze hebben van toepassing laat zijn in het toevoegen van de projectcode. Zodoende wordt de 20% aangiftes aan het bureau niet uitgesloten d.m.v. een andere werkwijze en ontstaat er een uniform werkproces die geldig is voor alle eenheden.

ORGANISATIE

Vanwege een mogelijke toename in het aantal aangiftes van online handelsfraude is het wellicht een optie om een meer uniforme wijze op sturing van het werkproces binnen de advisering en Intake aan te houden. Door middel van het meer onder de aandacht brengen van het Click, Call, Face principe is het mogelijk om de burgers meer te verwijzen naar de digitale mogelijkheden van het doen van aangifte van online handelsfraude.

Relevante informatie op de site www.politie.nl met betrekking tot internetoplichting dient dan wel paraat en up- to- date te zijn. Vanwege de veranderingen is er tot op heden nog geen inventarisatie gemaakt van het (gewenste) aanbod van informatie op deze site of voor collega's op een intranetsite.

FINANCIËN

Ondanks een mogelijke toename van het aantal aangiftes is het niet mogelijk om een personele uitbreiding op de afdeling Intake & Service te bewerkstelligen. Binnen de RSC' s komen er na de reorganisatie wel mogelijkheden voor uitbreiding van personeel, echter dit is niet specifiek gekoppeld aan en noodzakelijk voor de implementatie van de CCIII wetgeving. Op dit gebied zijn dan ook geen tot nauwelijks toenemende kostenposten te verwachten. Tevens is het inrichtingsplan per eenheid/ regio op dit moment leidend en kunnen er qua personele bezetting nauwelijks aanpassingen worden gedaan.

Omdat binnen OIV en DLOC, ten tijde van het opmaken van dit document, nog niet specifiek is vastgesteld hoeveel medewerkers beschikbaar worden gesteld om de frontoffice werkzaamheden te verwerken van de meldingen die digitaal binnen komen is het nog niet mogelijk om dit in geld of middelen

uit te drukken. De aantallen verschillen van 5 tot en met 10 medewerkers en zijn wellicht ten tijde van dit nieuwe traject en het aanbod nog aan te passen. Hierbij dient vermeld te worden dat deze personeelsuitbreiding tot op heden nog niet samenhangt met de mogelijke implementatie van de CCIII wetgeving op het gebied van online handelsfraude.

ADMINISTRATIE

De implementatie van de nieuwe wetgeving behoeft geen extra administratieve belasting voor het personeel van Intake & Service, het RSC en DLOC te betekenen, echter, dit valt ook niet geheel uit te sluiten. De processen binnen de politiesystemen worden op kleine onderdelen aangepast maar is daarmee niet verantwoordelijk voor een uitbreiding van de administratieve werkzaamheden binnen de advisering en intake ten aanzien van de werkzaamheden zoals deze nu uitgevoerd worden.

Met een verwachte toename in het aanbod en daarmee ook een toename in de verwerking van het aantal aangiftes nemen echter wel de administratieve lasten voor de medewerkers toe omdat er mogelijk vaker aangifte gedaan wordt. Om een afname van de administratieve lasten te creëren is het van belang om de (wettelijke) beperkingen, die op dit moment het proces van het digitaal aangifte doen van online handelsfraude in de weg staan, aan te passen. Indien een directe koppeling tussen het doen van aangifte door een burger en de verwerking in de systemen van politie mogelijk is, draagt dit bij aan een administratieve lastenverlichting omdat er dan een automatische koppeling met de politiesystemen mogelijk is. Het wetsvoorstel om digitale aangifte van een feit gepleegd door een ‘bekende’ dader mogelijk te maken zou in februari 2015 behandeld worden echter hier is nog geen uitsluitsel over.

COMMUNICATIE

Respondenten geven aan dat het wel van belang is om via meerdere kanalen de wijziging van de wetgeving te communiceren met de medewerkers van de Intake & Service, het RSC en DLOC/LSCEC te communiceren. Men spreekt dan voornamelijk over het vermelden van deze wetgeving op intranet, via de mail en via briefings maar men onderschrijft voornamelijk de verspreiding via ‘warme’ communicatie.

Binnen de Intake & Service kunnen met name de beleidsmedewerkers van het Dienstverleningsconcept, teamchefs en direct leidinggevenden een rol spelen in de overdracht van de aangepaste wetgeving. Indien dit op de diverse bureau’ s binnen de diverse eenheden verspreidt wordt door middel van meldingen via intranet, mails en briefings aangevuld met ‘warme communicatie’, daar waar nodig, dan is het mogelijk om binnen een redelijk korte termijn de medewerkers op de hoogte te stellen van de wijziging. Voor de melding op intranet zal een deskundige op het gebied van communicatie moeten worden ingeschakeld evenals de beheerders van de intranetsites van de diverse eenheden om de boodschap op eenduidige wijze te kunnen communiceren.

Bij de implementatie van de wetgeving valt wellicht ook te denken aan de externe communicatie. Hiermee wordt gedoeld op de berichtgeving van de overheid richting de burgers omtrent de aanpassingen binnen deze wetgeving. Hierbij kan gedacht worden aan het vertonen van SIRE-spotjes, maar zijn programma’s als Radar/ Opgelicht of andere media (journaal/kranten) ook een optie om de aanpassing in de wetgeving en daarmee de noodzaak en mogelijkheden tot het doen van aangifte kenbaar te maken. Een mogelijke indirecte consequentie die hieruit voortvloeit is een impliciete belofte dat de politie werk maakt van online handelsfraude en dat men zich niet achter excuses kan verschuilen om dit soort zaken niet op te pakken. Hier dient de organisatie dan ook goed rekening mee te houden.

Diverse respondenten uit meerdere eenheden hebben aangegeven dat het hun voorkeur heeft om meer aandacht te besteden aan manieren om internetoplichting te voorkomen of het fenomeen beter kenbaar te maken aan het publiek. Naar hun mening wordt daar op dit moment te weinig aandacht aan besteed. Respondenten geven wel aan dat er op dit moment veel sites online zijn waar dit wordt gemeld, echter ze betwijfelen de functionaliteit van al deze diverse sites omdat men merkt dat de burger pas in aanraking komt met deze sites als het leed al is geschiedt. Het gebruik van de checkfunctie op de voormalige site

www.mijnpolitie.nl (nu www.politie.nl) was tevens bij een aantal respondenten nog niet bekend. Wellicht dat de collega's die veelvuldig contact hebben met de burger hier op een simpele doch doeltreffende manier van op de hoogte kunnen worden gebracht en dit via de 'warme' communicatie tijdens klantcontact kunnen doorgeven.

HUISVESTING

Ondanks dat de afdeling Intake & Service en het RSC, vanwege de reorganisatie en de implementatie van de Dienstverleningsconcept, aan veranderingen onderhevig zijn, heeft de CCIII wetswijziging voor wat de betreft deze afdelingen nog geen specifieke consequenties op de huisvesting. In het inrichtingsplan is al bepaald is welke locaties behouden blijven en welke locaties gesloten gaan worden en de invoering van de CCIII- wetgeving heeft daar geen verdere invloed op.

4.2 Werkproces LMIO

Het LMIO is een afdeling die in 2010 is gestart als een Pilot binnen de toenmalige regio Kennemerland. Vanwege een toenemende handel en fraude op internet en de ontoereikende informatiepositie bij zowel de politie als het Openbaar Ministerie werd er gezocht naar een afdeling die deze aangiftes kon verwerken, analyseren en clusteren. Het LMIO is geen operationele afdeling maar is verantwoordelijk voor de projectvoorbereiding. Hierbij veredelen ze de aangiftes en vorderen ze gegevens, stellen ze een proces- verbaal van relaas op en doen ze projectvoorstellen voor de eenheid die het uiteindelijke dossier in behandeling krijgt.

4.2.1. Huidig werkproces

Volgens een medeweker van het LMIO komen op jaarbasis 80 % van het totaal aantal meldingen van internetoplichting digitaal binnen bij de politie en 20 % persoonlijk via de bureau' s. Als we over aantallen spreken dan gaat het volgens het LMIO om 50.000 'digitale' meldingen. Van deze 50.000 meldingen zijn op dit moment zo' n 5000 meldingen niet als strafbaar feit te classificeren volgens de huidige wet- en regelgeving. Als de burger digitaal een melding heeft gemaakt van internetoplichting dan wordt deze eerst door medewerkers van DLOC gescreend en indien deze aan de vereisten voldoet in de BVH- omgeving van de Landelijke Eenheid ingevoerd.

Als de meldingen in BVH zijn ingevoerd zijn deze direct via BOSZ en Blueview te bezichtigen. Vanuit Blueview worden de meldingen geëxporteerd naar 7-11-12 . Dit gebeurt door middel van 7-11-12 . Tevens start er een traject waarbij er automatisch een mail verzonden wordt naar Marktplaats en de banken zodat zij op de hoogte worden gesteld van mogelijke verdachte transacties of handelingen.

De analisten van LMIO werken vervolgens met de gegevens die 7-11-12 geïmporteerd zijn met de intentie om een strafrechtelijk onderzoek te kunnen starten. Het systeem 7-11-12 maakt dat de analisten van het LMIO in de mogelijkheid zijn om entiteiten te clusteren. Als stelregel hanteert het LMIO dat er voor het starten van een onderzoek voldaan dient te worden aan een van de volgende drie criteria:

- Er dient per cluster sprake te zijn van 10 of meer aangiftes of
- Er dient per cluster een schadebedrag van minimaal 5000,00 euro te zijn of
- Er is sprake van een minderjarige verdachte

In de werkomschrijving geeft LMIO aan dat er in overleg in specifieke gevallen van deze criteria afgeweken kan worden, echter bij navraag blijkt dat hier amper sprake van is.

Indien er clusters worden gedetecteerd door de analisten dan vind er overleg plaats met een coördinerend Officier van Justitie om een strafrechtelijk onderzoek te starten. Bij goedkeuring worden de meldingen en aangiftes geformaliseerd en krijgen de aangevers een origineel exemplaar thuisgestuurd met het verzoek om deze ondertekend te retourneren. Het LMIO neemt de verantwoordelijkheid in deze en neemt contact op met de afdeling invoer van DLOC zodat de aangiftes uitgeprint en verzonden kunnen worden. Indien er besloten wordt dat het LMIO een aangifte niet in een onderzoek meeneemt dan worden de mensen in termijnen van een aantal weken tot een aantal maanden op de hoogte gehouden van de status van hun aangifte.

Het LMIO verzorgt het versturen van de originele aangifte naar de aangever met het verzoek om deze te ondertekenen en retour te zenden (Elenbaas, 2015). Enkele respondenten geven aan dat dit proces mogelijk versneld kan worden door de medewerkers van LMIO te autoriseren voor de BVH- omgeving van de Landelijke Eenheid zodat zij zelf in de mogelijkheid zijn om de aangiftes te printen echter de respondenten zijn zich er ook van bewust dat als deze taak bij het LMIO ligt dit een impact heeft op de totale bezetting van het personeel aldaar. Als het LMIO de getekende aangiftes ontvangen heeft en deze dus geformaliseerd is dan worden deze bij het dossier gevoegd.

De medewerkers van het LMIO doen ondertussen bij 7-12 Het geniet de voorkeur om ook van BVH gebruik te maken om bevindingen vast te leggen. Ondanks dat het LMIO zich niet profileert als operationele afdeling voeren zij dus wel gedeeltelijk operationele werkzaamheden uit ter voorbereiding van een onderzoeksdossier.

De werkvoorbereider van het LMIO stelt naar verloop van tijd een onderzoeksdossier samen waar het volgende in verwerkt is:

- PV- relaas
- Projectvoorstel
- Preweeg indicatie
- Aangiftes die ondertekend zijn geretourneerd
- Resultaten Blue View
- BOB- aanvragen
- Bewijsstukken
- Toelichtend schrijven (Fomutra)

Bij het samenstellen van het onderzoeksdossier voegen de medewerkers van het LMIO tevens een check uit in 7-11-12 te bekijken of aangiftes die door burgers persoonlijk aan een bureau zijn gedaan ook bij het betreffende onderzoek kunnen worden meegenomen. Indien een aangifte een match vertoont met het onderzoeksdossier zal deze er nog in worden opgenomen. Als het onderzoeksdossier is samengesteld wordt in overleg met de Officier van Justitie bekeken welke eenheid het betreffende onderzoek oppakt. Dit verdelingsmechanisme zal echter nader worden verklaard bij het hoofdstuk opsporing.

Het LMIO heeft veel goede contacten met de netwerkpartners zoals 7-12 . Deze instanties onderschrijven ook de functionaliteit van het LMIO in diverse brieven naar P. Zorko. Door deze goede contacten is het mogelijk dat het LMIO de aanvragen m.b.t. informatie in bulk aanlevert en binnen afzienbare tijd weer terug heeft. De tijdswinst die dit oplevert wordt duidelijk als een van de voordelen van

het LMIO gezien en respondenten binnen de opsporing geven aan dat deze procedures bij hun erg lang duren.

Tevens levert het LMIO een bijdrage aan het verwijderen van valse websites en web-shops. Via een Notice & TakeDown verzoek schrijft het LMIO diverse hostingsmaatschappijen aan met de mededeling dat er een strafbare en/of onrechtmatige inhoud op een site vermeld staat en verzoekt de hostingmaatschappij om de site offline te halen. In Nederland wordt er in 9 van de 10 keer goed gereageerd en sites direct verwijderd of ontoegankelijk gemaakt. Anno 2015 zijn er veel maatschappijen aangesloten bij deze NTD- gedragscode (https://ecp.nl/werkgroep-notice-and-takedown). In het buitenland ervaart het LMIO dat de verzoeken ook steeds vaker ingewilligd worden.

Volgens het LMIO wordt het Notice & TakeDown verzoek via bovenstaande werkwijze sneller toegepast dan als men de officiële weg middels een verzoek bij de Rechter Commissaris (RC) bewandeld. Indien een verzoek aan een hostingprovider niet gehonoreerd wordt, is het altijd nog mogelijk om dit via de RC af proberen te dwingen, echter volgens het LMIO duren deze procedures vaak te lang. In dat opzicht bezien biedt de aanpassing van dit artikel in de CCIII wetgeving dan ook geen verbetering op het gebied van online handelsfraude.

Het LMIO vermeld de bevindingen voornamelijk in SUMMIT zodat andere regio's dit ook digitaal kunnen lezen door middel van bevraging van de betreffende informatiesystemen. Tevens maakt LMIO per dossier, ongeacht welke eenheid het onderzoek draait en ongeacht het aantal aangiftes dat een dossier bevat, een (1) startregistratie met maatschappelijke klasse F600 (oplichting) in de BVH- omgeving van Noord- Holland op. In deze startregistratie vermeld men in de toelichting de namen van de aangevers, emailadressen en rekeningnummers en mogelijke andere relevante gegevens. Deze gegevens staan per categorie onder elkaar vermeld en leveren volgens diverse respondenten geen aanvullende informatie op, mede ook omdat de informatie niet in de daarvoor bestemde velden zijn verwerkt. Respondenten van gegevensbeheer geven tevens aan dat door deze startregistratie de cijfers een vertekend beeld opleveren en deze registraties ook weer in BOSZ gecoördineerd moeten worden. De respondenten pleiten allereerst voor het gebruik van de Maatschappelijke Klasse E53; assistentie ander korps. Dit zou met betrekking tot de coördinatie in BOSZ ook logischer zijn en cijfermatig voor COGNOS minder problemen opleveren v.w.b. dubbele tellingen.

De medewerkers van het LMIO stellen het dossier op door alle opgevraagde gegevens en bevindingen in een of meerdere mappen samen te voegen en te voorzien van een PV- Relaas. Hierdoor moet het voor de opsporingsafdeling die het onderzoek draaien in een oogopslag duidelijk worden wat de inhoud van het dossier is, welke handelingen al verricht zijn en welke werkzaamheden nog afgehandeld dienen te worden. Over het algemeen geven respondenten aan dat zij de opmaak van de dossiers van het LMIO heel overzichtelijk vinden en duidelijk is welke werkzaamheden er nog van ze verwacht worden. Helaas geven ook veel respondenten aan dat vanwege andere prioriteiten en capaciteitsgebrek de 'kant – en-klaar' aangeleverde dossiers van het LMIO niet direct opgepakt worden.

Een van de weinige punten van kritiek die respondenten binnen de opsporing aangeven is de onduidelijkheid van de gegevens met betrekking tot de katvangers. Omdat het LMIO bij de aanvraag naar NAW- gegevens bij 7-12 , is het lastig voor de opsporing om te bepalen om wie dit nu daadwerkelijk gaat. 7-12 is volgens de respondenten de grootste ontbrekende factor. Dit maakt dat het opsporingsproces naar hun idee een vertraging op loopt die niet noodzakelijk zou hoeven zijn.

Op dit moment zijn er in wisselende samenstellingen 7-12 werkzaam bij het LMIO, variërend in de functies van administratief ondersteunend medewerker tot en met analist. Continuïteit van personeel is evenals relevante ervaring en opleidingen niet geborgd (Tsjebanova, 2014). De afdeling is gevestigd in Heemskerk en per jaar worden er, afhankelijk van de grootte van de dossiers, ongeveer 80 onderzoekdossiers opgesteld. Met dit aantal zitten de medewerkers van het LMIO op het maximum aantal dossiers dat zij kunnen leveren op basis van de huidige personele capaciteit.

Van de 450.000 potentiele benadeelden geeft men aan dat men bij het LMIO op jaarbasis ongeveer 50.000 meldingen/aangiftes ontvangt. Dit betekent dat zo' n 11% van het potentieel aantal zaken maar bij de politie bekend is. Van deze 50.000 meldingen schat het LMIO dat 5000 meldingen niet onderzocht kunnen worden omdat het conform de huidige wet- en regelgeving geen strafbaar feit is. Van de overgebleven 45.000 aangiftes worden er, volgens het LMIO, naar schatting 12.500 aangiftes verwerkt in dossiers door het LMIO en de eenheden pakken zelf ook nog aangiftes op. In de tabel hieronder staat aangegeven hoeveel dossiers het LMIO aan elke Eenheid verstrekt.

Tabel 2: Dossiers online handelsfraude per eenheid in 2013

Eenheid	Dossiers vanuit het LMIO
1. Noord Nederland	12
2. Oost- Nederland	8
3. Midden- Nederland	5
4. Noord Holland	6
5. Amsterdam	13
6. Haaglanden	6
7. Rotterdam	9
8. Zeeland & West-Brabant	3
9. Noord- Oost Brabant	11
10. Limburg	4
11. Totaal	77

(bron; QuickScan 2014)

De medewerkers van het LMIO zitten, volgens een respondent, qua verwerkingscapaciteit aan hun maximum. Het feit dat het LMIO niet in het inrichtingsplan is opgenomen is mogelijk een factor die nadelig kan werken voor de gewenste personeelsuitbreiding. Ook het feit dat het LMIO niet als operationele afdeling geclassificeerd wil worden kan nadelig zijn voor een eventuele uitbreiding. Wil men daadwerkelijk optimaal gebruik maken van de implementatie van de CCIII- wetgeving en conform de doelstellingen de burgers een antwoord kunnen geven dan zal er een oplossing moeten komen voor de behandeling van de, volgens ruwe schatting, 30.000 aangiftes waar op dit moment weinig tot niets mee gebeurd.

Omdat dit een erg groot aantal aangiftes betreft, is er een pilot binnen het LMIO gestart waarbij er getracht wordt om ook projectvoorstellen op te starten met 2 tot 9 aangiftes erin. Het LMIO probeert hiermee te bewerkstelligen dat niet alleen de 'top van de berg' opgepakt wordt. Helaas zorgt een combinatie van drukte door de huidige werkzaamheden op basis van de bestaande criteria en het gebrek aan personele capaciteiten ervoor dat de pilot niet van de grond komt.

4.2.2. Impact van de nieuwe CCIII wetgeving

Respondenten geven aan dat het mogelijk is dat het aantal aangiftes toe gaat nemen. Enerzijds zou dit verklaard kunnen worden doordat er meer benadeelden zijn en transacties via internet op steeds grotere schaal plaats gaan vinden. Anderzijds kan een verklaring voor het toenemende aantal aangiftes geboden worden in het gedeeltelijk opheffen van de discrepantie tussen het aantal meldingen dat het LMIO op jaarbasis binnen krijgt en de berekeningen van het aantal benadeelden door het CBS vanwege het feit dat de burgers naar aanleiding van de veranderde wetgeving andere adviezen krijgen.

Indien het aantal aangiftes, om welke reden dan ook, toeneemt, betekent dit dat het LMIO meer meldingen binnen krijgt die geclusterd en geanalyseerd dienen te worden. Tevens heeft dit tot gevolg dat er een kans is dat meer aangiftes aan de criteria van het LMIO gaan voldoen zodat er meer of grotere

dossiers gevormd kunnen worden. In elk scenario die een toename van het aantal aangiftes tot gevolg heeft is het noodzakelijk dat de personeelscapaciteit bij het LMIO toe gaat nemen.

Vermoedelijk zal een toename in de personele capaciteit niet de volledige werkdruk op kunnen vangen en dienen ook werkprocessen beter gestructureerd te worden echter indien men de werkzaamheden van het LMIO op korte termijn beter wil optimaliseren dan is een uitbreiding van het personeelsaanbod een zeer gewenste beslissing. Concrete aantallen kunnen wederom niet gegeven worden omdat het LMIO niet in het inrichtingsplan vermeld is maar een respondent van het LMIO geeft aan dat een minimum aantal van 9 medewerkers al erg welkom zou zijn.

Over het algemeen zijn de medewerkers van het LMIO goed geïnformeerd over de geldende wet- en regelgeving en werkprocedures. Omdat een kleine groep medewerkers in wisselende samenstellingen deel uitmaakt van het LMIO is het niet noodzakelijk om de medewerkers van extra opleidingen te voorzien. Specialistische kennis over het werkproces doet men vaak gelijktijdig met het uitvoeren van de werkzaamheden op. Voor zover nu bekend verandert ook de huisvesting van het LMIO niet en blijft men in Heemskerk gevestigd. De invoering van de CCIII-wetgeving lijkt dan ook binnen het werkproces op het LMIO weinig tot geen effect te hebben. Voor wat betreft de personele bezetting dient er zowel in de huidige situatie als bij een toename van het aantal aangiftes wel aanvulling noodzakelijk te zijn.

4.2.3 Implementatie

Omdat de CCIII- wetgeving amper invloed heeft op het werkproces van het LMIO zelf is er van implementatie nauwelijks sprake. Wel kan het LMIO, als landelijk coördinerende afdeling, proberen de overige afdelingen, met name die met de administratieve werkzaamheden geconfronteerd worden, ondersteunen in het zo efficiënt mogelijk te laten verlopen, structureren en indien nodig ontlasten van de werkzaamheden totdat er voor een ieder in elke eenheid een (1) uniforme werkwijze is. Een verhoging van de personeelscapaciteit is vermoedelijk in zowel de huidige situatie als de nieuwe situatie onvermijdelijk.

4.3 Werkproces Opsporing

4.3.1. Huidig werkproces

Op het moment dat het LMIO een dossier als projectvoorbereiding af heeft gerond word er in overleg met de cybercrime- officier besloten welke eenheid het betreffende onderzoek gaat doen. Als leidraad wordt hierbij het document ‘beslissingen recherche officieren ; Landelijk Meldpunt Internet Oplichting’ (2013) gebruikt. De uitgangspunten in dit document zijn bepalend welke eenheid het dossier ter afhandeling toegezonden krijgt. In eerste instantie is daarbij doorslaggevend in welke regio de verdachte(n) woonachtig is of zijn. Bij meerdere verdachten uit meerdere regio’s wordt het dossier verzonden naar de eenheid waarin de meeste verdachten woonachtig zijn. Indien er sprake is van een gelijk aantal verdachten in meerdere regio’s, een verdachte die niet in Nederland woonachtig is of een verdachte die geen vaste woon- of verblijfsplaats heeft, wordt de casus nader bekeken. De coördinerend officier van het LMIO bepaald vervolgens welke eenheid de afhandeling van het dossier oppakt.

In de meeste gevallen levert deze wijze van beoordeling welke eenheid het dossier oppakt geen problemen op. Een (1) van de respondenten geeft aan dat er echter wel uitzonderingen zijn waarin verdachten tijdens het voorbereidende onderzoek zijn verhuisd naar een andere regio en dat dit vervolgens problemen oplevert bij het geven van een motivatie naar de recherche waarom het onderzoek door hun eenheid gedraaid dient te worden.

Als er bepaald is welke eenheid het onderzoek draait dan stuurt het LMIO het dossier met het verzoek om het onderzoek op te pakken op naar het betreffende eenheid. In een aantal regio’s zijn er vaste

contactpersonen in de eenheid zelf of bij het Regionaal Informatie Knooppunt in de eenheid. Het LMIO verzoekt het RIK of de contactpersonen om het dossier, inclusief de onderliggende stukken zoals aangiftes, vorderingen, lijsten van katvangers en hun mogelijke aangiftes, door te geleiden naar de betreffende rechercheafdelingen binnen de eenheid en zorg te dragen voor de afhandeling van het dossier. Het LMIO beoogt, met het sturen van het dossier naar het RIK, voor elkaar te krijgen dat er op cijfermatig gebied een betere inzage in de problematiek van de online- handelsfraude komt. Het verkrijgen van een vast contactpersoon bij het RIK is volgens het LMIO een lastige kwestie omdat niemand verantwoordelijkheid wil dragen voor het dossier. Een respondent stelt echter vraagtekens bij het feit of het RIK wel de juiste afdeling is waar dit soort dossiers in eerste instantie naar verzonden moeten worden.

In de praktijk blijkt dat het RIK in niet alle gevallen het dossier over kan dragen bij de betreffende recherche- afdeling vanwege tegenstrijdige richtlijnen, capaciteitsgebrek of andere argumenten. Dit zorgt voor veel onduidelijkheid in de eenheden en tussen de diverse recherche-afdelingen en maakt dat de projectvoorstellen van LMIO niet opgepakt worden.

Om in veel gevallen discussie te voorkomen zijn er specifiek afspraken gemaakt. In een document van 7 februari 2014 opgesteld door het college van procureurs- generaal van het Openbaar Ministerie met het onderwerp ‘Regionale afspraken aanpak horizontale fraude 2014’ is gesteld dat op basis van landelijke afspraken met private partijen elke regio de prioriteit heeft om ten minste 15 zaken met het onderwerp internet gerelateerde fraude op te pakken. Het LMIO heeft daarbij nog specifiek aangegeven in het stuk ‘aanpak van internetoplichting door de politie’ van het ministerie van Veiligheid en Justitie (Tsjebanova, 2014) dat het hun voorkeur heeft om 11 eenvoudige zaken op Basisteamniveau aan te leveren, 3 middelzware zaken op het niveau van Districtsrecherche en 1 gecompliceerde zaak op het niveau van de Regionale Recherche.

Over het algemeen blijkt dat de eenheden voldoen aan het oppakken van het minimum aantal van 15 zaken. Nadere bevraging over dit onderwerp geeft echter weer dat er geen afbakening van het begrip ‘zaken’ bestaat. Hierdoor is het mogelijk dat een onderzoek met 1 aangever/ benadeelde als ‘zaak’ gezien kan worden maar ook een aangeleverd dossier vanuit het LMIO met minimaal 10 aangevers/ benadeelden. Doordat deze discrepantie optreedt met betrekking tot de begripsomschrijving van het woord ‘zaken’, is het voor de mensen van het LMIO of het RIK lastig om nieuwe onderzoeken aan te bieden of verwerkt te krijgen bij de betreffende afdelingen. De betreffende afdelingen geven hier volgens een aantal respondenten meerdere argumenten voor.

Respondenten geven aan dat de voorkeur van het LMIO om de zaken te verdelen over de diverse recherche- afdelingen in de praktijk moeilijk valt uit te voeren. Volgens deze respondenten levert het LMIO meestal dossiers aan waar minimaal 10 aangevers dan wel benadeelden in zitten. Sommige respondenten die betrokken zijn bij de recherche op Basisteamniveau (BR) geven aan dat dit soort dossiers niet bij hun thuishoren. Volgens hun is het in strijd met het Toewijzingskader opsporing (2013) waarin staat aangegeven dat het wijkteam alleen ‘enkelvoudige’ zaken op dient te pakken. Aangezien het LMIO over het algemeen zaken aanlevert die een stelselmatigheid bevatten wordt dit naast het gebrek aan capaciteit en de hoge administratieve lasten, die met het draaien van een onderzoek van online handelsfraude gepaard gaan, als reden aangegeven om dit soort onderzoeken niet op te hoeven pakken.

Respondenten vanuit de recherche op Basisteamniveau geven aan dat ze ervaren dat het LMIO nauwelijks begrip voor deze situatie toont, niet altijd bereid is om mee te denken naar oplossingen en alsnog verwacht dat de zaak gedraaid wordt. Respondenten geven aan dat hierdoor de motivatie om op Basisteamniveau dit soort de zaak op te pakken afneemt. LMIO geeft aan dat men het idee heeft dat dit soort argumenten als excuses worden gebruikt om dit soort zaken niet te hoeven draaien en de prioriteiten te verleggen. Respondenten geven aan dat de Districtsrecherches (DR) ook met capaciteitsproblematiek zitten wat ervoor zorgt dat zaken van het LMIO wel aangeleverd worden maar weinig prioriteit krijgen. Dit heeft tot gevolg dat aangeleverde dossiers onderin een kast belanden of helemaal niet behandeld worden.

Een ander discussiepunt is de wijze waarop de onderzoeken aangeboden dienen te worden bij Justitie. Als er bij een onderzoek van online handelsfraude sprake is van een zaaksofficier, wat volgens de gestelde afspraken altijd zo zou moeten zijn, dan kan het onderzoek op de reguliere wijze gedraaid worden. Respondenten geven aan dat er bij dossiers en onderzoeken over online handelsfraude echter niet altijd sprake is van een gespecialiseerde zaaksofficier conform de afspraken. Volgens respondenten gebeurt dit met name als een dossier op het basisteam aangeleverd wordt. Omdat er geen sprake is van een zaaksofficier is de huidige werkwijze dat ontboden verdachten, minimaal 7 dagen voor hun ontbiedingsdatum, aangemeld dienen te worden bij ZSM. Een beoordelaar van ZSM kan zich dan alvast inlezen op de zaak en een insteek bepalen. De vraag die men zich hierbij stelt is of men ZSM met dit soort, over het algemeen grote en gecompliceerde, zaken moet belasten. Omdat de werkwijzen hieromtrent in de diverse eenheden van elkaar verschillen is het wellicht raadzaam om ook hier eenduidigheid in te krijgen en een uniforme werkafspraak in te maken. Het LMIO geeft aan dat het de behandeling van dossiers via ZSM toe zou juichen, echter, dit dient dan wel goed met het OM geregeld te worden.

Ongeacht de werkwijzen van de diverse afdelingen blijkt de grootste problematiek, volgens de respondenten, te zitten in de administratieve lasten die gepaard gaan met het draaien van het opsporingsonderzoek. Hierbij valt te denken aan het (nogmaals) invoeren van alle aangevers/ benadeelden in BVH in de betreffende eenheid en de plicht om burgers op de hoogte te stellen over de voortgang van het onderzoek in combinatie met de beperkte personeelscapaciteit. 7-12

Vanwege de wens om een beter cijfermatig inzicht te krijgen in de afhandeling van zaken geeft 9 van het LMIO aan dat het volgens hun, alhoewel een veroordeling de voorkeur geniet, niet zozeer van belang is welke afdoening er in een zaak is maar dat er een afdoening is. Volgens het LMIO heeft de afdoening, of de afdoening nu een sepot betreft of een uitspraak met een veroordeling is, geen toegevoegde waarde voor het cijfermatige inzicht dat er een onderzoek heeft gedraaid.

Meerdere respondenten geven aan dat er in overleg met het OM uit de regio veelal bepaald wordt om de zaak op te leggen en uiteindelijk helemaal niet te behandelen. 7-12

De administratieve lasten die bij dit soort onderzoeken horen blijven echter bestaan en zijn dermate groot te noemen dat een verandering in de werkwijze geadviseerd wordt ondanks dat meerdere respondenten zich bewust zijn van het feit dat het OM naar aanleiding van dit besluit verplicht is om de aangevers/ benadeelden op de hoogte te stellen. Een omschrijving van de omvang van de administratieve lasten zal hieronder worden weergegeven.

ADMINISTRATIEVE LASTEN

Per 1 mei 2015 voeren de medewerkers van de afdeling DLOC van de Landelijke Eenheid de geselecteerde aangiftes die digitaal bij hun binnen komen in de BVH- omgeving van de Landelijke Eenheid in, ongeacht de pleegplaats van het delict. Dit proces is anders dan de werkwijze die in de rest van het land en o.a. voor het Landelijk Informatiecentrum Voertuigcriminaliteit (LIV) geldt, maar niet geheel onlogisch gezien de afgesproken doelstellingen van het LMIO. Op het moment van invoer is er

tevens een koppeling met diverse systemen 7-11-12 op basis waarvan het LMIO de clustering toepast.

Het LMIO verzorgt op basis van deze informatie een clustering en maakt de analyses en met behulp van deze analyse wordt een dossier samengesteld en een projectvoorstel geschreven dat aan een eenheid wordt aangeboden. Omdat dit dossier aan een andere eenheid wordt aangeboden dan de eenheid die de aangiftes invoert en er nog geen sprake is van een overkoepelende BVH- omgeving is het op dit moment noodzakelijk dat alle aangiftes in de betreffende eenheid die het onderzoek draait wederom ingevoerd worden. Dit heeft een dubbele hoeveelheid administratieve lasten tot gevolg omdat de gegevens van de aangevers inmiddels twee keer ingevoerd worden. Het invoeren van deze gegevens is tevens noodzakelijk omdat de 7-11-12 , weer ingesteld moet worden omdat 7-11-12 status bij de eerste invoer van de aangifte in de BVH-omgeving van de Landelijke Eenheid is afgewezen.

Men heeft in overleg met het LMIO besloten om 7-11-12 - status van de aangiftes bij de Landelijke Eenheid af te melden wegens 7-12-14 Tevens dient wellicht gekeken te worden naar een werkwijze voor de invoer van aangiftes die meer samenhangt met de werkwijze van het Landelijk Informatiecentrum Voertuigcriminaliteit (LIV). 7-12-14

7-12-14

In de praktijk leidt de huidige werkwijze tot een situatie waarbij de meldingen die door DLOC als aangifte behandeld zullen worden twee maal ingevoerd worden door diverse eenheden, namelijk allereerst door de Landelijke Eenheid bij de aangifte en vervolgens door de betreffende eenheid die het onderzoek gaat draaien. Het LMIO voorziet hier geen problemen omdat dit immers nu ook al gebeurt. Respondenten geven aan dat indien men een administratieve lastenverlichting kan toepassen op dit front, de efficiëntie van het werkproces beter gestroomlijnd kan worden met als mogelijk gevolg dat er meer onderzoeken op het gebied van online handelsfraude gedraaid kunnen worden omdat de opsporingsafdelingen zich daadwerkelijk met opsporing bezig kunnen houden en minder met administratieve ‘randzaken’. Het LMIO zou hier mogelijk , alhoewel men aangeeft dit niet te ambiëren, een grotere coördinerende taak in kunnen krijgen. Het feit dat het LMIO vernomen heeft dat de diverse BVH- omgevingen van de eenheden in januari 2016 tot een (1) BVH- omgeving samen vloeit waardoor zij aangeven dat zij de noodzaak tot het aanpassen van deze werkwijze niet zien, spreken diverse respondenten tegen. Meerdere respondenten

geven aan dat er niet tot nauwelijks meer geïnvesteerd gaat worden in het BVH- systeem en dat een samensmelting van de diverse BVH- omgeving per 1 januari 2016 al helemaal niet realistisch is.

Respondenten van gegevensbeheer geven aan dat de bovenstaande werkwijze tevens een vertekend beeld op gaat leveren voor de cijfers vanwege dubbele invoer. Daarbij kaarten zij aan dat het programma 7-12-14

Respondenten geven als oplossing aan dat het mogelijk moet zijn om het LMIO een grotere coördinerende rol te geven waarbij men zelf de regie over de onderzoeken houdt en alleen de verhoren uitbesteedt aan de betreffende eenheden. In deze gevallen hoeft men alleen de incidentcode ‘verzoek aan ander korps’ (E53) te gebruiken en is de mogelijkheid tot de invoer van dubbele cijfers tot een minimum beperkt. Problematiek die men hierbij mogelijk ondervind is dat het LMIO verantwoordelijk wordt gemaakt voor een dossier en dat het onduidelijk blijft welk parket de zaak op zich neemt. Wellicht is het een mogelijkheid dat diverse betrokken afdelingen wel gaan bekijken wat de mogelijkheden hieromtrent zijn zodat in ieder geval de dubbele invoer van gegevens zo veel mogelijk voorkomen kan worden. Ook de optie tot een specialistische afdeling op het gebied van online handelsfraude die de werkzaamheden van advisering tot en met opsporing verricht, behoort volgens de respondenten tot de mogelijkheden.

INDIVIDUELE AANGIFTE EN BIJBEHOREND ONDERZOEK

Buiten de mogelijkheid dat het LMIO dossiers aanlevert is er nog een tweede manier waarop onderzoeken met betrekking tot internetoplichting opgepakt worden. Indien een burger aan een bureau persoonlijk aangifte heeft gedaan dan komt het voor dat deze zaken door de Coördinator werkProcessen (COP) uitgezet wordt bij een verbalisant van het Basisteam die het onderzoek naar de individuele aangifte moet gaan uitvoeren. Mogelijk dat deze aangifte onderdeel van een groter onderzoek is dat bij het LMIO wordt gedraaid. Indien de betreffende verbalisant of de Coördinator niet in BlueView kijkt, of de mogelijkheid heeft in BlueView te kijken, dan bestaat de kans dat er dubbel werk wordt verricht.
Aangezien een individueel onderzoek als 1 van de 15 beschouwd kan worden, kan dit mogelijk als reden worden aangevoerd waarmee eenheden al snel kunnen aangeven dat zij aan de gestelde verplichtingen van het uitvoeren van 15 onderzoeken op het gebied van internet, zoals gesteld door de Procureurs-Generaal van het Openbaar Ministerie (2014), hebben voldaan.
Ook hier geven respondenten aan dat het raadzaam is dat er nogmaals goed gecommuniceerd wordt over een uniforme werkwijze voor elke eenheid die bij elke aangifte online handelsfraude toegepast kan worden.

4.3.2. Impact van de nieuwe CCIII wetgeving

Het primaire artikel dat tot op heden over het algemeen ten laste wordt gelegd is het artikel oplichting in de zin van artikel 326 Sr.

326 SR: Oplichting; Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

Zowel in de memorie van toelichting (2014) als diverse respondenten geven aan dat het tot op heden in een aantal zaken lastig is om de oplichting te bewijzen. Het aanbieden van goederen of diensten via het internet, zonder de intentie tot leveren, levert niet zonder meer oplichting op. Het probleem zit hem, en dat blijkt ook uit jurisprudentie, 7-12

Tevens is het noodzakelijk dat in elke afzonderlijke casus de oplichting wordt bewezen. Aangezien een 7-12-14 Met de komst van het artikel 326d kan deze problematiek worden voorkomen.

Na de invoering van het artikel 326d verandert er voor de opsporing volgens diverse respondenten wel het een en ander alhoewel men aangeeft dat deze wijzigingen niet schokkend te noemen zijn. De administratieve lasten die gepaard gaan met dit soort onderzoeken blijft echter met de komst van het artikel 326d hoopt men voornamelijk dat de bewijslast vergemakkelijkt wordt.

Waar men, bij het primair ten laste leggen van artikel 326 Sr, in elke individuele aangifte/zaak moest bewijzen of aan de wettelijke bestanddelen is voldaan, hoeft dit volgens o.a. een oud medewerker van het LMIO met de komst van artikel 326d SR maar een keer te gebeuren. 7-12 Volgens respondenten van zowel het LMIO als daarbuiten is het bij de invoering van het wetsartikel 326d mogelijk om op het gebied van internetoplichting dit artikel primair ten laste te leggen in plaats van 326 Sr.

Art 326d:

Hij, die een beroep of gewoonte maakt van het door middel van een geautomatiseerd netwerk te koop aanbieden van goederen of aanbieden van diensten, met het oogmerk om die goederen of diensten, na betaling, niet te leveren wordt, indien betaling is gevolgd, gestraft met een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vijfde categorie.

In dit artikel zitten een aantal bestanddelen, te weten; * Beroep op gewoonte maken van het door middel van een geautomatiseerd netwerk te koop aanbieden van goederen of diensten * Het oogmerk hebben om die goederen of diensten niet te leveren* Er dient sprake te zijn van een betaling.

In de gevallen van internetoplichting geven respondenten die met de opsporing zijn belast aan dat zaken na de wetswijziging veel beter te bewijzen zijn. De onderzoeken die men via het LMIO aangeleverd krijgt, hebben al een voorselectie ondergaan. In de onderzoeken is er concreet vastgesteld dat er sprake is van goederen of diensten die via een geautomatiseerd netwerk aangeboden zijn. Ook is er in deze gevallen sprake van een betaling aan de betreffende verkoper. De aangever/ benadeelde wordt namelijk tijdens het aangifteproces ook verzocht om een kopie van het bankafschrift bij te sluiten.

Respondenten uit de opsporing geven aan dat het voor hun met name noodzakelijk wordt om aan te kunnen tonen dat er sprake is ‘van het maken van een beroep of gewoonte van het aanbieden van goederen of diensten via geautomatiseerde netwerken’ en ‘dat er een oogmerk was om die goederen of diensten niet te leveren’. Aangezien het grootste gedeelte van de dossiers die het LMIO aanlevert 10 of meer aangevers/ benadeelden hebben, voorzien zij met het aantonen van het beroep of gewoonte maken verder geen problemen. Het Openbaar Ministerie hanteert volgens diverse jurisprudentie (www.jure.nl) bij het beroep of gewoonte maken de volgende standaard: ‘een meervoud van op zichzelf staande handelingen’. Indien deze standaard toegepast wordt bij internetoplichting geeft dit volgens respondenten geen problemen en zullen dit soort zaken in de toekomst makkelijker te bewijzen zijn dan met de huidige wet- en regelgeving.

Het aantonen van het oogmerk om de goederen of diensten niet te leveren zal de uitdaging in het opsporingsonderzoek blijken te worden. Een kanttekening over hoe de rechters dit bij het aanbieden van dit soort zaken gaan interpreteren valt niet te maken en in de beoordeling van de impact van de wetgeving kan daar nog niet op worden vooruitgelopen.

4.3.3 Implementatie

Uit bovenstaande blijkt dat respondenten in de opsporing positief staan tegenover het gebruik van 326d Sr en subsidiair 326 Sr. Wel maken respondenten de kanttekening dat afspraken en afwegingen die aan het begin worden gemaakt over de werkprocessen van invloed zijn op het aanbod van en de mogelijkheid tot uitvoering van het aantal onderzoeken. Het artikel 326d in combinatie met deze afwegingen kan als mogelijke consequentie hebben dat er een groter aanbod aan onderzoeken van internetoplichting aan de opsporing aangeboden gaat worden in de toekomst, omdat meer zaken beter bewijsbaar zijn. Men kan er zeker van uitgaan dat het aanbod van onderzoeken groter wordt als de pilot binnen het LMIO, zoals het draaien van de onderzoeken met 2-10 aangevers, ook wordt meegenomen.

Diverse respondenten binnen de opsporing geven aan dat erop dit moment al een gebrek aan personeelscapaciteit is om de huidige werklast te kunnen verwerken. Indien het aanbod van het aantal onderzoeken toe zal nemen, zal dit tot gevolg hebben dat veel van deze onderzoeken niet gedraaid kunnen worden. Wil men daadwerkelijk een goed antwoord aan de burger kunnen bieden dan is het noodzakelijk dat de opsporingsafdelingen die belast zijn of wellicht worden met dit soort onderzoeken uitgebreid worden. Het specifieke aantal fte's dat nodig is om gevolg te kunnen geven aan het draaien van dit soort onderzoeken is per eenheid vanwege het aanbod van dossiers verschillend. Een concreet aantal valt dus niet te geven, echter de ervaring leert op basis van alleen al de huidige situatie dat het aantal medewerkers binnen de opsporing kwantitatief onvoldoende is om het volledige aanbod van onderzoeken m.b.t. online handelsfraude te kunnen verwerken.

Elke eenheid is op dit moment zijn eigen inrichtingsplan aan het opstellen waardoor het mogelijk is dat personen herplaatst worden. Op dit moment is er nog geen volledige inzage en overzicht van de diverse inrichtingsplannen en bijbehorende fte's in de betreffende eenheden. Pas indien dit traject is afgerond is het mogelijk om op basis van een inventarisatie een inschatting te maken hoeveel personeel beschikbaar is of kan worden gesteld voor de afhandeling van onderzoeken m.b.t. online handelsfraude. Ten aanzien van de huidige situatie is een vermeerdering van de personeelscapaciteit op het gebied van de opsporing absoluut gewenst zoals ook al eerder is aangegeven in de QuickScan (2014) echter vreest men ook dat men een eventuele toename in het aantal onderzoeken niet meer alleen op basis van capaciteit op kan vangen. Een positief advies voor een efficiëntere verwerking en daarmee dus een noodzakelijke verandering in het (administratieve deel van het) werkproces om aan de vraag te kunnen voldoen en de doelstellingen te kunnen behalen is dan ook gepast.

Respondenten uit de eenheden en binnen LMIO hebben tevens geopperd dat het wellicht, vanwege een gebrek aan 'specialistische' kennis en kunde bij met name de medewerkers vanuit het wijkteam, wijsheid is om binnen een eenheid een afdeling op te richten welke zich in grote mate met dit soort specialistische zaken vanuit het LMIO bezig kan houden. Tevens geven sommige respondenten signalen af dat het wellicht voor het stroomlijnen en de effectiviteit van het werkproces binnen de politiesystemen beter is om van het LMIO een meer operationele afdeling te maken en deze volledig uit te breiden. Argumenten die voor laatstgenoemde situatie worden gegeven zijn dat er vanwege de informatievoorziening een centrale afdeling functioneler werkt. Tevens kan het grensoverschrijdende karakter bij eenheden van de gepleegde misdrijven hierdoor volgens respondenten functioneler aangepakt worden.

De kennis en kunde is bij het LMIO aanwezig en daar kan meer gebruik van worden gemaakt. Het LMIO heeft zeer goede contacten bij de netwerkpartners waardoor de snelheid van het verwerken van verzoeken door LMIO bij de 'partners' beter is dan de bij de contacten die de opsporingsafdelingen met

deze netwerkpartners hebben. Tevens zou het LMIO, omdat zij alles in eigen beheer houden, een verbeterde informatiepositie en daarbij ook een verbeterd overzicht krijgen over de feiten gerelateerd aan online handelsfraude. Dit zou mogelijk ook kunnen betekenen dat er eerder gesignaleerd kan worden dat criminelen hun werkwijze veranderen en het monitoren van zaken zal vermoedelijk efficiënter zijn omdat men alles in eigen beheer houdt. Omdat het LMIO aangeeft dat het over het algemeen deze meer operationele taakuitbreiding niet als positief ervaart zal hier verder door een onafhankelijke persoon of instantie bekeken moeten worden wat de mogelijkheden op dit gebied zijn.

Uiteraard zijn er ook mogelijke nadelen te bedenken bij het volledig centraliseren van een afdeling zoals het LMIO. Een mogelijk nadeel zou kunnen zijn dat de werkwijze van het aanbieden van onderzoeken bij justitie hierdoor verandert en mogelijk een parket met een overvloed van onderzoeken m.b.t. online handelsfraude te maken krijgt. Tevens zal de huisvesting tot een discussiepunt leiden omdat het LMIO qua verantwoordelijkheid onder de Landelijke Eenheid valt maar de huisvesting en het personeel/ personeelsbeleid van de eenheid Noord- Holland gebruikt. Een onderverdeling waarbij in elke eenheid een op LMIO ingerichte afdeling komt die alleen de opsporing doet is wellicht een reëlere optie maar gezien de status van de inrichtingsplannen op dit moment niet haalbaar.

Buiten het feit dat iedere verbalisant zelf op de hoogte dient te blijven van de geldende wet- en regelgeving en daar dus bij iedere medewerker een eigen verantwoordelijkheid ligt, is het ook in de opsporing noodzakelijk om top- down de communicatie over de aanpassing in de wetgeving in te zetten.

In ieder geval dienen de opsporingsafdelingen die onderzoeken van online handelsfraude verwerken op de hoogte te worden gesteld van deze aangepaste wetgeving. Via diverse kanalen zal dit aangeboden moeten worden zoals ook te lezen viel bij de Intake & Service. Het meest makkelijke medium dat daarbij gebruikt kan worden is het intranet van de diverse eenheden. De afdeling communicatie kan hier een goede ondersteuning in bieden door voor elke eenheid eenzelfde berichtgeving eruit te sturen.

Verder geven diverse respondenten aan dat het prettig is om via de ‘warme communicatie’ aan kennisoverdracht te doen. Deze wijze heeft de voorkeur boven het verstrekken van aanpassingen via de mail, alhoewel respondenten aangeven dat laatstgenoemde wijze van verspreiding wel een goede ondersteuning kan bieden. Als primaire overdrachtswijze heeft dit echter niet de voorkeur.

Leidinggevenden binnen de opsporing geven aan dat het prettig is om hun op de hoogte te stellen zodat zij dit met de medewerkers van de afdeling kunnen bespreken. Via de beleidsmedewerkers van het dienstverleningsconcept zou het mogelijk zijn om een vergadering te beleggen in de eenheden waar de benodigde leidinggevenden bij aanwezig zijn. Dit is een standaardprocedure dat nu al plaatsvind bij de introductie van andere wet- en regelgeving. Via dit netwerk kan gebruik gemaakt worden door tijdens zo’ n vergadering een aantal minuten tijd te vragen om de wetswijzigingen te introduceren. Via deze weg kunnen de betreffende leidinggevenden hun kennis, opgedaan tijdens zo’ n vergadering, implementeren in hun directe werkomgeving. Op deze wijze is het mogelijk om binnen een redelijk kort tijdsbestek een groot gedeelte van de medewerkers die met de wijziging van deze wetgeving geconfronteerd zullen worden op de hoogte te stellen.

Op basis van het gegevensbeheer verandert er ten opzichte van de huidige situatie weinig voor de medewerkers van de opsporing. Tot op heden blijft de situatie dat de aangiftes bij het ontvangen van het dossier alsnog in het BVH van de betreffende eenheid gezet dienen te worden zodat ook het opsporingsproces 7-11-12 verwerkt kan worden. In BVH dient, net zoals bij de Intake & Service, gebruik te worden gemaakt van een specifieke incidentcode/ maatschappelijke klasse die de internetoplichting voor artikel 326d weergeeft. Omdat dit echter al besproken is zal hier nu niet verder over worden uitgeweid.

5. Conclusie

In deze impactanalyse is getracht om een antwoord te formuleren op de onderzoeksvraag: ‘Wat is de impact van de invoering van de wijzigingen in de CCIII wetgeving op het gebied van online handelsfraude binnen de politie?‘.

De afgelopen jaren is er, volgens zowel het CBS als de politie, een stijgende lijn waargenomen in het aantal meldingen en aangiftes omtrent online handelsfraude. Waar het CBS heeft berekend dat er sprake is van 450.000 benadeelden komen er bij de politie 50.000 meldingen binnen. Bij de politie komt 80% van deze meldingen digitaal binnen via het Landelijk Meldpunt Internet Oplichting. Deze afdeling heeft dan ook een zeer grote coördinerende rol en houdt zich voornamelijk bezig met projectvoorbereiding van opsporingsonderzoeken.

Over het algemeen kan gesteld worden dat men goed op weg is met het vaststellen van een aanpak dat tot uiteindelijke doel heeft om de burgers in Nederland van een antwoord te kunnen voorzien en diverse netwerkpartners onderschrijven ook de hoge mate van functionaliteit van het LMIO. Een wijziging in de CCIII wetgeving kan echter volgens velen daadwerkelijk nog een extra bijdrage leveren aan de effectiviteit en efficiëntie in het gehele opsporingsproces. Met name de aanvulling van het artikel 326d:

‘Hij, die een beroep of een gewoonte maakt van het door middel van een geautomatiseerd werk te koop aanbieden van goederen of aanbieden van diensten met het oogmerk om die goederen of diensten na betaling niet te leveren wordt, indien betaling is gevolgd, gestraft met gevangenisstraf van ten hoogte vier jaren of een geldboete van de vijfde categorie’

wordt als functioneel gezien. Deze wetgeving kan er volgens respondenten toe bijdragen dat het makkelijker is om de bewijslast op basis van de gestelde wettelijke bestanddelen rond te krijgen. Het 7-12 wordt met het nieuwe wetsartikel vermeden en indien er aangetoond kan worden dat er geen sprake van een voorraad of bezit bij de verkoper dan is dit geldig dit voor alle zaken binnen het betreffende dossier. Binnen de opsporing en het LMIO ziet men het voordeel van deze wetgeving in. Beide afdelingen erkennen echter dat er op dit moment al te weinig personeelscapaciteit is om een optimale invulling te geven maar vermelden ook dat zij op dit moment nog niet in kunnen schatten hoe dat in de toekomst, met het oog op de reorganisatie en invulling van het inrichtingsplan, vorm krijgt. Wel geeft men binnen de opsporing aan dat het in ieder geval efficiënter zou zijn als ook een gedeelte van het werkproces aangepast kan worden zodat dubbele werkzaamheden worden voorkomen. Binnen het werkproces van het LMIO zal naar aanleiding van de aanpassing in de CCIII- wetgeving nauwelijks iets veranderen.

Binnen de afdelingen van advisering en intake voorziet men, buiten een mogelijke toename van het aantal aangiftes en adviesaanvragen, geen problemen mits de communicatie op adequate en eenduidige wijze verloopt. Volgens respondenten zijn de betreffende medewerk(st)ers goed op de hoogte van de huidige wet- en regelgeving en voorzien zij geen problemen met mogelijke wetswijzigingen.

Respondenten geven aan dat zij, doordat er nu minder zaken als ‘civiel’ afgedaan worden, verwachten dat er een toename in het aantal aangiftes op zal treden. Geen van de respondenten kan echter inschatten om welke hoeveelheden het hier gaat. Ook de afdelingen die met advisering en intake zijn belast zijn onderhevig aan de reorganisatie en de invulling van inrichtingsplan. Mede daardoor geven zij aan dat het lastig is om te bepalen wat de daadwerkelijke invloed op de personeelscapaciteit wordt.

Tevens houden zij rekening met het feit dat maar 20% van het totaal aantal aangiftes via deze afdelingen binnen komt en dat de mensen van o.a. het RSC de burger kunnen sturen met het advies om digitaal aangifte te doen. Wel dient er rekening te worden gehouden met het feit dat een stijgend aantal

meldingen en/of aangiftes een grotere administratieve belasting binnen de diverse afdelingen van de politie veroorzaakt. Een aanpassing in andere wetgeving kan mogelijk bijdragen aan een vermindering van deze administratieve lasten voor het personeel.

Over het algemeen kan er dus gesteld worden dat de impact van de wetgeving voornamelijk zal liggen op het mogelijk hogere aantal meldingen en aangiftes dat bij de politie aan de frontoffice binnen zal komen, met alle administratieve handelingen als gevolg. Binnen het LMIO zal de wetswijziging nauwelijks invloed hebben op de werkprocessen. Wel kan het LMIO geconfronteerd worden met een groter aanbod aan meldingen/aangiftes waardoor er nog meer dossiers samengesteld kunnen worden. De opsporingsafdelingen voorzien dat met de invoering van de genoemde wetswijziging het makkelijker wordt om de bewijslast rond te krijgen om zodoende tot een veroordeling te kunnen komen. Met een mogelijke toename in het aanbod van het aantal dossier nemen echter ook de administratieve lasten voor deze afdelingen toe. Of dit uiteindelijk tot een uitbreiding van de personeelscapaciteit en eventuele aanpassing in huisvesting zal leiden, dient te worden bezien na de reorganisatie en uitvoering van de inrichtingsplannen van de diverse eenheden.

6. Discussie

Aangezien de politieorganisatie in rap tempo aan verandering onderhevig is en de onderzoekstermijn op 1 juli 2015 is afgelopen, is het mogelijk dat bepaalde bevindingen uit dit onderzoek inmiddels gedateerd zijn. Er wordt dan ook verzocht om bij het lezen van dit document hiermee rekening te houden.

Ondanks dat uit dit onderzoek blijkt dat de impact van de CCIII- wetgeving op bepaalde punten mogelijk van invloed is, blijkt uit de gesprekken met respondenten dat in de huidige werkprocessen ook al aanpassingen geadviseerd worden. Respondenten vermelden deze aanpassingen vanuit het inzicht dat met een toenemend aantal meldingen/aangiftes dit niet alleen opgevangen kan worden door een uitbreiding van de personele inzet. Het verdient dan ook de aanbeveling om ervoor te zorgen dat de wetgeving op het gebied van digitaal aangifte doen aangepast wordt.

Indien het mogelijk is om de digitale aangiftes van online handelsfraude, net zoals bij o.a. diefstal fiets, automatisch na beoordeling verwerkt te krijgen in BVH dan scheelt dit medewerkers aan de frontoffice veel administratieve werkzaamheden. Bij het digitaal maken van een melding/ aangifte dient dit tot op heden nog handmatig in BVH ingevoerd te worden. Aangezien het CBS spreekt over 450.000 benadeelden en de politie jaarlijks 50.000 meldingen binnen krijgt spreken we hier over zeer grote hoeveelheden meldingen/ aangiftes die een grote administratieve belasting veroorzaken.

Een bijkomend aandachtspunt volgens respondenten is dat de eenheden nog elk een aparte BVH-omgeving hebben. Dit maakt dat werkzaamheden zoals het invoeren van aangiftes gebeurd in de eenheid waar de aangifte binnen komt, echter als een andere eenheid het onderzoek draait dan wordt de aangifte daar nogmaals ingevoerd. Het LMIO schrijft de projectvoorstellen, echter deze maakt daarvoor ook gebruik van een specifiek registratienummer. Respondenten geven aan dat dit veel tijd kost en mogelijk ook van invloed kan zijn op de cijfers. Daarbij kan 7-11-12 op deze wijze (on)bewust beïnvloed worden.

In de regio waar de aangifte in eerste instantie is ingevoerd, wordt de registratie volgens respondenten afgeboekt met de mededeling: geen opsporingsindicatie+ niet schokkend feit. Pas indien de betreffende eenheid die het onderzoek gaat draaien de zaak in BVH invoert gaat de doorlooptijd, die met het OM gecommuniceerd wordt, weer lopen. Buiten het feit dat het hierdoor dus eerder mogelijk is om dossiers kwijt te raken, levert dit mogelijk een discrepantie op tussen de mogelijke en daadwerkelijke behaalde resultaten en doorlooptijden. Aangezien de gegevens 7-12-14 Tevens is het daarbij wellicht een optie om te kijken naar een werkwijze waarbij de dubbele invoer van gegevens in BVH of Summit, en daarmee een extra administratieve belasting, voorkomen kan worden.

Respondenten geven aan dat de omvang van het aantal aangiftes omtrent online handelsfraude inmiddels zulke grote proporties aanneemt, en daarmee veel inzet van de huidige collega's vraagt, dat ze zich afvragen of het niet handig is om deze specifieke delict soort binnen een specifieke afdeling, vanaf de intake tot aan het aanbieden bij het OM, te behandelen. Respondenten geven aan dat dit mogelijk een specifieke afdeling binnen elke eenheid kan zijn, maar sommigen opperen ook een operationele uitbreiding van het LMIO als landelijke afdeling. Respondenten geven aan dat zij het idee hebben dat hiermee de kennis en kunde van de collega's optimaal benut wordt en dit tot een efficiënter en uniformer werkproces kan leiden. Daarbij is het mogelijk dat met een specifieke afdeling gericht op online handelsfraude de dossiers de prioriteit krijgen die ze behoren te krijgen. Respondenten zijn zich echter ook bewust van het feit dat dit voor het OM wellicht een lastige situatie creëert omdat dossiers niet bij een (1) parket aangemeld kunnen worden maar mogelijk dat ZSM bij de 'kleine' dossiers uitkomst kan bieden hierin. Ondanks dat het buiten de scope van dit onderzoek valt is het wellicht mogelijk om in het kader

van de reorganisatie en de inrichtingsplannen een overzicht te krijgen hoeveel personeel voor welke afdeling beschikbaar wordt gesteld en wat de mogelijkheden binnen deze plannen voor andere voorstellen zijn.

Tevens verdient het de aanbeveling voor wat betreft zowel de interne- als externe communicatie van de wetswijziging deze via een top-down methode te laten verlopen. Bijna iedere respondent binnen de politieorganisatie heeft aangegeven het prettig te vinden om via warme communicatie op de hoogte te worden gesteld, aangevuld met berichtgeving via de mail en naslagmogelijkheden op intranet.

Respondenten zijn zich bewust dat de externe communicatie naar burgers op eenduidige wijze dient te verlopen en dat dit mogelijk gevolgen heeft voor de advisering en het aantal meldingen/ aangiftes. Voorgesteld wordt om eerst de medewerkers goed op de hoogte te stellen van de betreffende materie voordat de burger geïnformeerd wordt, dit om te zorgen dat burgers optimaal geadviseerd kunnen worden en medewerkers niet voor verrassingen komen te staan. Het verwerven van een grotere bekendheid van (de werkzaamheden van) het LMIO kan hiermee samenhangen en kan zelfs een positieve bijdrage leveren aan de coördinerende rol van het LMIO.

7. Afkortingenlijst

AVS	Aangifte Volg Systeem
BOA	Buitengewoon Opsporing Ambtenaar
7-11-12	
BR	Basisteam Recherche
BVH	BedrijfsVoering Handhaving
CBS	Centraal Bureau Statistiek
7-11-12	
DLOC	Dienst Landelijk Operationeel Centrum
DR	Districtsrecherche
DVC	Dienst Verlening Concept
I&S	Intake & Service
LMIO	Landelijk meldpunt Internet Oplichting
LSCEC	Landelijk Service Centrum E- Crime
OIV	Operationele Informatie Verwerking
RSC	Regionaal Service Centrum
ZSM	Zorgvuldig, Snel en op Maat; samenwerkingsverband tussen Politie, OM, Reclassering, Slachtofferhulp en Raad voor de kinderbescherming.

8. Literatuurlijst

- Algera S. Leeftink, M. (2014) *Impactanalyse Computer Criminaliteit III, Deel II QuickScan Online Handelsfraude versie 1.0*, Driebergen: Nationale Politie
- Antwoorden op Kamervragen over het Jaarverslag 2013. (2014,06 juni). Geraadpleegd van file13 lp-v-j-0000005748.pdf op 3 februari 2015
- Bolhaar, H.J. (2014). *Regionale Afspraken aanpak horizontale fraude 2014.* Den Haag: Openbaar Ministerie; College van procureurs- generaal
- Dienst VerleningsConcept (mei 2012). Geraadpleegd via http://www.politie.nl/binaries/content/assets/politie/wob/00-korpsstaf/dienstverleningsconcept_def.pdf
- Elenbaas, N. (2015). *Afhandelen melding internetoplichting*. Driebergen: Nationale Politie
- Holst, L. (2014). *Landelijk Service Centrum e-Crime. Plan van aanpak*. Driebergen: Nationale Politie
- Holst, L. (2014). Rapport vooronderzoek Landelijk Servicecentrum e-Crime. Driebergen: Nationale Politie
- https://ecp.nl/werkgroep-notice-and-takedown
- http://jure.nl/een%20beroep%20of%20een%20gewoonte%20heeft%20gemaakt%20van%20het%20kopen%20van%20goederen%20met%20het%20oogmerk%20om%20zonder%20volledige%20betaling%20zich%20de%20beschikking%20over%20die%20goederen%20te%20verzekeren
- Kloosterman, R. (2014, 16 juni). Meer oplichting via internet, minder skimming. Geraadpleegd van http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2014/2014-4083-wm.htm
- Loerts, A. (2013). *Toewijzingskader opsporing; Werkafspraken voor onderscheid tussen ondermijning, HIC en VVC.* Haarlem; Politie Kennemerland
- Ministerie van Veiligheid en Justitie (2013) Wetswijziging en Memorie van Toelichting; wijziging van het wetboek van strafrecht en het wetboek van strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III); Den Haag
- Putte, van der J. (2013). Beslissingen recherche officieren, Landelijk Meldpunt Internet Oplichting
- Tsjebanova, V. (2014). *Aanpak van internetoplichting door de politie'.* Inspectieonderzoek naar een vorm van cybercrime. Den Haag; Ministerie van Veiligheid en Justitie

Van: 10.2.e
Verzonden: woensdag 10 augustus 2016 17:12
Aan: 10.2.e
CC: 10.2.e 10.2.e 10.2.e
Bijlagen: Bijlage 2.c - Concept aanbiedingsbrief Impactanalyse.doc

Deze versie is in de Stuurgrope CCIII van december 2015 behnadeld en goedgekeurd, gr 10.2.e

10.2.e
Projectleider

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl

Organisatieonderdeel I

POLITIE

Behandeld door
Functie
Postadres

Bezoekadres

Telefoon
E-mail

Retouradres(zichtbaar in venster van envelop)

Ons kenmerk Ons kenmerk
Uw kenmerk Uw kenmerk
In afschrift aan In afschrift aan
Datum
Bijlage(n) 0
Pagina 1

Onderwerp Impactanalyse Online Handelsfraude

12-14

Van: 10.2.e
Verzonden: woensdag 10 augustus 2016 17:48
Aan: 10.2.e
CC: 10.2.e 10.2.e 10.2.e
Onderwerp: FW: Aanbiedingsbrief Online Handelsfraude
Bijlagen: Impactanalyse Online Handelsfraude def..pdf; Aanbiedingsbrief Impactanalyse.doc

10.2.e,

Nu herinner ik me het weer, ik meen wegens het vertrek van 10.2.e heeft 10.2.e het project CCIII binnen de portefeuille onder zich gehad, vandaar de adressering.
Ik meen dat vanwege de ondertekening of een foutje, de brief met rapport zelfs twee keer is aangeboden, formeel aan de portefeuillehouder dus.
Die ondertekende exemplaren kan ik nou net niet vinden, die zitten in het archief bij 10.2.e en/of 10.2.e maaar voorlopig ben je voldoende geinformeerd hoop ik.

Als je nog wat nodig hebt of wat dan ook, hoor ik het

m.vr.gr , 10.2.

Dubbel. Zie doc 241 (ordner 1)

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

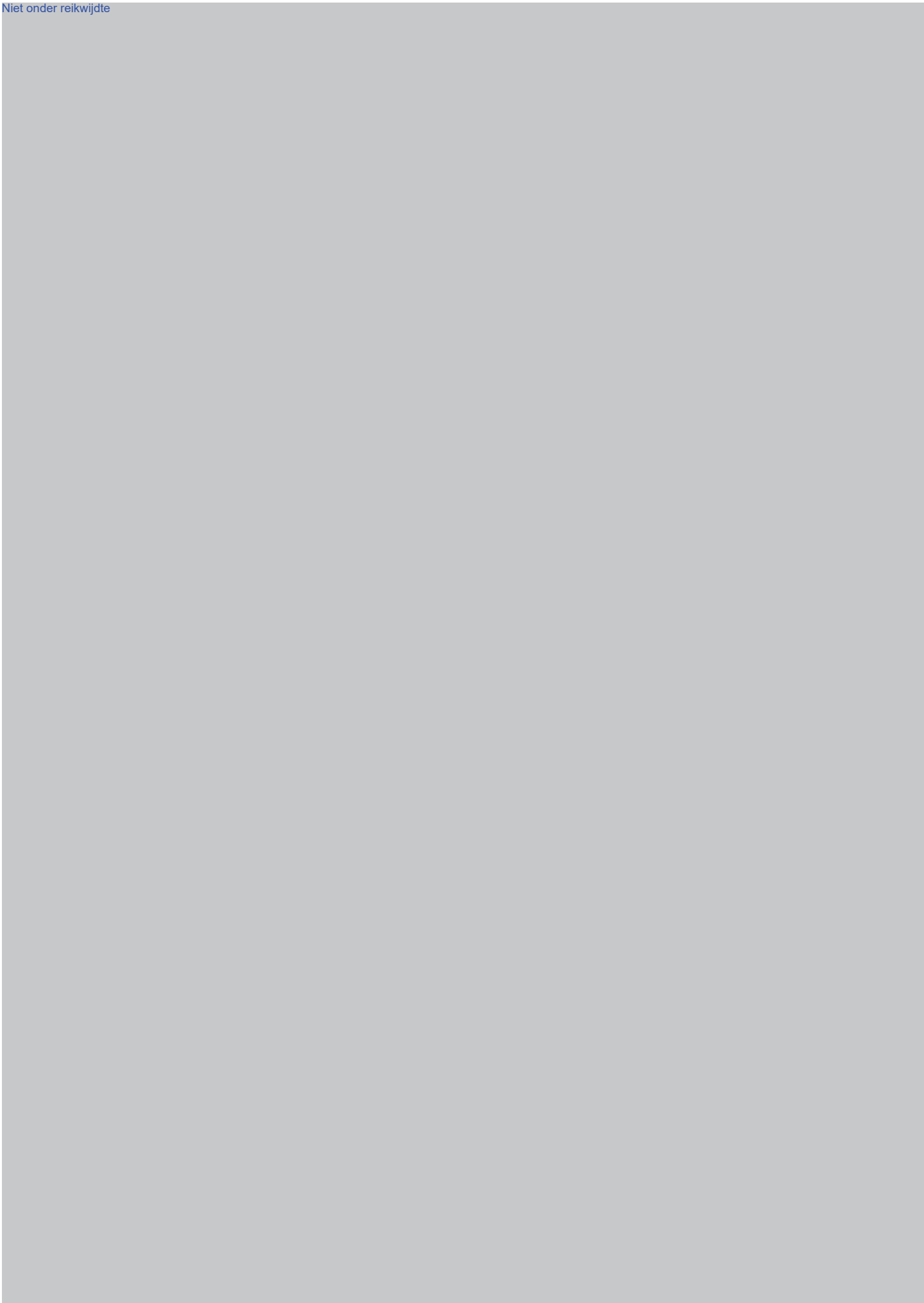
Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411

Is gelijk aan doc. 411


Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

From: 10.2.e
Sent: Wednesday, August 17, 2016 09:57 PM W. Europe Standard Time
To: 10.2.e
Subject: CCIII

Hallo 10.2.e

Zoals beloofd hier de stand van zaken voor CCIII op basis van parate kennis.

Belang van het project is groot voor de operatien. Niet alleen voor cybercrime, maar in principe voor alle vormen van gedigitaliseerde criminaliteit. In dit verband is ook CTER bv. zeer relevant. Dit zou een extra middel kunnen zijn om op te treden. Ook terroristen gebruiken steeds meer de digitale mogelijkheden.
Het is een bevoegdheid waar we als politie al lang op wachten en die we steeds harder nodig hebben omdat encryptie steeds verder toeneemt en dit op niet al te lange termijn feitelijk nog de enige manier is om dan op te kunnen treden.

Het gaat vooral om het voorbereiden van de nieuwe bevoegdheid om binnen te dringen in een geautomatiseerd werk (computer, server etc.). Dit ligt heel erg gevoelig bij de politiek, maar ook bij de ICT sector. Het is daarom van belang de bevoegdheid zorgvuldig uit te kunnen voeren en bv. ook forensisch correct. Er zal veel aandacht zijn voor ons optreden. We hebben er nog geen ervaring mee en ook de collega's die dit in de praktijk moeten doen moeten goed kunnen oefenen om te voorkomen dat ze fouten maken.

Het project, dat voor een groot deel een ICT project is (er moet een testomgeving wordt ingericht en getest wordt met software) is bezig met de voorbereiding, maar dit loop heel moeizaam met dienst ICT. Er zijn steeds wel uren toegekend in het portfolio, maar in de praktijk levert de dienst ICT niet wat is toegezegd. Vorige week hoorde ik dat dat 9 ermee is gestopt en dat de dozen onuitgepakt in de gang staan. Ook 9 gaf aan zorgen te hebben hierover.

We moeten ook steeds vechten om dit onderwerp op het portfolio te houden. Bij de vaststelling van het operationeel portfolio was het bijna gesneuveld omdat er nog geen datum van in werking treding van de wet was. Dat is hier niet relevant, want we hebben alle tijd nodig die we kunne krijgen om goed voorbereid te zijn. Als de ICT omgeving niet goed staat lopen we vertraging op in de voorbereiding.

Verder is het zo dat is uiterste noodgevallen de RC blijkbaar ook al eens opdracht heeft gegeven tot binnendringen (9). Deze infrastructuur is feitelijk dus al zo snel mogelijk nodig om ook in dit soort gevallen zorgvuldig te kunnen handelen.
Inge kan je hier alles over vertellen, want LR en DLOS zijn hierbij betrokken. Inge trekt dit CCIII project namens Theo vd Plas. 10.2.e is projectleider en kent alle details.

Dit gesprek is een mooie kans om de ontstane risicovolle situatie los te krijgen. Mijn advies en verzoek is om Inge en 10.2.e hierin vanuit het grote operationele belang te steunen en te helpen er weer schot in te krijgen.

Ik hoop dat dit voldoende beeld geeft om het gesprek te kunnen voeren. Inge en 10.2.e zullen de situatie waarschijnlijk toelichten, maar dan heb je vast een beeld.

Groet,
10.2.e

From 10.2.e @politie.nl>
Subject **RE: CCIII**
To 10.2.e @politie.nl>
Date 17 augustus 2016 22:35:38 CEST

Helder en henkenbaar, 10.2.e Ik doe er mijn voordeel mee. De bijeenkomst kwam voor mij wat verrassend oppoppen in mijn agenda en er was kennelijk niet vooraf advies gevraagd, vandaar de lastminute improvisatie. Niettemin bruikbaar, bedankt. Groet, Peije.

Van: 10.2.e
Verzonden: donderdag 25 augustus 2016 16:06
Aan: 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>; 10.2.e l@politie.nl>
Onderwerp: Concept PSD CCIII tbv Directie Operatien

Beste 10.2.e e.a.,

Bijgaand treffen jullie aan een bijgewerkte PSD CCIII (versie 0.3). Deze is opgesteld mede naar aanleiding van de opmerkingen die zijn gesteld tijdens het overleg tussen 10.2.e 10.2.e en 10.2.e

Graag maken we nog een afspraak met 10.2.e en/of 10.2.e om de lege plekken in de tabellen van de PDC ondersteuning op te vullen. Het traject met IM/IV loopt goed en wordt nader gespecificeerd.

Ik hoor graag wanneer dit zou kunnen. Ik ben zelf volgende week i.v.m. een dienstreis niet aanwezig, maar in de week van 5 september zijn 10.2.e en ik in staat om dit gesprek aan te gaan.

Daarnaast hoor ik natuurlijk graag of deze versie meer in lijn is met de verwachting. Opmerkingen en aanvullingen ontvang ik graag.

Met vriendelijke groet,
10.2.e

10.2.e
9
Politie | DLOS | ATOE | KLC | Project CCIII
Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl

Van: 10.2.e
Verzonden: maandag 29 augustus 2016 14:00
Aan: 10.2.e @klpd.politie.nl>
Onderwerp: RE: Concept PSD CCIII tbv Directie Operatien

10.2.e

De PSD zit er niet bij. Kun jij die alsnog sturen?

Dank,
10.2.e

Van: 10.2.e - BD/DRC/CV
Verzonden: dinsdag 30 augustus 2016 13:41
Aan: 10.2.e BD/DCS/ACSB; 10.2.e @politie.nl)'; '10.2.e @klpd.politie.nl)'; 10.2.e @om.nl)'; 10.2.e '; '10.2.e @mindef.nl'; '10.2.e @mindef.nl'; 10.2.e @minbzk.nl)'; 10.2.e . - BD/DGPOL/PBT/PT
CC: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
Onderwerp: Concept Kamerbrief onbekende kwetsbaarheden

Beste collega's,

Hopelijk hebben jullie allemaal een goede vakantie gehad. Bij deze stuur ik jullie de huidige versie van de concept-Kamerbrief over het gebruik van kwetsbaarheden. Ik ben voornemens deze morgen met EZ en BZ te delen.

Groet,
10.2.e

Van: 10.2.e @minvenj.nl>
Verzonden: dinsdag 30 augustus 2016 13:42
Aan: 10.2.e
Onderwerp: FW: Concept Kamerbrief onbekende kwetsbaarheden
Bijlagen: Conceptbrief kwetsbaarheden V30aug2016zt.docx

...verkeerde adres...

Zie voor definitieve versie doc 447

Zie voor definitieve versie doc 447

Zie voor definitieve versie doc 447

Zie voor definitieve versie doc 447

Zie voor definitieve versie doc 447

Zie voor definitieve versie doc 447

Van: 10.2.e
Verzonden: dinsdag 30 augustus 2016 15:34
Aan: 10.2.e .)
CC: 10.2.e
Onderwerp: RE: Concept PSD CCIII tbv Directie Operatien

10.2. sti,

We snapten al niet dat we niks terug hoorden, maar dat is dus fout gegaan.
Vandaag zou ik naar Warnsveld gaan, maar we zaten in wervingssessie voor lab CCIII, dus dat lukte niet e 10.2.e zit in Las Vegas.
Nou is het probleem dat ik wel over de conceptversie beschik, maar niet dit exemplaar wat in de bijlage had moeten zitten.
Ik zal vragen of 10.2.e dat uit LV kan regelen, anders krijg je het zsm, gr 10.2.e excuses

Het proces loopt overigens goed, we zijn met IM/IV al rond en HRM schiet ook al op,
Er volgt dus ook nog voor 15-9 een eindversie uiteraard

Van: 10.2.e
Verzonden: dinsdag 30 augustus 2016 22:50
Aan: 10.2.e @klpd.politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Concept PSD CCIII tbv Directie Operatien

Hoi 10.2.e

Maak je niet te druk. Ik dacht dat het handig was om hem vandaag te hebben bij die sessie. Heb hem niet acuut nodig hoor.
En fijn om te horen dat de afstemming goed loopt. Ik ben ook benieuwd hoe het gesprek met 10.2.e ea. Laatst ging.
Binnenkort maar weer even bellen.

Er is overigens morgen 10.00 eenzelfde sessie 9 als je aan wil sluiten. Geen probleem, gewoon gaan al het uitkomt. Ik heb 10.2.e ter info meegenomen in cc.

Groet,
10.2.e

From 10.2.e @klpd.politie.nl>
Subject **RE: Concept PSD CCIII tbv Directie Operatien**
To 10.2.e @politie.nl>
Date 31 augustus 2016 14:37:05 CEST

OK, thx

Agenda hier vol, we proberen er capaciteit bij te krijgen en dat is prio I voor CCIII.
12-14

Er zijn prio en urgency noodzakelijk op strategisch niveau

Alsnog de rapportage ingestuurd met begeleidende mail en wederom de uitnodiging langs te komen, ook 10.2.e . Was ook al naar 10.2.e na persoonlijk contact 9 .
Maar ze reageren niet,… wij gaan gewoon maar door, gr 10.2.e

Vanuit Las Vegas lukte het niet, dus volgende week stuurt 10.2.e de volgende versie, gr 10.2.e

Strategisch Beleidsplan Operatiën 2017-2021

Auteur: Directie Operatiën

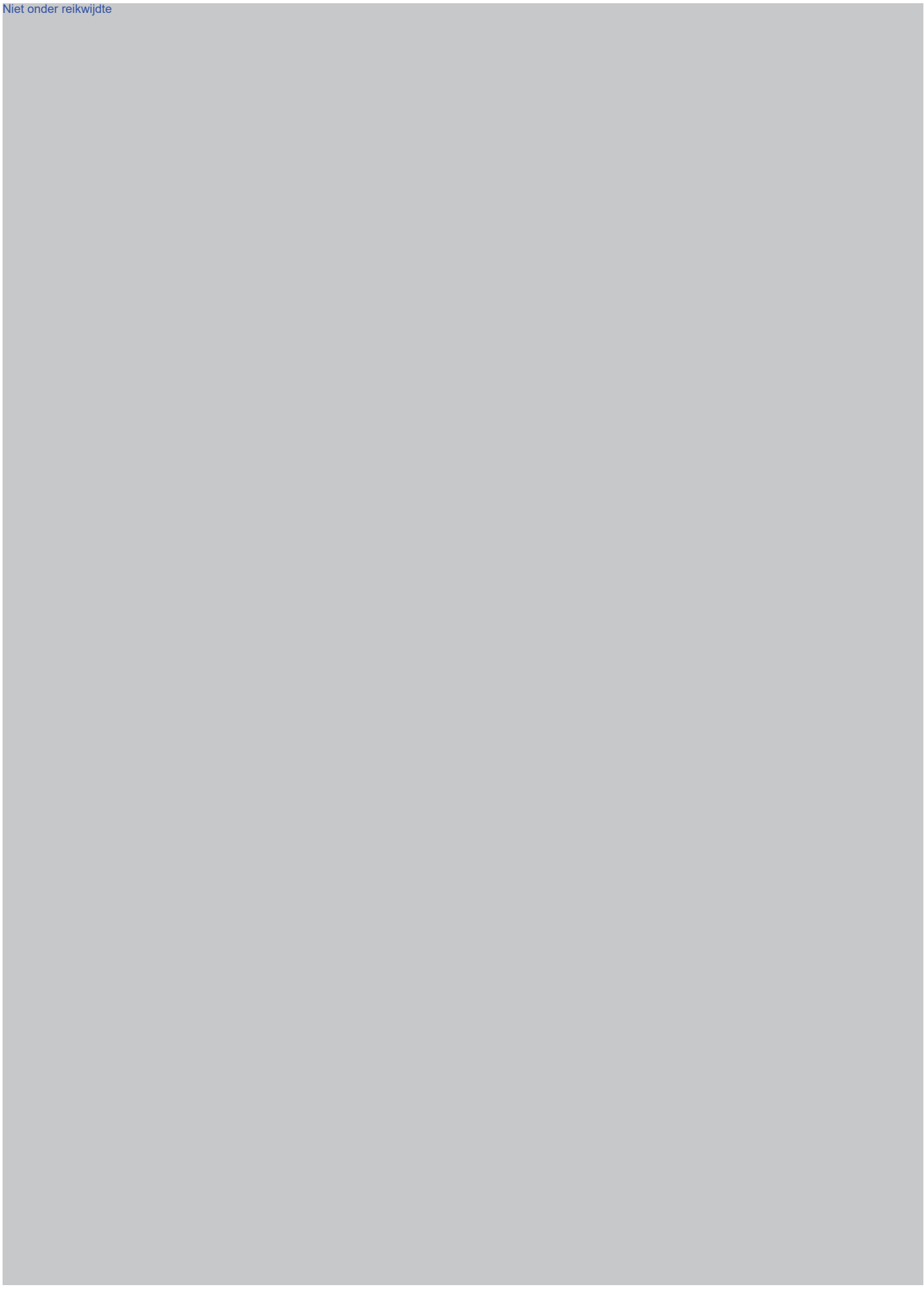
Status: vastgesteld

Versie 1.1

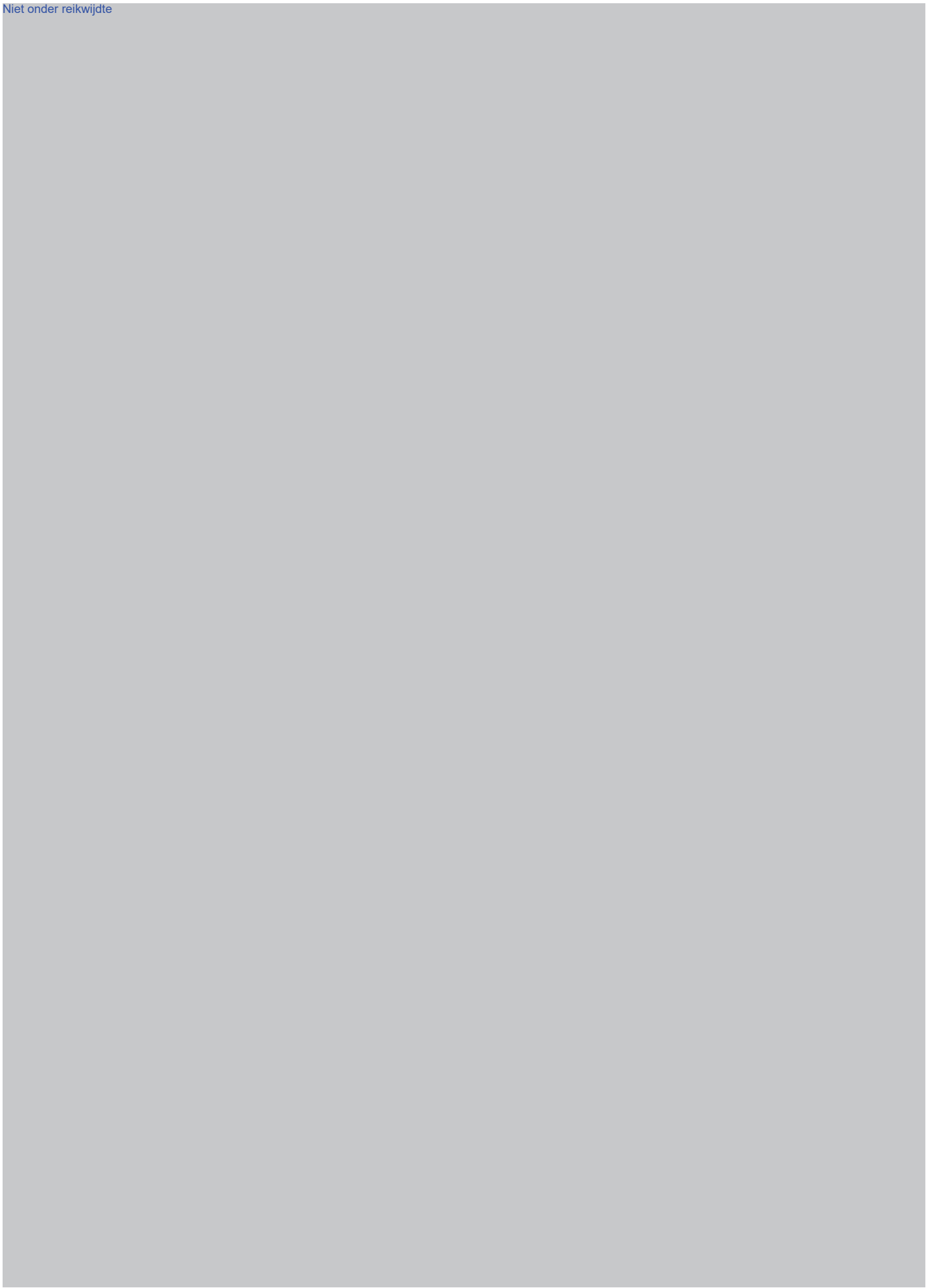
10-09-2016

Rubricering: Politie Intern

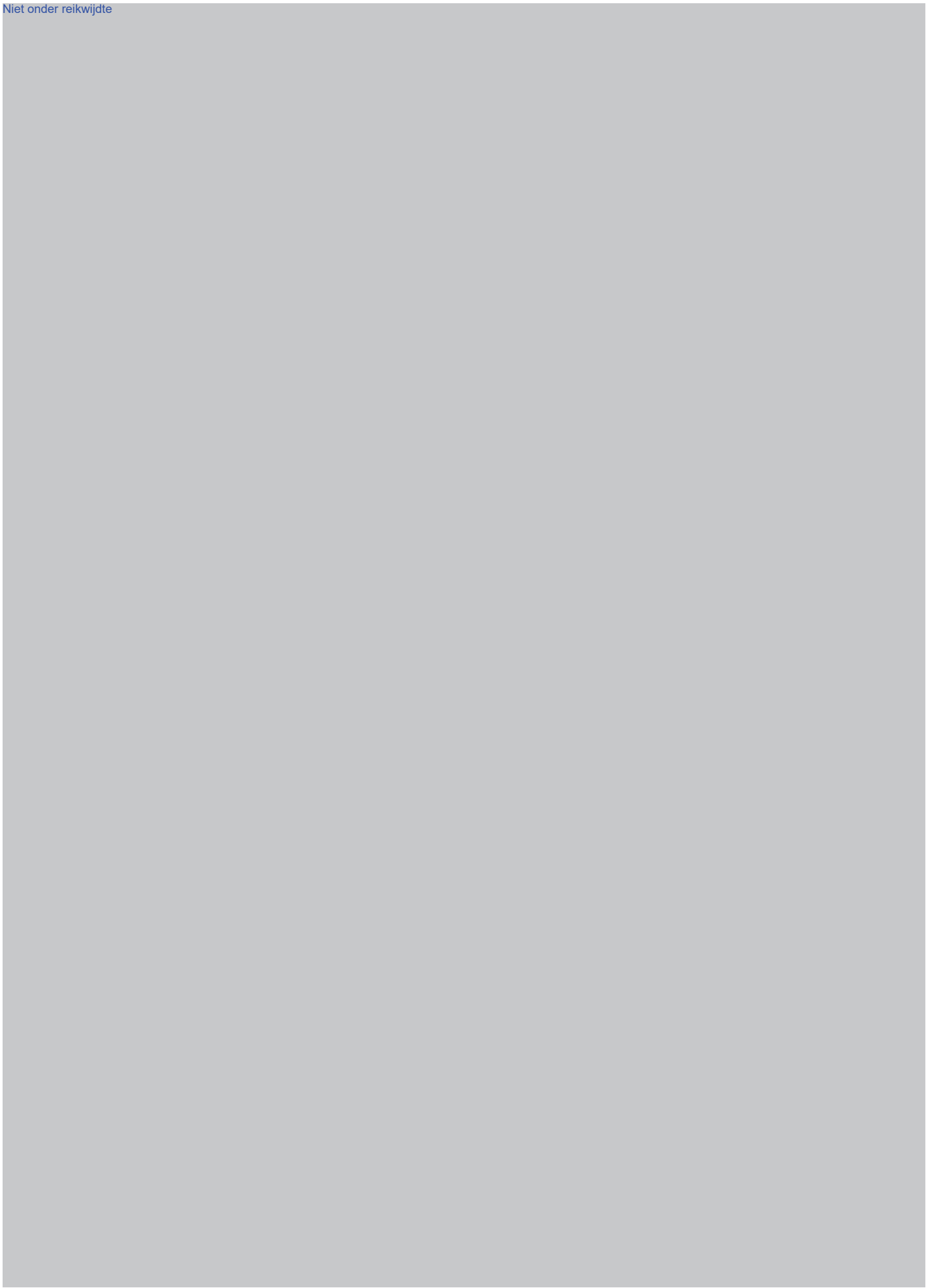
Niet onder reikwijdte



Niet onder reikwijdte



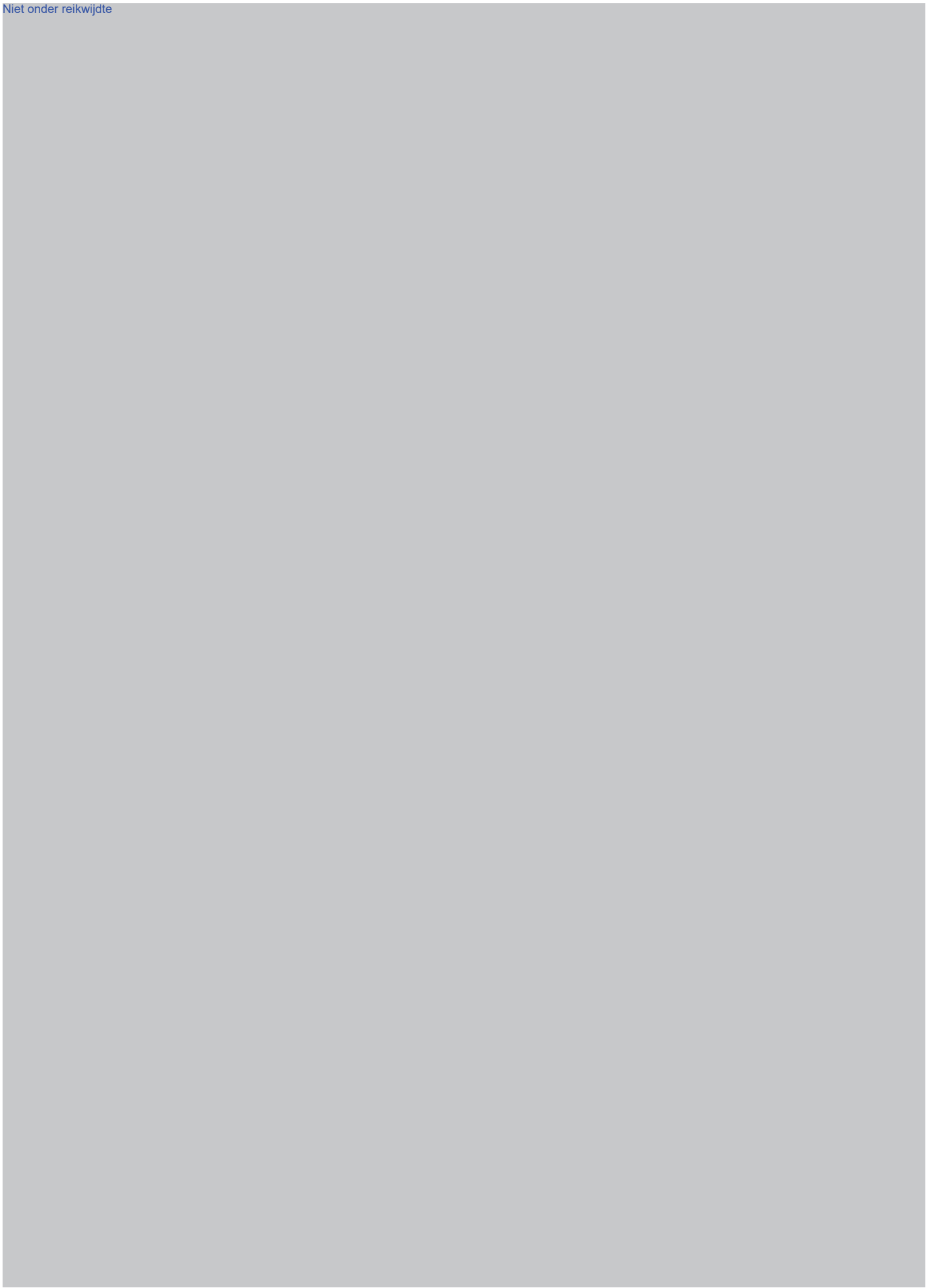
Niet onder reikwijdte



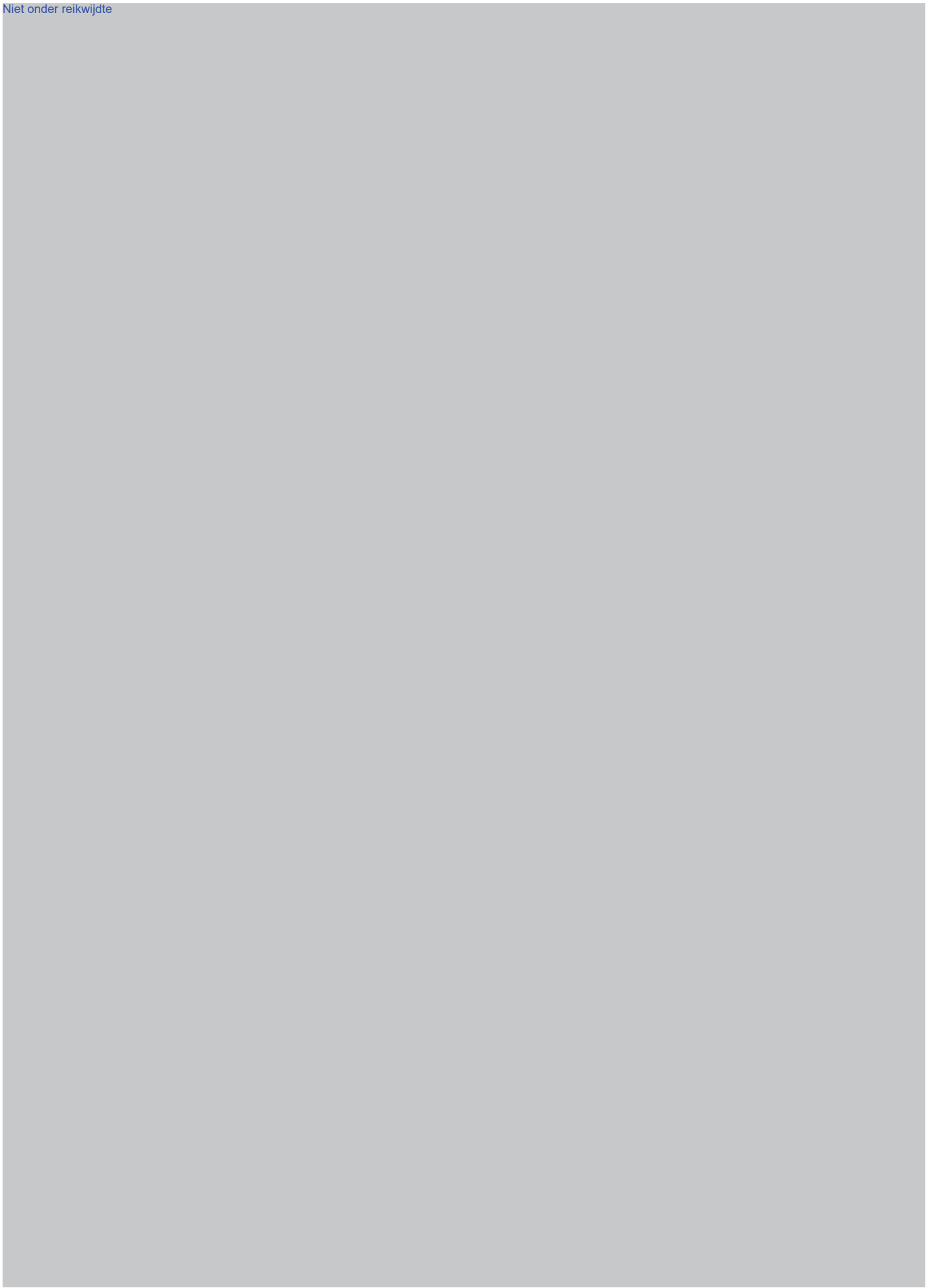
Niet onder reikwijdte

Niet onder reikwijdte

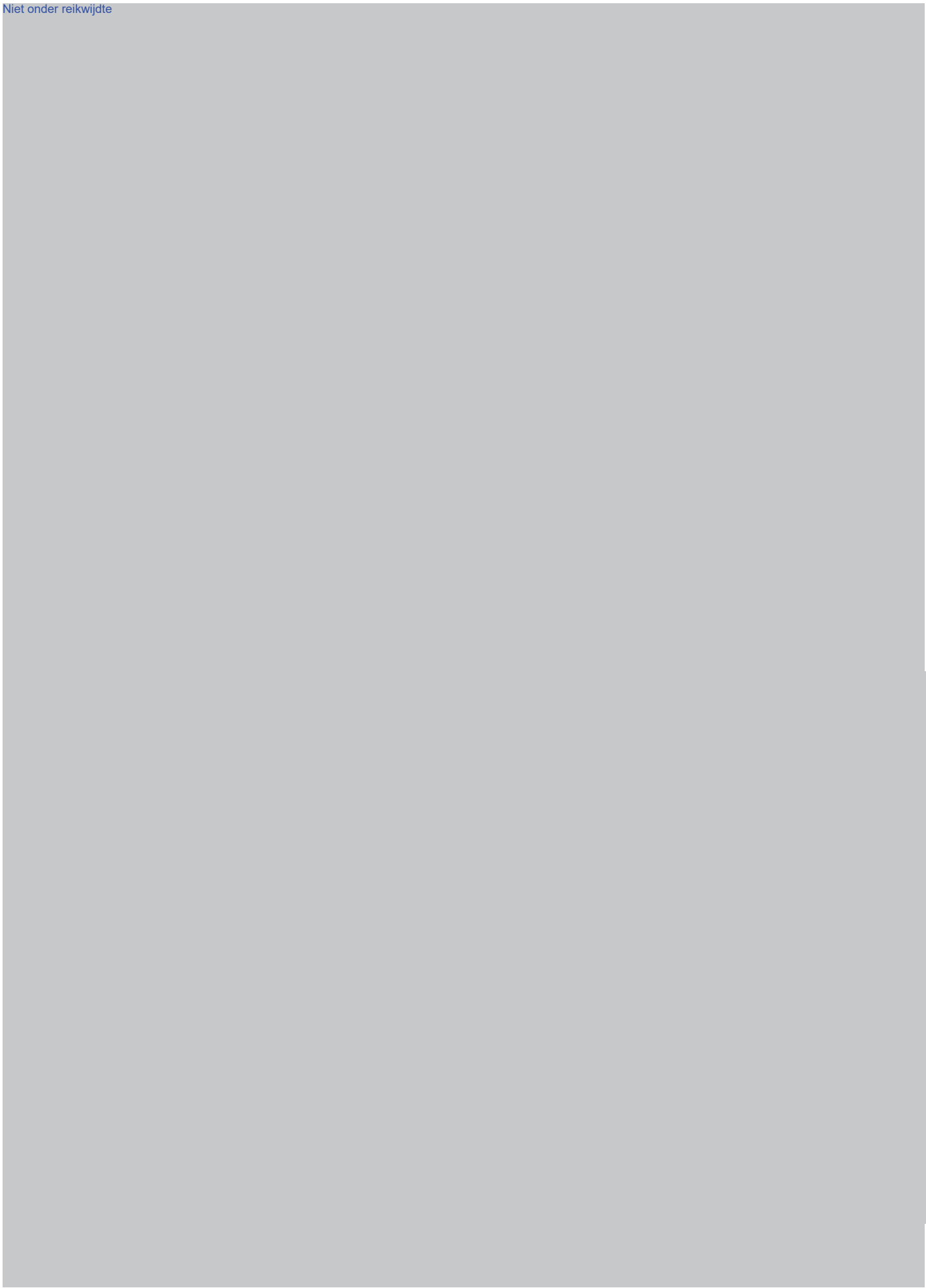
Niet onder reikwijdte



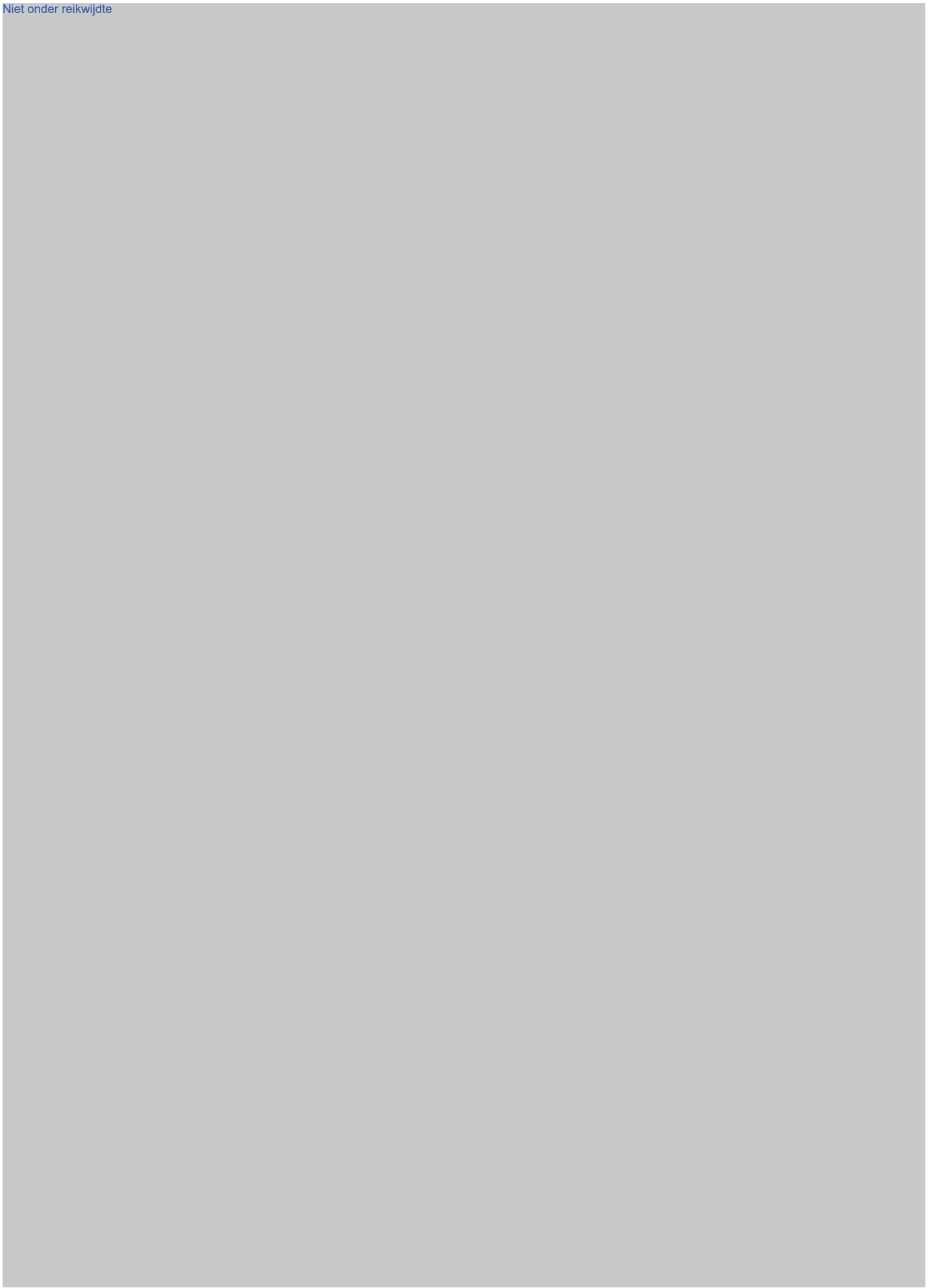
Niet onder reikwijdte



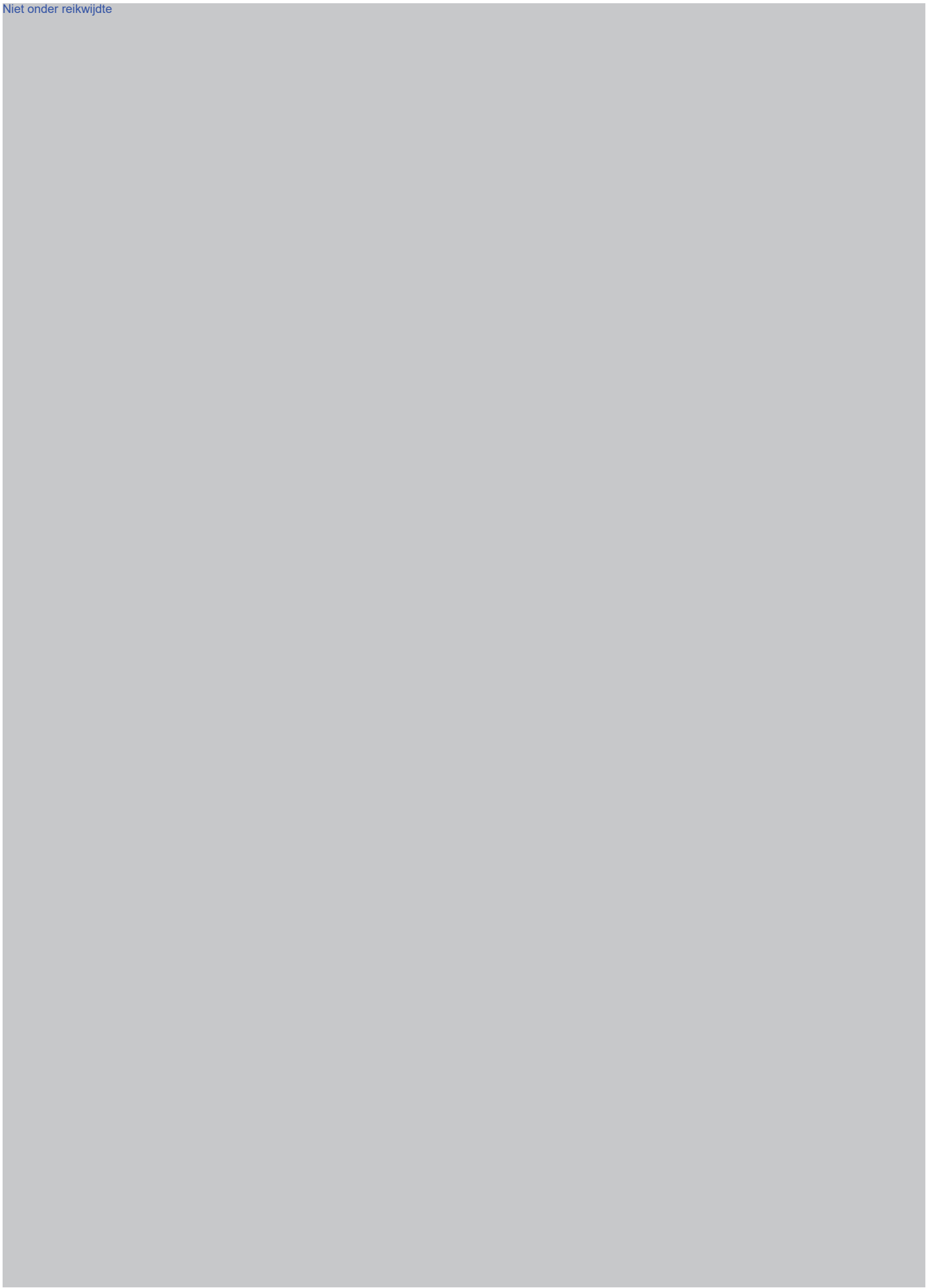
Niet onder reikwijdte



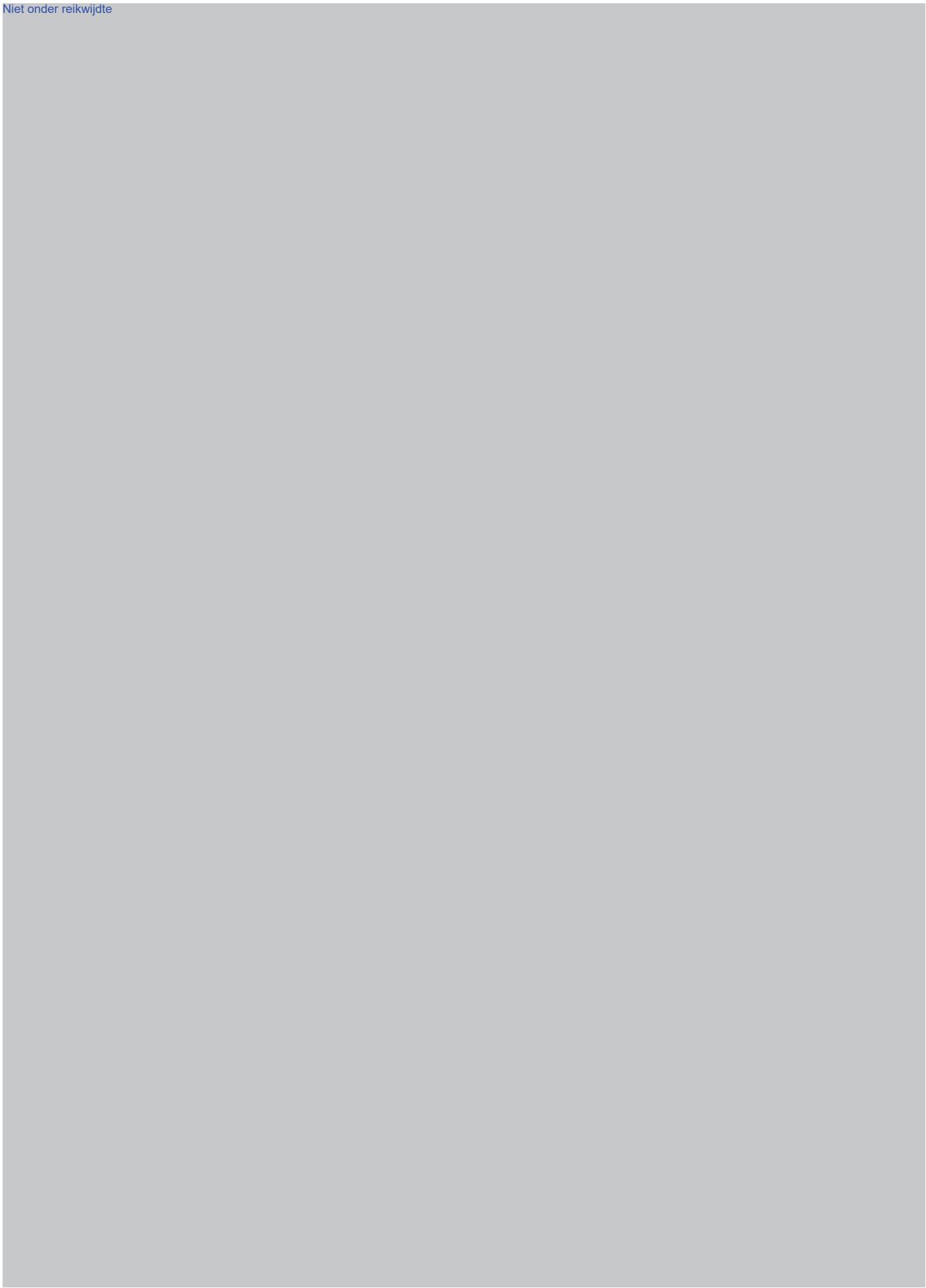
Niet onder reikwijdte



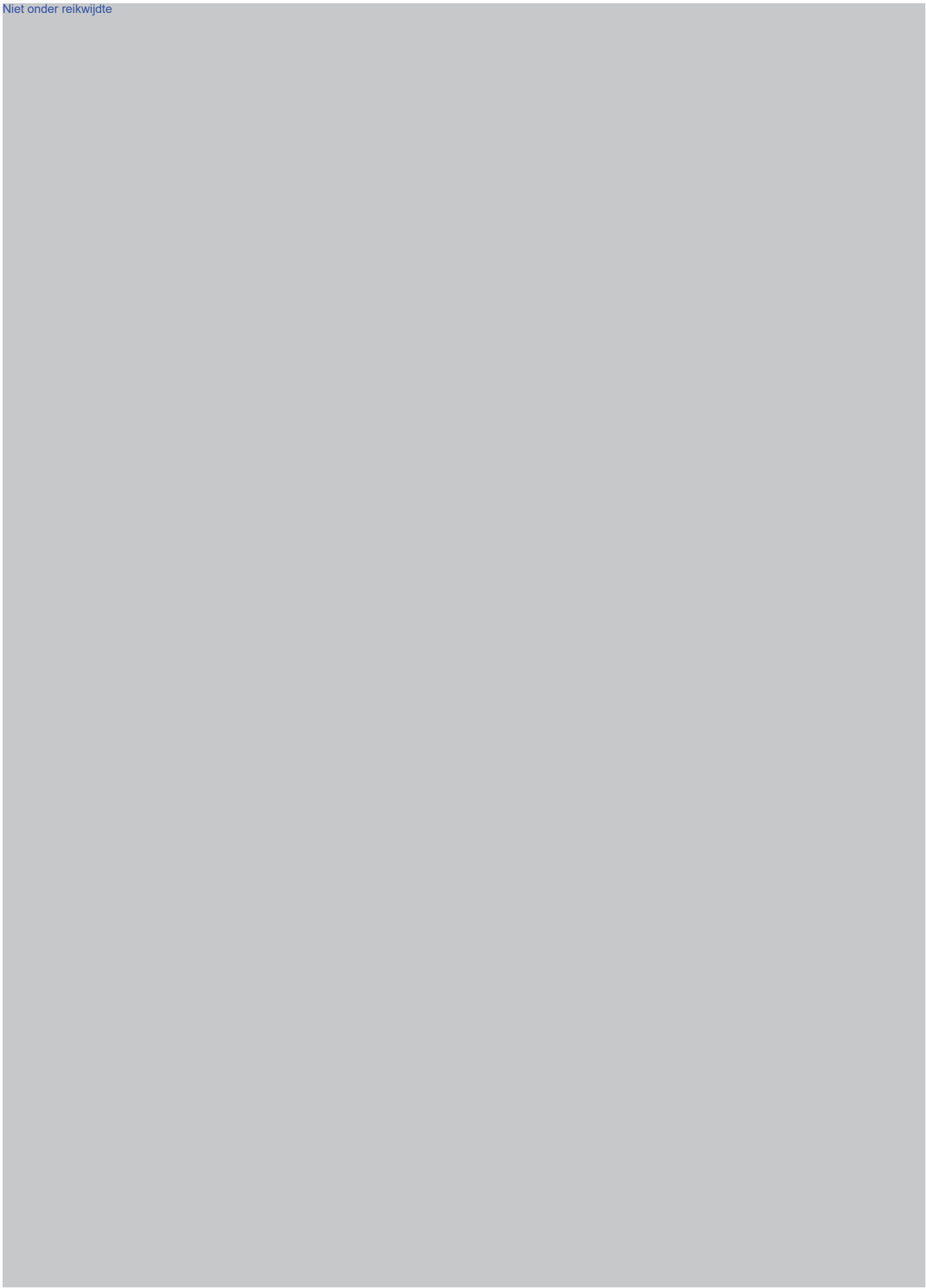
Niet onder reikwijdte



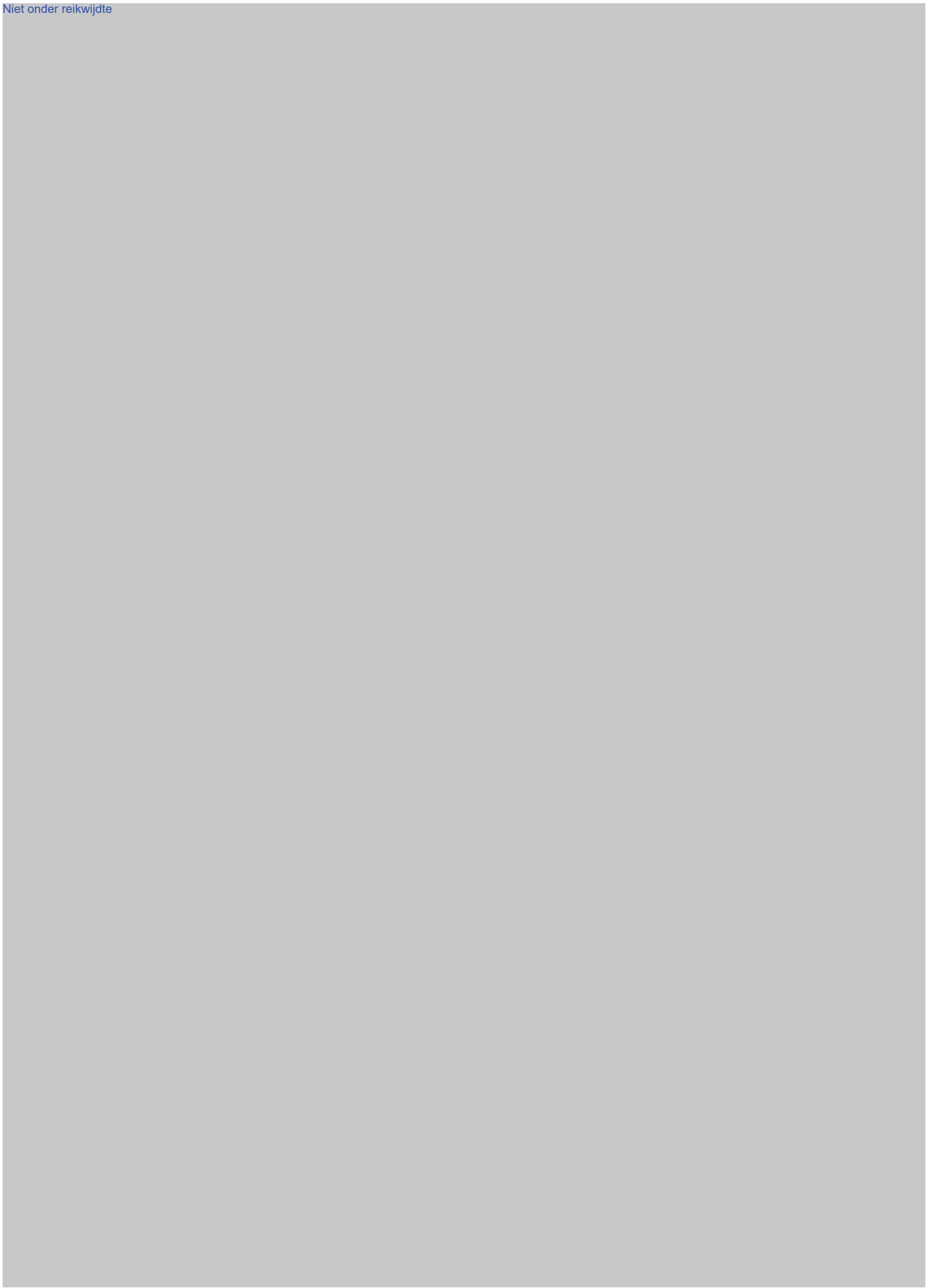
Niet onder reikwijdte



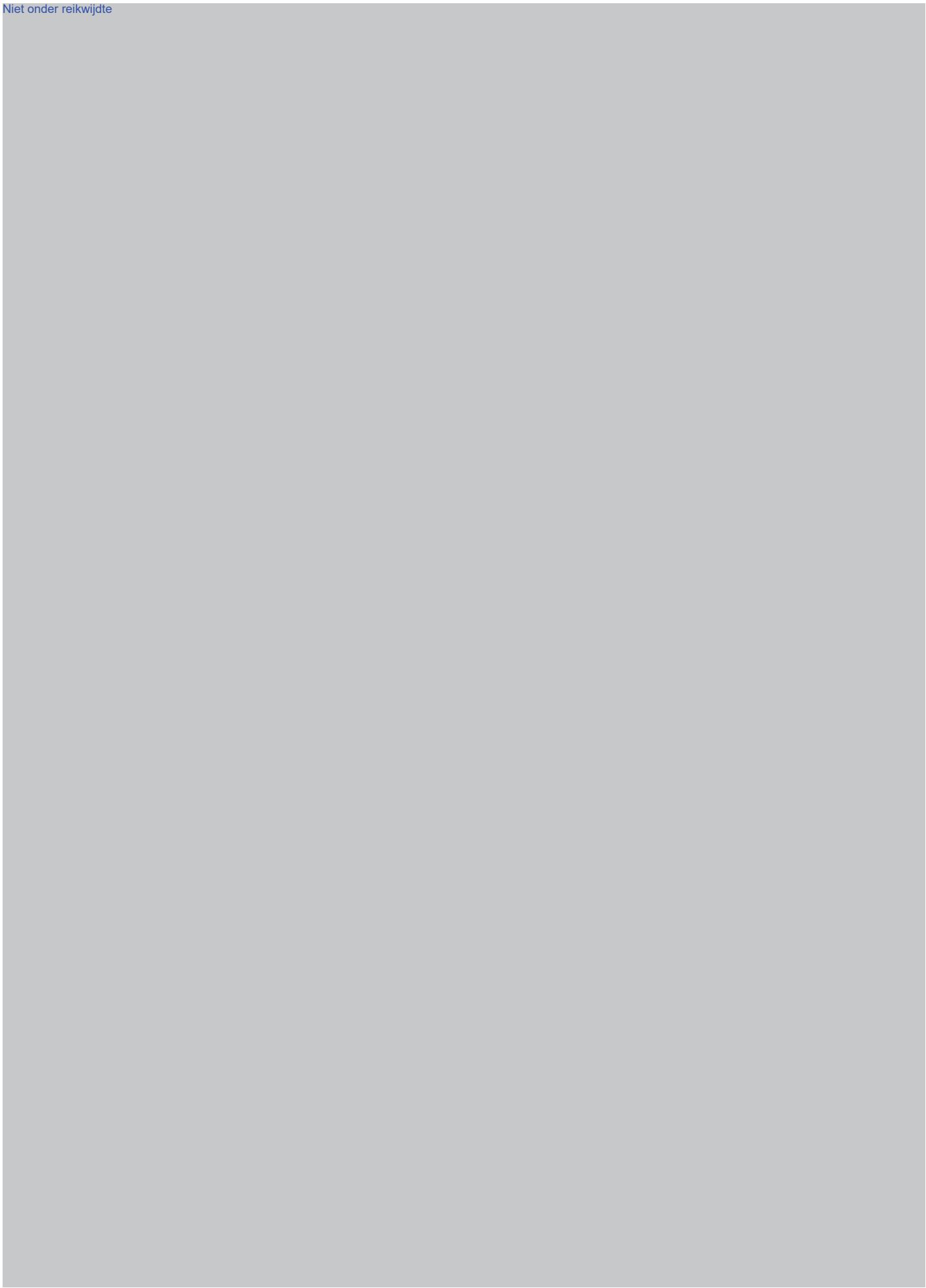
Niet onder reikwijdte

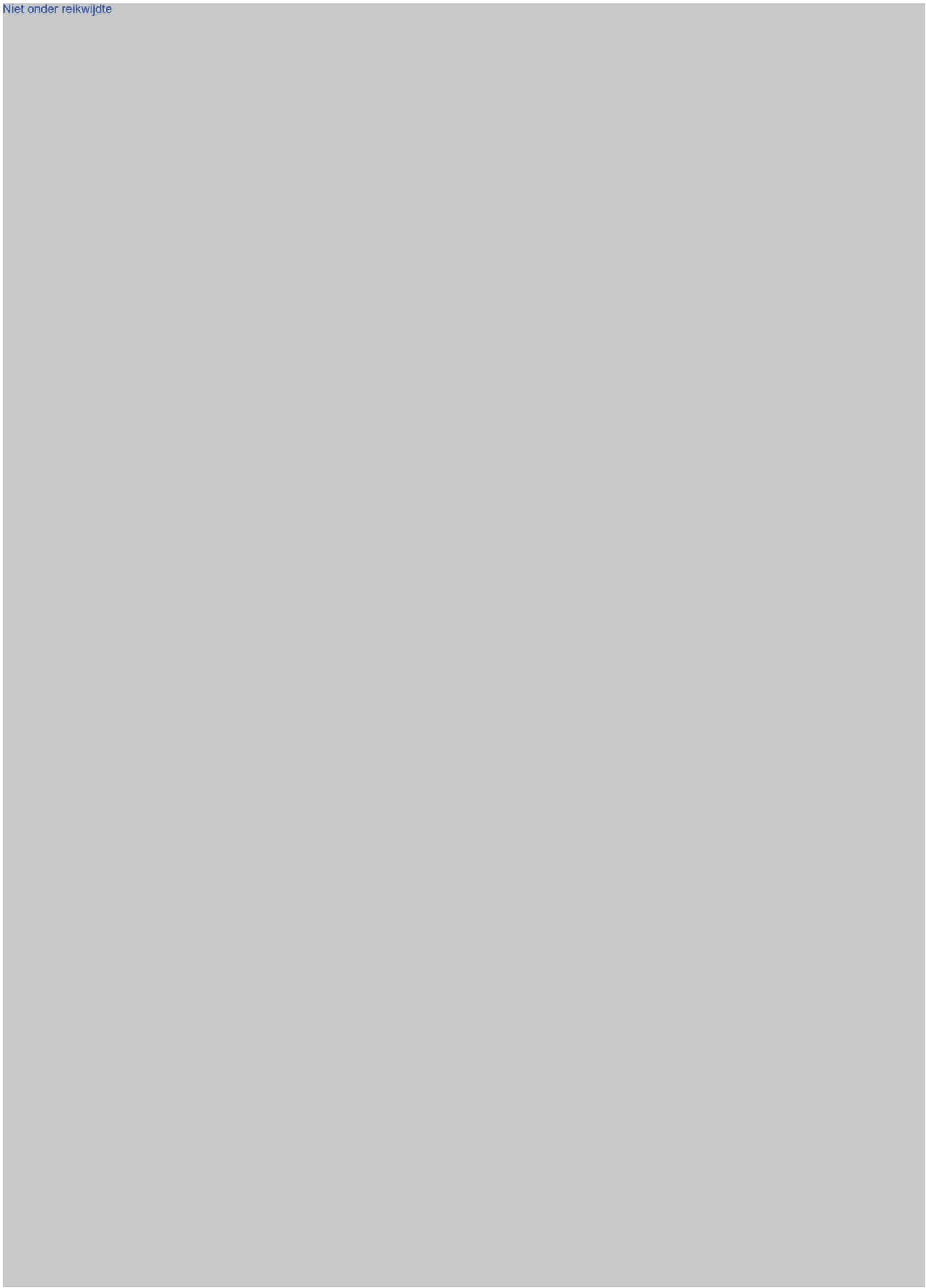


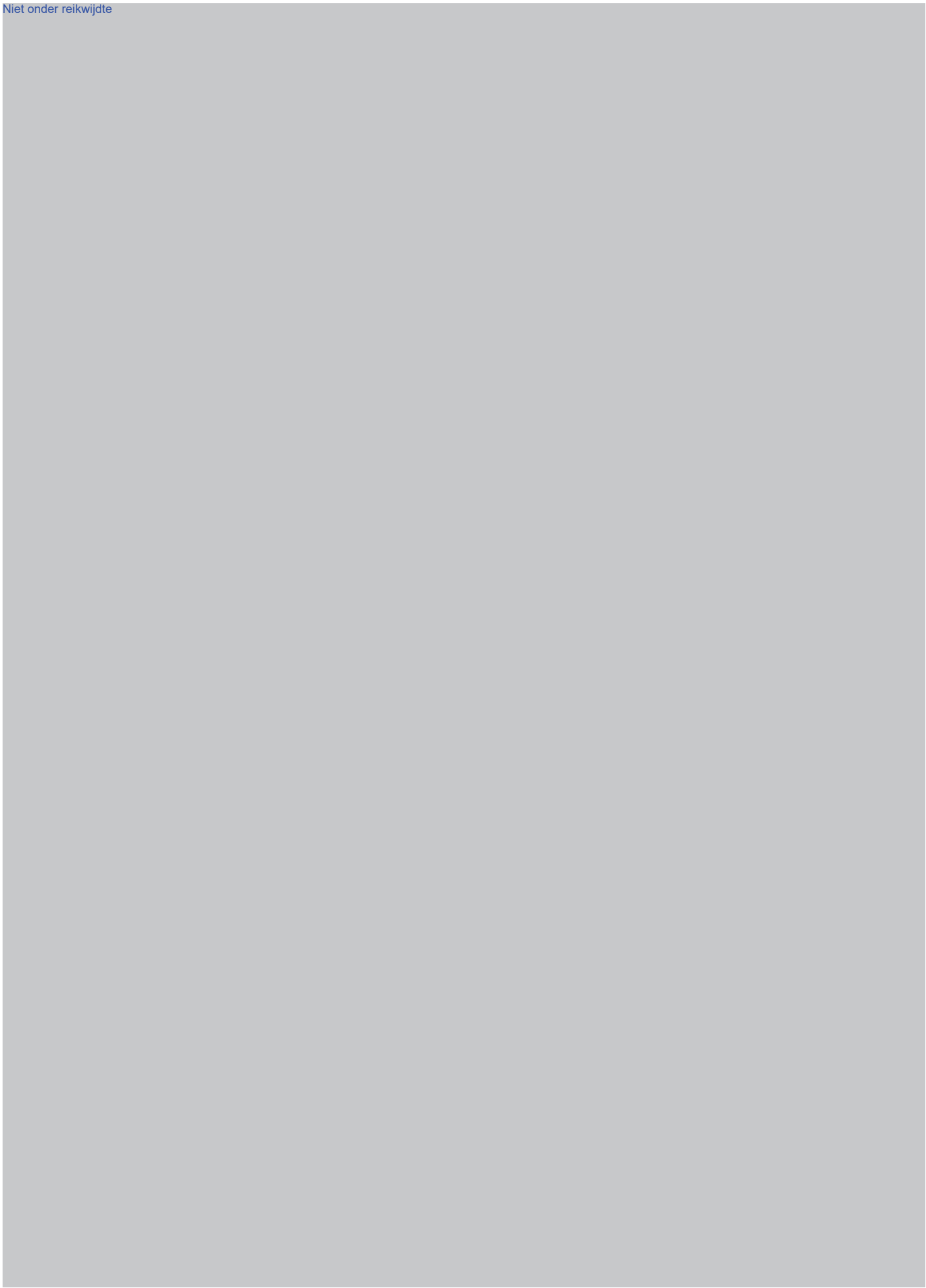
Niet onder reikwijdte

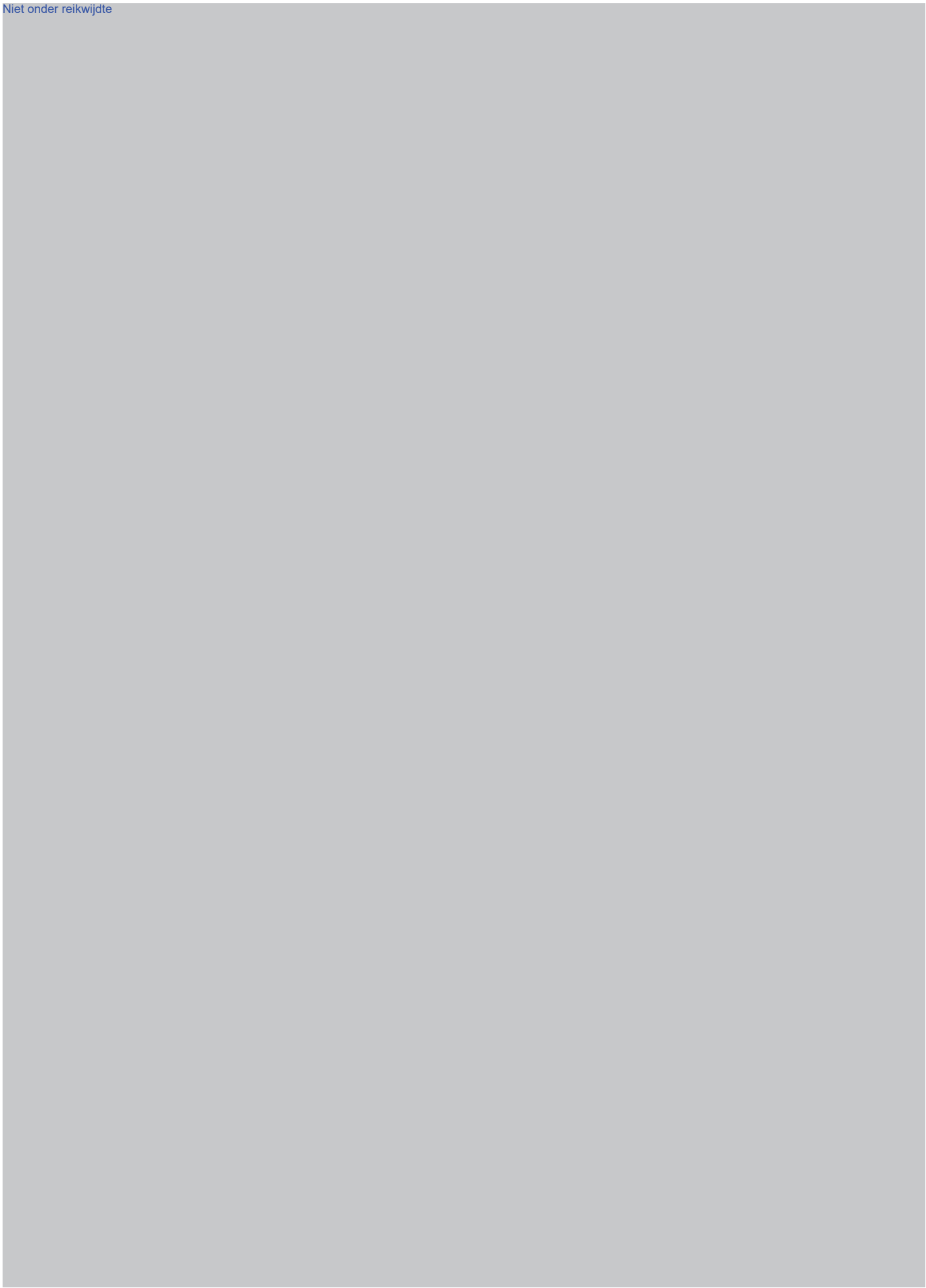


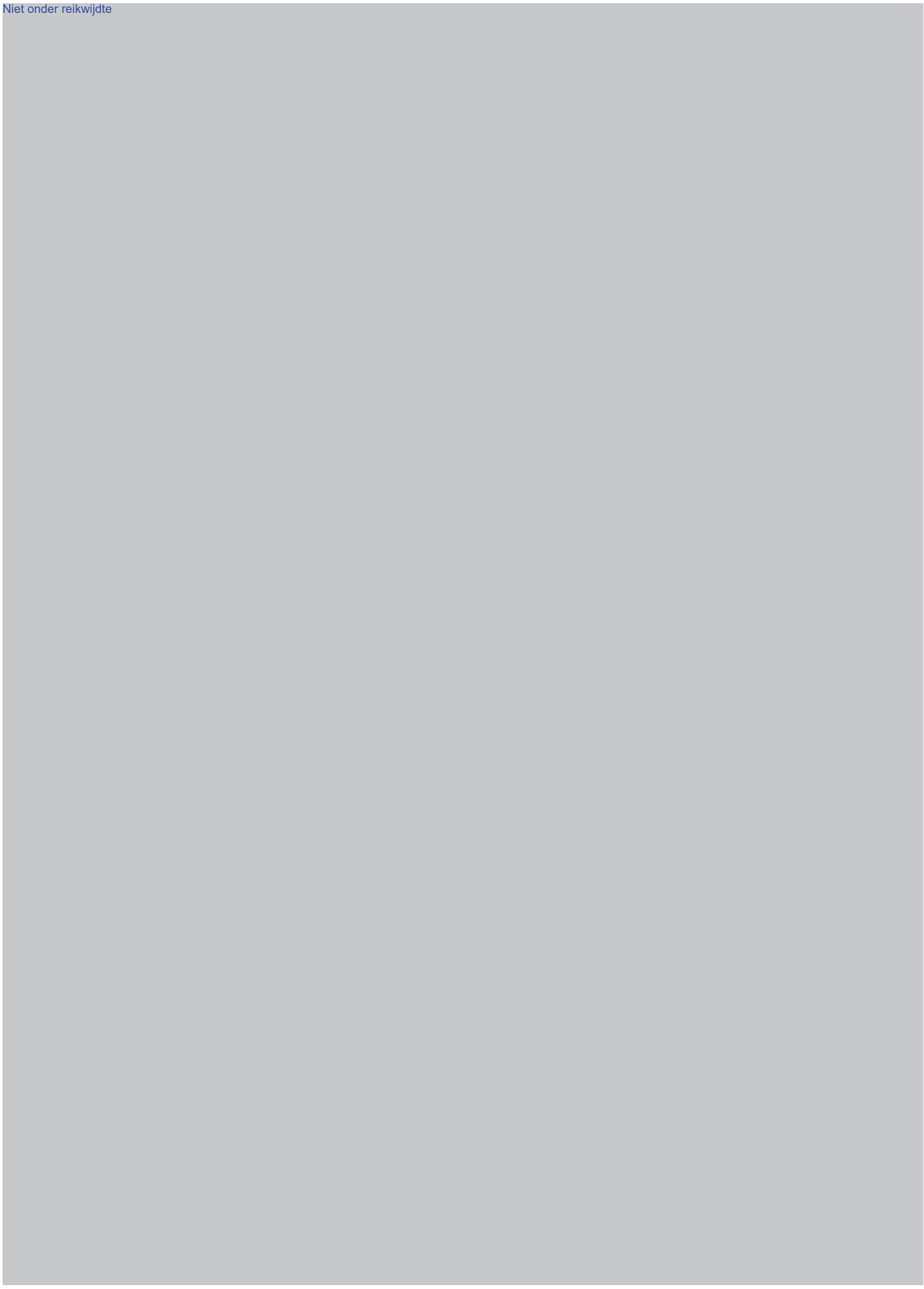
Niet onder reikwijdte




Niet onder reikwijdte

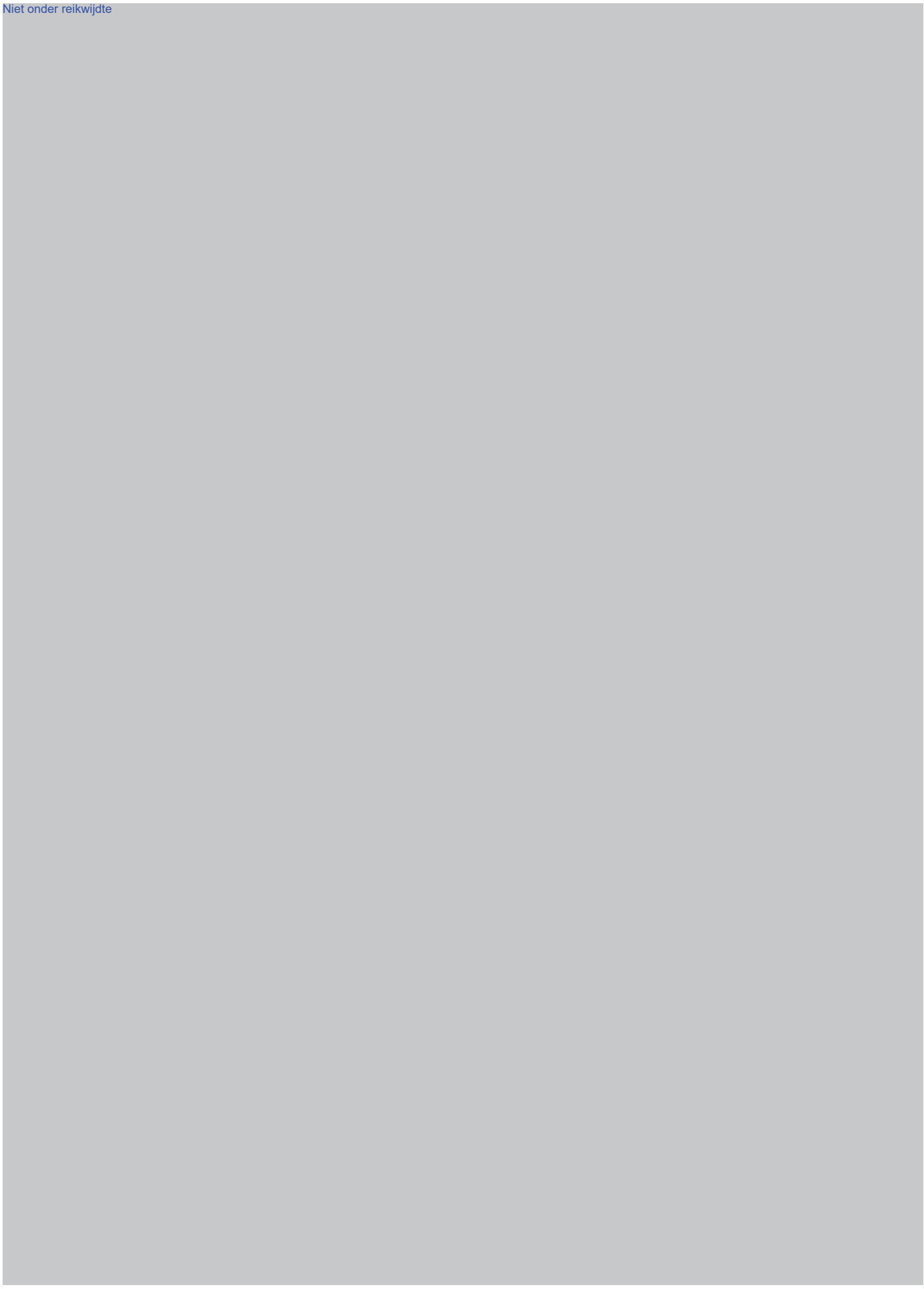

Niet onder reikwijdte


Niet onder reikwijdte

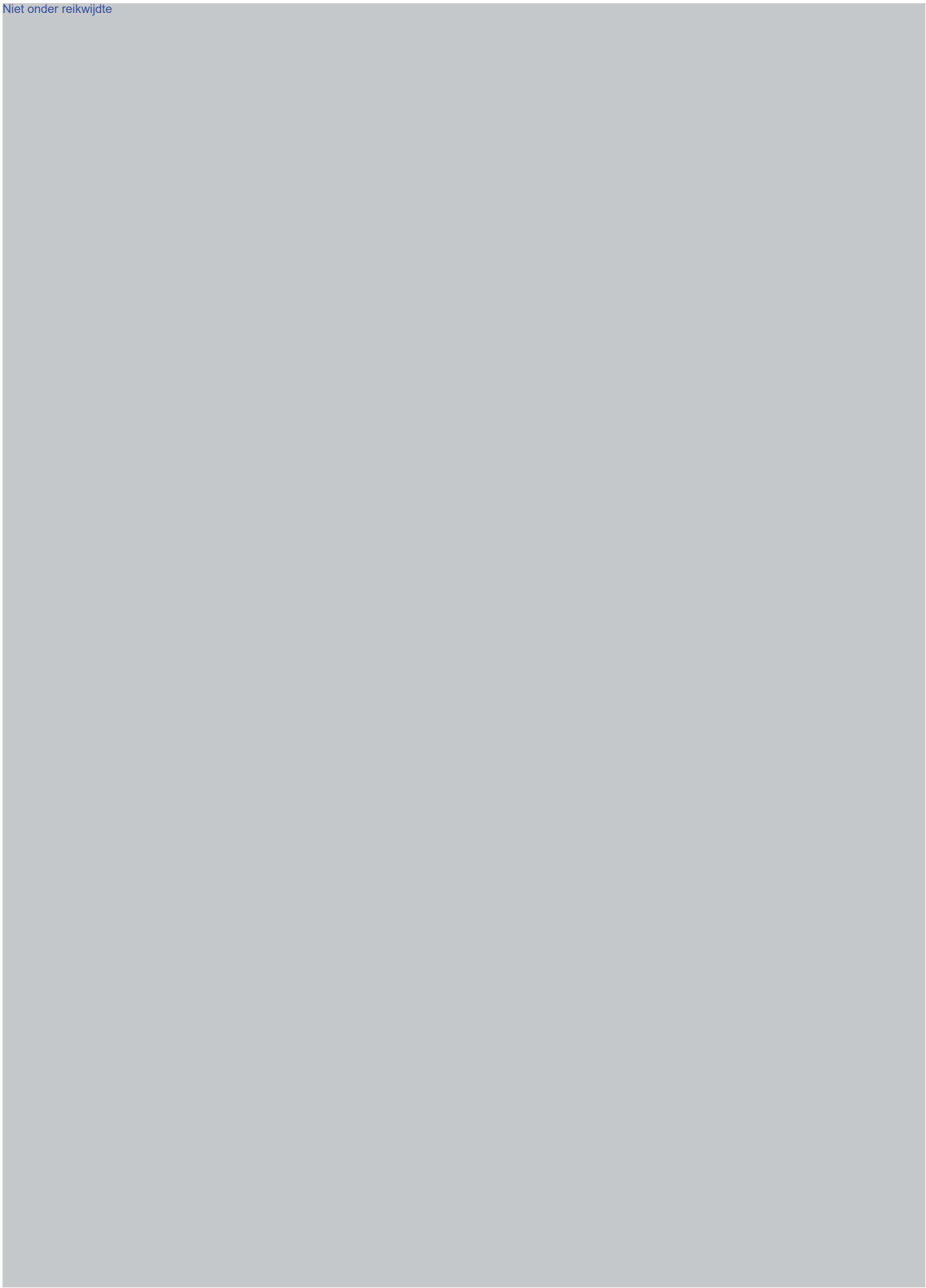

Niet onder reikwijdte

Niet onder reikwijdte

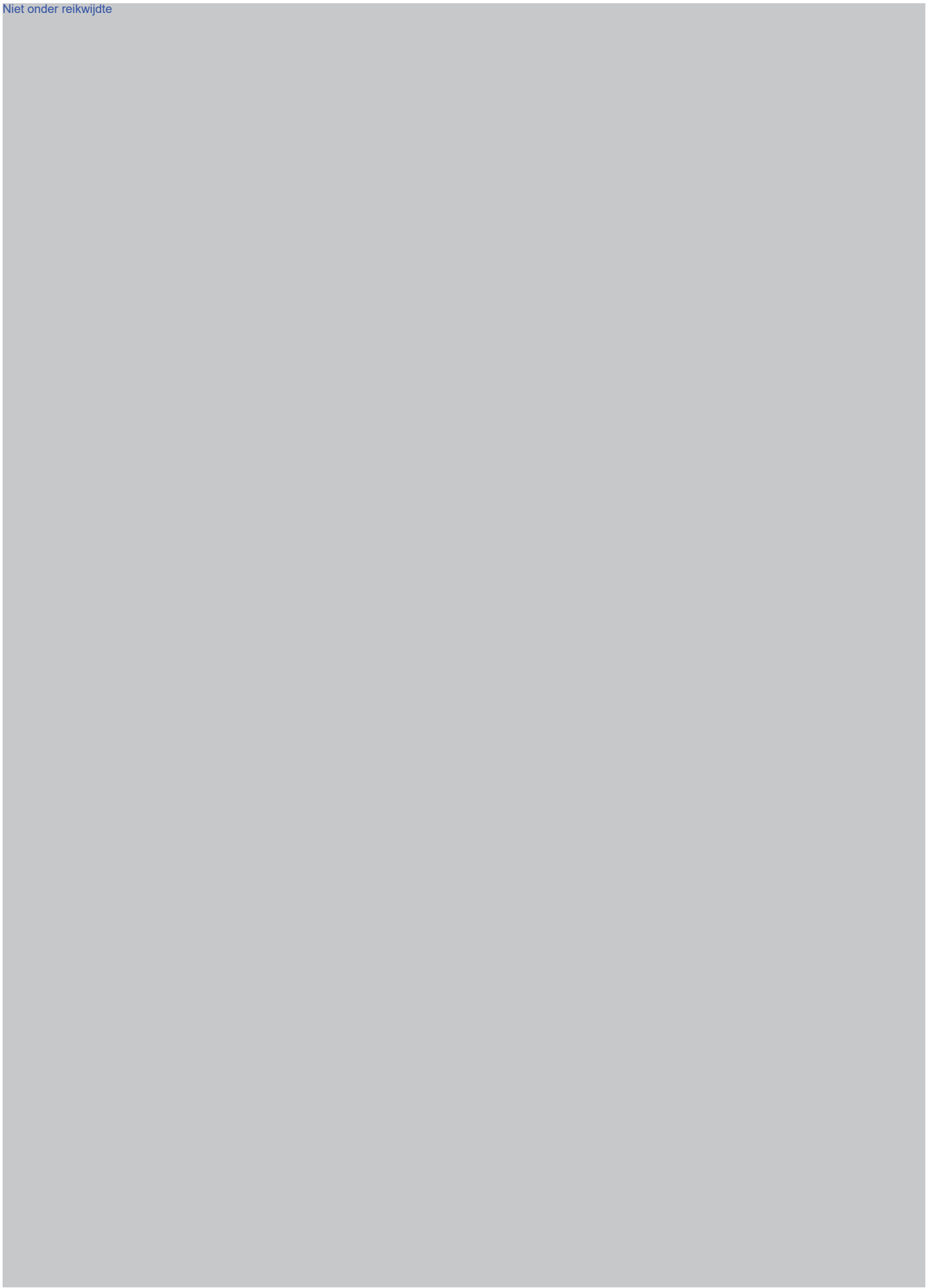
Niet onder reikwijdte



Niet onder reikwijdte



Niet onder reikwijdte



AF NR.:
20130617085202
0550

POLITIE

Aanvraagformulier Producten of Diensten

Dit aanvraagformulier dient ondertekend te worden voordat dit ingeleverd wordt bij de afdeling Inkoopmanagement / Operationele Inkoop (IKM/IO) inkoopstafkl@vtspn.nl

Bestelling
Er is sprake van een bestelling wanneer de aanvrager reeds een order tot het leveren van een product of dienst heeft opgevraagd bij zijn / haar leverancier. Afdeling IKM zal in dit geval enkel een inkoopopdracht uitvaardigen aan de leverancier.

Inkoopopdracht
Indien u de afdeling inkoop wilt inschakelen een behoefte te laten inkopen dient u uw inkoopbehoefte te formuleren. Afdeling IKM zal indien mogelijk uw behoefte in de markt uitzetten en u informeren over de verschillende mogelijkheden.

AF Nummer	13
Type aanvraag	Bestelling
Naam aanvrager	10.2.e
Omschrijving product / dienst	7-11-12
Bedrag / raming kosten	€ 6-10
Kostenplaats	SKBB000 / Kostenplaats 10210
Motivatie	Benodigde hardware tbv de inrichting van de lab omgeving CCIII conform vastgesteld PID fase 1 CCIII-binnendringen dd 14-08-2015
Handtekening + Naam	Aanvrager 10.2.e / 10.2.e Budgethouder 10.2.e Bij bedragen ma ☐ Directeur Kc ☐ Directeur Cc ☒ Directeur Op ☐ Directeur HF ☐ Directeur Facility Management ☐ Directeur Financiën ☐ Directeur Informatievoorziening Bij bedragen > € 50.000,00 ☐ Korpschef ☐ Lid Korpsleiding
Datum	~~22-08-2016~~ 05-09-2015

Aanvraagformulier inkoopopdracht / bestelling

Prestatieverklaring

Akkoord	☐ Ja ☐ Nee
Naam	
Datum	

Factuuradres	Nationale Politie T.a.v. Politie / PDC / Centrale Financiele Administratie Postbus 8300 3503 RH UTRECHT

Van: 10.2.e
Verzonden: vrijdag 30 september 2016 12:43
Aan: 10.2.e
CC: 10.2.e
Onderwerp: SBO, PSD en CCIII
Bijlagen: SBO 2017-2021 1 1.pdf

Beste 10.2.e ,

Ik krijg zojuist via intranet door dat het SBO van de Directie Operatien klaar is. Ik heb het even bijgevoegd.

Een snelle blik laat zien dat CCIII er niet in staat en ook niet als prioritaire wetgeving is benoemd. Ik vraag me nu dus even af hoe zich dit allemaal verhoudt met de onlangs door ons ingeleverde PSD (waar we ook nog niet van weten wat er mee gebeurd is). Betekent dit nu dat we het PSD voor niets in hebben lopen vullen of wordt er wel wat mee gedaan?

Daarnaast vraag ik me af of er al gewerkt wordt aan een begroting va de portefeuillehouder D&C en of wij daar nog in voorkomen? En er is in juli in Kerngroep gesproken over de onderbesteding van de portefeuillegelden en mogelijke oplossingen om het alsnog uit te geven dit jaar (bijvoorbeeld aan CCIII). Weet jij wat hier mee is gebeurt?

Zoals je ziet een hoop vragen en vanuit onze kant ziet het er allemaal niet erg positief uit… Wellicht dat je het e.e.a. kunt verduidelijken voor ons.

Met groet
Rogier

10.2.e
9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M: 10.2.e
E: 10.2.e @politie.nl

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Is gelijk aan doc. 431 - niet onder reikwijdte

Van: 10.2.e
Verzonden: zondag 2 oktober 2016 10:47
Aan: 10.2.e
CC: 10.2.e
Onderwerp: RE: SBO, PSD en CCIII

Hallo 10.2.e ,

Ik stel voor even te bellen en bij te praten. Een korte reactie.

Het SBO heeft een andere vorm gekregen en inhoudelijk staat er dit keer weinig beleid in maar is het meer een kader geworden voor het PSD proces.
Een van de onderdelen van dat kader is dat er 10 prioritaire pf's zijn waaronder cybercrime en dat ook financiën een kader is. Zowel qua onderwerp als financiering zitten we er dus goed in.

12-14

Maandag even bellen?
Wil graag even met je afstemmen over de speech van 10.2.e . Deze gaat niet over CCIII maar raakt er zijdelings aan hen ik zou graag een klein achtergrond dossiertje met jullie willen maken om aan 10. mee te geven als achtegrondinfo. Laten we even afstemmen wat daarin te stoppen.

Groet,

10.2.

From 10.2.e @knp.politie.nl>
Date: 3 October 2016 at 14:12:29 GMT+2
To 10.2.e @politie.nl>
Cc 10.2.e @politie.nl>, 10.2.e @politie.nl> 10.2.e @politie.nl> 10.2.e @politie.nl>
Subject: annotaties PSD's portfolio 2017

Beste collega,

U heeft één of meerdere PSD's ingeleverd voor het portfolioproces 2017.
Allereerst dank voor inzet van een ieder die heeft bijgedragen aan de totstandkoming van deze PSD's.
Uw ingediende PSD is verwerkt op Agora. Vanuit meerdere disciplines en expertises is uw PSD
bekeken. Zij hebben hun bevindingen én vragen weergegeven in één gezamenlijke annotatie.
Tevens is uw PSD het categoriseringsproces ingegaan en is er, bij voldoende informatie, een voorlopige categorie aan het PSD toegekend.

In het bijgevoegde bestand (een extract uit Agora), ziet u uw PSD met daaraan gekoppeld het annotatiedocument.
Het volledige bestand met alle ingediende PSD's kunt u zien op Agora. Vanuit onderstaande tabel kunt u direct doorklikken naar de betreffende documenten.

In de tijd tussen deze mail en het indienen van de PSD's, hebben wij al een aantal herziene versies van de PSD's ontvangen.
Deze zijn nog niet verwerkt in de annotaties, wat maakt dat u wellicht al iets heeft toegevoegd, waar in de annotatie (nogmaals) om gevraagd wordt.

Het vriendelijke maar doch dringende verzoek om uw aangepast PSD maandag 10 oktober 2016 voor 12.00 uur in te zenden naar dit mailadres 10.2.e @knp.politie.nl).

nr portefeuille	nr onderwerp	PSD	Annotatie
5	C		
5	D		
5	E	DenC 20160908 PSD CCIII v0.4.docx	Annotatie PSD D en C CCIII versie 0.4.docx
5	F	Niet onder reikwijdte	
5	G		
5	H		

Met vriendelijke groet,

10.2.e & 10.2.e

Staf Korpsleiding | Directie Operatiën

9

Nieuwe Uitleg 1, 2514 BP Den
HaagPostbus 17107, 2502 CG
Den Haag
M 06 10.2.e
M 06 10.2.e
werkdagen ma-do

AGORA 13 /Over%20ons.aspx

Van: 10.2.e @politie.nl]
Verzonden: maandag 3 oktober 2016 20:59
Aan: 10.2.e - BD/DGPOL/PBT/PT
CC: 10.2.e - BD/DRC/CV
Onderwerp: CCIII

Hallo 10.2.e 10.2.e

Er wordt gewerkt aan het Operationele portfolio voor komend jaar. Onderdeel daarvan is wetgeving. Nu schetst mij verbazing dat mijn collega's die dit proces begeleiden van DGWS te horen hebben gekregen dat CCIII niet op lijst hoeft omdat er geen meerderheid in de eerste kamer is en de wetgeving er de komende jaren toch niet gaat komen.
Vind ik apart met alle afstemming die wij hierover gehad hebben, met verkiezingen voor de deur en met een aangepast voorstel dat nog afgestemd moet worden.???

Kunnen jullie dit ophelderen?

Thnx,
10.2.e

From 10.2.e @minvenj.nl>
Subject **RE: CCIII**
To 10.2.e @politie.nl>10.2.e - BD/DGPOL/PBT/PT"
10.2.e @minvenj.nl>
Date 4 oktober 2016 8:45:52 CEST

Dit hoor ik voor het eerst, en wij zouden hier toch enig zicht op moeten hebben. Onze leiding wil juist vaart maken met het wetsvoorstel.

Wie is de bron van deze opmerkingen?

Groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 6 oktober 2016 10:12
Aan: 10.2.e @knp.politie.nl>
CC: 10.2.e n@politie.nl>;10.2.e @politie.nl>10.2.e @klpd.politie.nl>10.2.e @politie.nl>;10.2.e @politie.nl>; Plas, Theo van der (T.G.)10.2.e @politie.nl>;10.2.e @politie.nl>
Onderwerp: Re: annotaties PSD's portfolio 2017

Beste collega,

Dank voor het toezenden van deze mail. Ik kom op basis van deze mail en de annotatie voor het PSD CCIII tot de conclusie dat deze PSD niet gecategoriseerd is en dat dit PSD daarom ook geen opgave is en dat om deze reden dit PSD ook niet mee zal worden genomen in de prioritering volgende week. Ik ga er echter van uit dat hier een fout is gemaakt tijdens de balanceersessie.

Graag hoor ik tot welke categorie deze PSD wel hoort en zodra dit bericht is ontvangen zal ik de PSD aanpassen conform de door jullie gestelde vragen.

Met vriendelijke groet,
10.2.e

Van 10.2.e **Namens** 10.2.e
Verzonden: donderdag 6 oktober 2016 14:27
Aan 10.2.e @politie.nl>
CC 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: annotaties PSD's portfolio 2017

Beste 10.2.e

We hebben bij dit PSD vanuit twee verschillende antwoorden gekregen.
Vanuit DGpol kregen wij te horen dat dit onderwerp prioriteit heeft en vanuit de wetgeving is aangegeven dat dit onderwerp niet volgend jaar mee hoeft. Dit wordt op dit moment uitgezocht.
Wij wachten daarom dit antwoord af.
Maw wij nemen dit PSD voorlopig gewoon in behandeling totdat wij het juiste antwoord krijgen.
Sorry voor de verwarring. Wij ontvangen graag een aangevuld PSD.

Met vriendelijke groet,

10.2.e &10.2.e

Staf Korpsleiding | Directie
9

Nieuwe Uitleg 1, 2514 BP Den
HaagPostbus 17107, 2502 CG
Den Haag
M 06 10.2.e
M 06 10.2.e
werkdagen ma-do

From: 10.2.e @politie.nl>
Subject: **RE: annotaties PSD's portfolio 2017**
To: 10.2.e @knp.politie.nl>
Date: 7 oktober 2016 15:46:18 CEST

Beste 10.2.e

Dank voor je bericht. Ik begrijp je antwoord niet helemaal. Is er vanuit wetgeving op het departement aangegeven dat het onderwerp volgend jaar niet mee hoeft of is dat binnen de politie aangegeven? Wetgeving op het departement is namelijk druk bezig om de behandeling nog voor het Kerstreces in de Tweede Kamer plaats te laten vinden.

Ik vind het wel verwonderlijk dat we ondanks geen categorisering wel worden meegenomen in de verdere behandeling, maar ik zal jullie maandag een aangevuld PSD aanleveren ter verdere behandeling.

Met vriendelijke groet,
10.2.e

10.2.e
9
Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M: +31 06 5 10.2.e
E: 10.2.e

)**Van:** 10.2.e @politie.nl>
Datum: 14 oktober 2016 13:15:17 CEST
Aan: Berg, Jannine van den (J.A.) <10.2.e @politie.nl>, Plas, Theo van der (T.G.) @politie.nl>
CC: 10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>, 10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>,10.2.e @politie.nl>
Onderwerp: Memo voorstel onderuitputting gelden D&C CCIII.docx

Geachte portefeuillehouder, beste Jannine en Theo,

In de Kerngroep van 14 juli 206 is gesproken over de onderuitputting van de gelden van de portefeuille Digitalisering
en Cybercrime. Daarbij is besproken dat deze gelden ten principale besteed zouden moeten worden binnen de portefeuille. Om hier invulling aan te geven is opdracht gegeven door de portefeuillehouder om voorstellen te ontwikkelen om deze gelden uit te geven.
Bijgaand treft u aan een voorstel vanuit het project CCIII om hier invulling aan te geven. Dit voorstel is een noodzakelijke stap in de versterking en ontwikkeling van de lab-omgeving van het project CCIII. Vanwege de heimelijkheid gaat het voorstel niet in op details, maar deze kunnen mondeling worden gepresenteerd door het project.

Graag ontvangen wij uw reactie op dit voorstel.

Met vriendelijke groet,

10.2.e

10.2.e
9
Politie | Project CCIII
Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M: 10.2.e
E: 10.2.e @politie.nl

Van: Plas, Theo van der (T.G.)
Verzonden: maandag 24 oktober 2016 15:53
Aan: Berg, Jannine van den (J.A.); 9
CC: 10.2.e 10.2.e ; 10.2.e C10.2.e
10.2.e 10.2.e ; 10.2.e
Onderwerp: Antw: Memo voorstel onderuitputting gelden D&C CCIII.docx

Hallo 10.2.e ,

Ik heb het stuk gelezen en besproken met IM. Kortweg gezegd: er is hierop nog zoveel onduidelijkheid dat ik niet zomaar6 wegzet om dit te realiseren. Er is blijkbaar gekeken naar een systeem, maar of dit het systeem moet zijn en of dit een langdurige oplossing kan zijn is geheel de vraag en vraagt echt meer onderzoek. Hiervoor nu dit bedrag opzij zetten is niet verantwoord.
Dat betekent niet dat in het verdere onderzoek rond CC3 dit een plaats kan krijgen in de verkenning wat er nodig is. Ik zou het als deelproject van verkenning verder uitwerken, als dit een optie is.

groeten, Theo

drs. Theo G. van der Plas EMPM
Plv. Politiechef/Hoofd Operatiën LE
Politie | Landelijke Eenheid
Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC Driebergen
T 10.2.e

From 10.2.e @politie.nl>
Subject **Re: Antw: Memo voorstel onderuitputting gelden D&C CCIII.docx**
To 10.2.e @politie.nl>, "Plas, Theo van der (T.G.)" 10.2.e @politie.nl>, "Berg, Jannine van den (J.A.)" 10.2.e @politie.nl>
Date 25 oktober 2016 7:46:45 CEST

Ha Theo, dit was een heel bijzondere aanvraag: vanwege de hoogte van het bedrag en vanwege de aard ervan. De aanvraag kan helemaal niet in de bestaande standaards en formats behandeld worden, want dan is het geld weggegooid en het middel binnen no time geheel bot en onbruikbaar. Alleen een geheim afgeschermd traject met een paar dedicated PDC mensen kan helpen en een 'ja' van de KL, in de wetenschap dat wijzelf en andere diensten al een marktverkenning hebben gedaan. Als we dit via de gebruikelijke kanalen gaan aanvliegen met vooral alle openheid en motiveringseisen van dien, dan gaat het niet lukken! Grt 10.2.e

Van: 10.2.e
Verzonden: woensdag 26 oktober 2016 14:12
Aan: Plas, Theo van der (T.G.); Berg, Jannine van den (J.A.)
CC: 10.2.e ; 10.2.e 10.2.e 10.2.e 10.2.e); 10.2.e 10.2.e 10.2.e)
Onderwerp: RE: Antw: Memo voorstel onderuitputting gelden D&C CCIII.docx
Bijlagen: Aanvullende memo CCIII onderuitputting D&C.docx

Beste Theo,

Dank je wel voor je mail. Na overleg met 10.2.e doe ik je hierbij een aanvullende memo toekomen waarin nader wordt uitgelegd waarom wij dit verzoek hebben ingediend.

Ik hoop dat hiermee je vragen kunnen worden beantwoord.

Uiteraard zijn 10.2.e en ik beschikbaar om nog nadere informatie te verschaffen.
Met vriendelijke groet,
10.2.e

Interne memo

POLITIE

Organisatieonderdeel Portefeuille DIgitalisering en Cybercrime
Project CCIII

Behandeld door 10.2.e
Functie 9
Telefoon 06 10.2.e
E-mail 10.2.e @politie.nl

Aan
Theo van der Plas

i.a.a.
10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e en 10.2.e

Datum 26-10-2016
Bijlage(n) 0
Pagina 1

Onderwerp **Nadere informatie verzoek CCIII**

Beste Theo,

Naar aanleiding van je mail van 24 oktober 2016 als reactie op onze memo van 14 oktober 2016 waarin het project CCIII verzoekt om 6 euro te benutten uit de onderuitputting van de gelden van de portefeuillehouder Digitalisering en Cybercrime, vind je onderstaand een nadere uitleg waarom dit verzoek is ingediend.

Op 25 oktober heb ik kort met 10.2.e gesproken over dit onderwerp en zij gaf aan dat je op zoek bent naar een antwoord op de vraag waarom er voor dit product is gekozen, of er geen mogelijkheid is om een abonnement af te sluiten en hoe een korte risico analyse er uit ziet. Onderstaand zal ik hier kort op in gaan. Benadrukt dient nog wel te worden, dat gelet op de gevoeligheden, er niet al te inhoudelijk kan worden ingegaan op het product. Details kunnen altijd mondeling worden toegelicht. IM is op de hoogte van alle activiteiten van het project CCIII en IM kan gedetailleerd worden geïnformeerd over de productspecificaties en worden betrokken bij de aanschafprocedure.

1. Waarom dit product?

7-12-14

Dit product is bekend bij een partner van het project CCIII die ook in de Stuurgroep CCII vertegenwoordigd is. 9 van de Stuurgroep CCIII, kan hierover mondeling gedetailleerde informatie verstrekken.

Bovenstaand geeft kort weer waarom er voor dit product is gekozen. De aanschaf van dit product past binnen het op korte termijn te verschijnen standpunt van de Nederlandse regering over hoe om te gaan met kwetsbaarheden op het internet en het gebruik van software die gebruik maakt van dergelijke kwetsbaarheden.

2. Abonnement

De aanschafkosten van dit product zijn ongeveer6 euro. 7-12-14

[redacted]

7-12-14

[redacted]

Vanwege het gebruik van een goedgekeurd middel en om zelf te bepalen op welke wijze het product ingezet wordt is het noodzakelijk om een product eenmalig aan te schaffen en jaarlijkse licentiekosten te betalen. De aanschaf van dit product maakt voor het eerst duidelijk welke investeringen noodzakelijk zijn om te komen tot een voorziening tot het binnendringen in een geautomatiseerd werk op afstand. Daarom is de opdracht om te komen tot een centrale voorziening voor de opsporing (zie hiervoor de impactanalyse en de PID 1.0). In de PID 2.0 zal dit volledig inzichtelijk worden gemaakt.

3. Risicoanalyse

7-12-14

[redacted]

De aanschaf van dergelijke producten zal altijd in lijn zijn met het binnenkort te verschijnen standpunt van het kabinet over hoe om te gaan met kwetsbaarheden op internet en het gebruik van software die gebruik maakt van dergelijke kwetsbaarheden.

Het is geen geheim dat de politie deze bevoegdheid gaat krijgen, de manier waarop we uitvoering willen gaan geven deze bevoegdheid wel. De aanschaf van producten zal met de grootste zorgvuldigheid worden uitgevoerd.

4. Tot slot

Hierboven is weergegeven waarom het project CCIII voor dit product heeft gekozen, waarom er voor een eenmalige aanschaf is gekozen en hoe er omgegaan wordt met de heimelijkheid van dit onderwerp. Hiermee is hopelijk voldoende duidelijk geworden waarom het verzoek van 14 oktober 2016 is ingediend en verzoekt het project CCIII de portefeuillehouder om de eerder genomen beslissing om geen gelden uit de onderuitputting beschikbaar te stellen te herzien.

Met vriendelijke groet,
10.2.e

From 10.2.e

Subject **RE: Antw: Memo voorstel onderuitputting gelden D&C CCIII.docx**

To 10.2.e @politie.nl>, "Berg, Jannine van den (J.A.)" 10.2.e @politie.nl>, "Plas, Theo van der (T.G.)" 10.2.e @politie.nl>

Date 26 oktober 2016 23:17:07 CEST

Beste collega's,

Als aanvulling op deze mailwisseling wil ik jullie (in kleiner verband) erop wijzen dat ik gisteren van DGRR gehoord heb dat er geen akkoord van de staatssecretaris is voor de huidige vertrouwelijke concept tekst van het Kabinetsstandpunt onbekende kwetsbaarheden. Dus dat is een tegenvaller.
De lijn die er nu in staat wordt aangescherpt voor de politie, met als uitgangspunt dat onbekende kwetsbaarheden in principe altijd moeten worden gemeld, tenzij… Er komt een onderscheid in voor de diensten en ons.

Uiteraard wordt hierover nog afgestemd met politie en OM en moeten we kijken wat de definitieve uitwerking hiervan wordt. Dit zal echter gevolgen hebben voor de middelen die we daadwerkelijk kunnen inzetten. Ik ken dit pakket niet in detail maar heb de indruk dat dit ook consequenties heeft voor de mogelijkheid van dit pakket gebruik te maken.

Ik stel voor dat 10.2.e , 10.2.e en ik de consequenties nog verder bespreken.

M.vr.gr.,
10.2.e

Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
2008352

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 8 november 2016
Onderwerp Kwetsbaarheden in hardware en software

De afgelopen jaren is het parlement enkele keren geïnformeerd over het gebruik van kwetsbaarheden in hardware en software door de overheid.[1] In het algemeen overleg cyber security op 20 januari jl. heeft de Staatssecretaris van Veiligheid en Justitie naar aanleiding van een vraag van het lid Verhoeven (D66) toegezegd een brief te sturen over het gebruik van onbekende kwetsbaarheden in hardware en software. Naar aanleiding van die toezegging sturen wij u deze brief.

De samenleving digitaliseert en de afhankelijkheid van het internet groeit. Dat biedt grote maatschappelijke en economische voordelen. Tegelijk zijn er zorgen over de mogelijkheid voor bedrijven, burgers en de overheid om op een veilige manier gebruik te kunnen blijven maken van het internet. Veilige computersystemen zijn daarvoor een voorwaarde, en voor het vertrouwen daarin is het van belang het aantal kwetsbaarheden in computersystemen te verminderen. Tegelijk is het voor de veiligheid, zowel fysiek als in de digitale wereld, van belang dat de daders van criminaliteit, terrorisme en spionage worden aangepakt. Daarvoor is het noodzakelijk dat de overheid onderzoek doet in computersystemen, onder meer via het internet. In het streven naar een open, vrij en veilig internet dient aan de diverse belangen recht te worden gedaan. Deze belangen zijn in de meeste gevallen met elkaar in overeenstemming, maar het komt ook voor dat een belangenafweging noodzakelijk is, bijvoorbeeld tussen veiligheid en vrijheden, of tussen verschillende veiligheidsbelangen. Het kabinet

[1] Eerste Kamer, vergaderjaar 2014–2015, CVIII, N
Eerste Kamer, vergaderjaar 2014–2015, CVIII, O
Eerste Kamer, vergaderjaar 2014–2015, CVIII, G
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van het lid Oosenbrug (PvdA), 3 juli 2015, aanhangsel ah-tk-201420152773
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Verhoeven en Hachci (beiden D66), 3 juli 2015, aanhangsel ah-tk-201420152772

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

hecht dan aan een zorgvuldige afweging die per geval wordt gemaakt. Deze brief behandelt eerst het bestaan van bekende en onbekende kwetsbaarheden en het verhelpen daarvan. Vervolgens wordt de relatie met nationale veiligheid en de opsporing van strafbare feiten behandeld, met bijzondere aandacht voor de bevoegdheid tot binnendringen in geautomatiseerd werk en de daarbij behorende voorwaarden en waarborgen. Tot slot wordt aandacht besteed aan de internationale markt voor kennis over kwetsbaarheden.

Bekende en onbekende kwetsbaarheden
Om een geautomatiseerd werk binnen te dringen is het gebruik van kwetsbaarheden in hard- en software één van de methoden. Indien een kwetsbaarheid bij de desbetreffende fabrikant bekend is, dan kan deze de kwetsbaarheid verhelpen door een update, patch of nieuwe versie van het product uit te brengen. Veel kwetsbaarheden zijn echter niet bekend bij de fabrikant. In dat geval is het voor de fabrikant niet mogelijk de kwetsbaarheid te verhelpen. Onbekende kwetsbaarheden blijven soms jarenlang onopgemerkt. Indien een ander dan de fabrikant een dergelijke kwetsbaarheid vindt, dan wordt dit ook wel een "zero-day vulnerability" genoemd. Een dergelijke kwetsbaarheid kan worden gebruikt om binnen te dringen door software te schrijven die van de kwetsbaarheid gebruik maakt. In dat geval is er sprake van een "zero day exploit".

Het bestaan, de ontdekking en het verhelpen van kwetsbaarheden
Kwetsbaarheden ontstaan bij het produceren van hard- en software, bijvoorbeeld door programmeerfouten of door beperkte aandacht voor veiligheid bij het ontwerp. Hard- en software worden vaak vanwege concurrentieoverwegingen snel op de markt gebracht. Bovendien zijn de omvang en complexiteit van software fors toegenomen. Veel gebruikte applicaties hebben tegenwoordig tientallen miljoenen regels broncode. Kwetsbaarheden zijn daarom talloos en wijdverbreid.

De risico's van specifieke kwetsbaarheden kunnen sterk verschillen. Bij de fabrikant onbekende kwetsbaarheden en het gebruik daarvan krijgen vaak de meeste aandacht in de media, bijvoorbeeld als het software betreft die zeer veel wordt gebruikt. In andere gevallen betreft het zeer specifieke systemen en zijn de kwetsbaarheden vaak lastig te gebruiken. In dergelijke gevallen brengen de kwetsbaarheden vaak minder maatschappelijke risico's met zich mee. Ook reeds bekende kwetsbaarheden kunnen grote risico's met zich mee brengen. Deze zijn vaak bij een grotere groep mensen bekend en kunnen door personen met kwade bedoelingen gemakkelijker worden opgezocht en ingezet.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

Veel kwetsbaarheden worden snel nadat ze worden ontdekt gemeld bij de fabrikant. Steeds vaker stimuleren fabrikanten het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Tevens maken veel fabrikanten regelmatig een nieuwe versie of update van hun product, waarmee de op dat moment bekende kwetsbaarheden worden verholpen. Soms duurt het echter lang voordat een fabrikant een update beschikbaar stelt, en soms gebeurt dat in het geheel niet. Het beschikbaar stellen van updates om kwetsbaarheden weg te nemen, is niet verplicht en kan veel tijd en kosten met zich mee brengen. Daarnaast blijken veel eindgebruikers niet of niet direct alle voor hen beschikbare updates te installeren, of ze doen dit niet op de juiste manier. Het gevolg is dat vele systemen niet alleen onbekende kwetsbaarheden bevatten, maar ook kwetsbaarheden die reeds langer bij de fabrikant bekend zijn.

De overheid stimuleert het melden van kwetsbaarheden, onder meer met het beleid voor *responsible disclosure*. Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (NCSC) in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. Ook heeft het kabinet het wetsvoorstel Gegevensverwerking en meldplicht cyber security aan het parlement gestuurd. Dit voorstel bevat een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen bij vitale sectoren.

De nationale veiligheid en de opsporing van strafbare feiten
Criminelen, terroristen en buitenlandse inlichtingendiensten en krijgsmachten maken voor hun activiteiten steeds vaker gebruik van het internet. Die activiteiten zijn zonder onderzoek te doen in het digitale domein steeds lastiger te onderkennen of te bewijzen. Voor een effectieve opsporing, het tegengaan van spionage, verstoring en sabotage, en het waarborgen van de nationale veiligheid is onderzoek in het digitale domein noodzakelijk. Daarvoor zijn in de wet verschillende bevoegdheden opgenomen voor de daarmee belaste diensten. Voorbeelden uit de opsporing zijn het vorderen van gegevens en het onderzoek aan een geautomatiseerd werk tijdens een doorzoeking of na inbeslagname. Dergelijke bevoegdheden zijn voor de inlichtingen- en veiligheidsdiensten vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) en voor de opsporing in het Wetboek van Strafvordering (WvSv). De Wiv 2002 bevat de bevoegdheid tot binnendringen in een geautomatiseerd werk voor de AIVD en de MIVD ten behoeve van de nationale veiligheid. Het wetsvoorstel Computercriminaliteit III bevat wijzigingen in het WvSv voor een bevoegdheid tot

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

binnendringen in geautomatiseerd werk voor vooraf bepaalde opsporingsdoeleinden, voorzien van specifieke voorwaarden en waarborgen.

Technische mogelijkheden
Er zijn verschillende technieken beschikbaar die het binnendringen in een geautomatiseerd werk mogelijk maken. Er zijn vele soorten geautomatiseerde werken en de beveiliging ervan kan vele vormen hebben. Bij de keuze van een methode om het werk binnen te dringen zijn, naast noodzaak, proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang. Of het gebruik van een kwetsbaarheid de meest aangewezen methode is, wordt per geval bepaald.

De inzet van wettelijke bevoegdheden voor de nationale veiligheid
Om een zorgvuldige afweging te kunnen maken over de inzet van de genoemde bevoegdheden, is elke bevoegdheid in de desbetreffende wet van specifieke voorwaarden en waarborgen voorzien. Dat geldt ook voor de bevoegdheid tot binnendringen in een geautomatiseerd werk in de Wiv 2002. De bevoegdheid mag alleen worden ingezet in het kader van de nationale veiligheid. De inzet van deze bevoegdheid wordt altijd getoetst aan de eisen van noodzaak, proportionaliteit en subsidiariteit. De inzet moet proportioneel zijn ten opzichte van het doel en het potentiele risico op onbedoelde effecten. Bovendien is de inzet alleen geoorloofd als niet met een minder ingrijpend middel hetzelfde doel kan worden bereikt. De bevoegdheid mag alleen worden ingezet indien vooraf toestemming is verleend door de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de AIVD of de Minister van Defensie voor de MIVD. Daarnaast ziet de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) toe op de rechtmatigheid van de taakuitvoering van de AIVD en de MIVD. Met het komende voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten beoogt de regering de waarborgen betreffende de inzet van deze bijzondere bevoegdheid verder te versterken.

Op 16 december 2014 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens de Minister van Defensie het parlement geïnformeerd over de omgang met kwetsbaarheden op internet door de AIVD en de MIVD.[2] De diensten kunnen bij de inzet van bijzondere bevoegdheden kwetsbaarheden in de digitale beveiliging van een target onderkennen en gebruiken. Indien de AIVD of de MIVD in het kader van hun wettelijke

[2] kenmerk 2014Z23370 en Eerste Kamer, vergaderjaar 2014–2015, CVIII, G

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

taakuitvoering stuiten op een kwetsbaarheid die de belangen van gebruikers van het internet kan schaden, zullen deze diensten belangendragers informeren. Veelal zal het de fabrikant van de hardware of software betreffen en/of een specifieke groep gebruikers die een groot risico loopt.

Er kunnen echter wettelijke bepalingen (de wettelijke plicht tot het beschermen van bronnen, actueel kennisniveau) of operationele redenen zijn die het melden van kwetsbaarheden (tijdelijk) in de weg staan. In dergelijke gevallen wordt het belang van informatieverstrekking afgewogen tegen het belang van geheimhouding en bronbescherming. Voorbeelden van situaties waarin het belang van het melden van een bij de fabrikant onbekende kwetsbaarheid mogelijk niet opweegt tegen andere zwaarwegende belangen zijn de inzet in een gewapend conflict, zwaarwegende belangen voor de nationale veiligheid of als de kennis van een kwetsbaarheid onder voorwaarde van geheimhouding met de Nederlandse overheid is gedeeld. Geconstateerde kwetsbaarheden hoeven niet noodzakelijkerwijs betrekking te hebben op een groot deel van de gebruikers van het internet. Sommige kwetsbaarheden betreffen zeer specifieke systemen. Als het zwaarwegend belang tijdelijk van aard is, dan zal de kwetsbaarheid daarna alsnog worden gemeld.

De inzet van wettelijke bevoegdheden voor de opsporing van strafbare feiten
In het wetsvoorstel Computercriminaliteit III is de inzet in het kader van de opsporing alleen mogelijk voor een beperkt aantal ernstige strafbare feiten en is vooraf toestemming van een rechter-commissaris vereist. De proportionaliteit en subsidiariteit worden zo voorafgaand aan de inzet onafhankelijk getoetst. Politie en justitie hebben, net als in de fysieke wereld, een groot belang bij het voorkómen en beperken van criminaliteit. Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit. Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hardware of software.

Ook voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt echter dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan. In dergelijke gevallen kan het Openbaar Ministerie, na een zorgvuldige afweging, besluiten de melding van een kwetsbaarheid uit te stellen. Dat kan zich bijvoorbeeld voordoen als de melding zou resulteren in onderkenning van het opsporingsonderzoek door de verdachte of als het een

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het Openbaar Ministerie centraal genomen. Daarbij wordt onder meer gelet op de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede.

De internationale markt voor kennis over kwetsbaarheden
Op internet kan kennis over kwetsbaarheden in hardware en software worden gekocht. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden. Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Fabrikanten stimuleren steeds vaker het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Dergelijke kennis kan bijdragen aan de veiligheid van systemen en van het gebruik ervan.

Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de verkoop ervan aan bepaalde partijen onwenselijk. De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen, waardoor het lastig is deze markt aan controle te onderwerpen. Wel is de verkoop van zogenaamde *intrusion software* die gebruik maakt van kwetsbaarheden in bepaalde omstandigheden onderhevig aan exportcontrole. Zoals gemeld in de antwoorden op vragen van de leden Oosenbrug (PvdA) en Verhoeven (D66) van 28 augustus 2015 hecht de regering aan beperking van de uitvoer van ICT-goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] De Europese Commissie heeft inmiddels een voorstel gedaan voor herziening van de dual use-verordening waarmee het toezicht op de internationale handel in goederen voor tweeërlei gebruik (dual use) wordt geregeld.

Conclusie
Het kabinet bevordert een vrij, open en veilig internet. Het beperken van kwetsbaarheden in hardware en software is daarvoor van belang. De overheid bevordert het melden van kwetsbaarheden, onder meer met het beleid voor

[3] Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Oosenbrug (PvdA) en Verhoeven (D66), 28 augustus 2015, aanhangsel ah-tk-201420153199

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

responsible disclosure. Het kabinet heeft tegelijk tot taak om binnen de wettelijke kaders de nationale veiligheid te waarborgen en strafbare feiten op te sporen, in de digitale en in de fysieke wereld. Daarvoor is toegang tot digitale informatie noodzakelijk, waarbij in bepaalde gevallen kan worden gekozen voor het binnendringen in een geautomatiseerd werk. Het gebruik van kwetsbaarheden is daarbij één van de technische mogelijkheden om de bevoegdheid tot binnendringen uit te voeren. Deze bevoegdheid is alleen onder strenge, bij wet bepaalde voorwaarden toegestaan en is met specifieke waarborgen omkleed. De noodzaak, proportionaliteit en de subsidiariteit zijn leidend bij de afweging tot inzet. De waarborgen verzekeren een zorgvuldige afweging van de betrokken belangen.

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff

De Minister van Binnenlandse Zaken en Koninkrijksrelaties

R.H.A. Plasterk

De Minister van Defensie

J.A. Hennis-Plasschaert

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Datum: 10 november 2016 09:30:35 CET
Aan: 10.2.e @politie.nl>
Onderwerp: FW: QenA's kwetsbaarhedenbrief
Bijlagen: Vragen voorlichting over brief kwetsbaarheden (4).docx

Beste 10.2.e ,

Door een collega van DGRR is een opzet gemaakt voor QenA's ter ondersteuning van de STAS bij beantwoording van vragen uit de pers mbt de kwetsbaarhedenbrief.
Ben je het eens met de antwoorden op de vragen (geel gearceerd wat voor de politie vooral van toepassing is), en/of heb je aanvullingen.
Omdat de brief waarschijnlijk binnenkort uit gaat hoop ik dat je spoedig kan reageren.

Alvast veel dank voor de medewerking.

Groeten,
10.2.e

Vragen voorlichting over brief kwetsbaarheden

Q: Wat is een kwetsbaarheid?
Een kwetsbaarheid is een zwakheid in een geautomatiseerd werk die gebruikt kan worden om heimelijk en op afstand het systeem binnen te dringen of anders te laten functioneren dan bedoeld. Een systeem kan meerdere typen kwetsbaarheden bevatten. Zo kunnen er fouten zitten in de gebruikte software of is het systeem niet goed geconfigureerd. Ook kan bij het gebruik van de systemen een fout worden gemaakt door bijvoorbeeld software van een onbekende bron te installeren of zeer zwakke wachtwoorden te gebruiken.

Q: Gaat dit ook over kwetsbaarheden die het NFI gebruikt voor bijvoorbeeld in beslag genomen telefoons?
Nee. Deze brief betreft kwetsbaarheden die worden gebruikt voor het heimelijk en op afstand binnendringen in geautomatiseerd werk.

Q: Zijn er nu veel kwetsbaarheden in computersystemen te vinden?
Ja. Door de enorme omvang, regels code, van hedendaagse software kan er van worden uitgegaan dat er zeer veel kwetsbaarheden zijn. Zo bestaat Microsoft Office 2013 uit ongeveer 45 miljoen regels computercode en Facebook uit 61 miljoen regels code. Windows NT, bestaande uit ca. 4 miljoen regels code, bevat naar schatting 64000 bugs. Ondanks vele initiatieven, zowel van de private partijen als van overheden, die er dagelijks voor zorgen dat er tal van nieuwe kwetsbaarheden bekend worden, is niet te verwachten dat er op korte termijn vrijwel geen kwetsbaarheden meer zullen zijn.

Q: Waarom is het nodig dat de politie gebruik maakt van onbekende kwetsbaarheden?
Er zijn veel soorten geautomatiseerde werken, en veel situaties te bedenken waarin de bevoegdheid tot binnendringen nodig is. Het gebruik van onbekende kwetsbaarheden kan daarbij niet worden uitgesloten. 12-14

Q: Hoe weet de politie of een kwetsbaarheid al bekend is bij de fabrikant?
Er bestaan verschillende databases waarin publiek bekende kwetsbaarheden geregistreerd staan. Het beleid van software producenten om kwetsbaarheden in hun software publiek bekend te maken verschilt per bedrijf. 12-14

Q: Hoe weten we dat onbekende kwetsbaarheden vaak lastig uit te buiten zijn? Is dat ook het geval voor wizkids?
Het vinden van een onbekende kwetsbaarheid is zeer specialistisch werk. Bovendien kunnen niet alle onbekende kwetsbaarheden ook effectief worden benut om binnen te dringen in een geautomatiseerd werk. Soms vergt het veel tijd en/of capaciteit om de code te produceren die kwetsbaarheid kan benutten. Voor criminelen kan dat een te grote investering zijn, en dan zullen zij eerder voor andere middelen kiezen. Het is voor criminelen of andere kwaadwillen vaak

gemakkelijker om gebruik te maken van al bekende kwetsbaarheden, of kwetsbaarheden die zij eerder hebben gebruikt.

Q: Hoe komen we tot de conclusie dat de risico's van specifieke onbekende kwetsbaarheden voor de algemene veiligheid sterk verschillen? Zijn niet alle onbekende kwetsbaarheden een veiligheidsrisico?
Sommige kwetsbaarheden zijn van toepassing op heel specifieke systemen of een heel specifieke groep gebruikers. Het kan bijvoorbeeld gaan om een wapensysteem van een vijandelijke krijgsmacht, of een specifiek systeem dat door een groep criminelen gebruikt wordt. Hoewel dit in zo'n geval wel degelijk een risico is voor de veiligheid van het betreffende systeem, is het risico voor de algemene veiligheid, ofwel het maatschappelijk risico kleiner. Voor software die door een brede groep gebruikers wordt gebruikt, zoals een onbekende kwetsbaarheid in Internet Explorer, is het maatschappelijk risico van een onbekende kwetsbaarheid een stuk groter. Dit maatschappelijk belang weegt zwaar bij de afweging die vervolgens wordt gemaakt.

Q: Werkt responsible disclosure?
Ja. Het beleid voor *responsible disclosure* is er op gericht het melden van kwetsbaarheden te stimuleren. De afgelopen jaren is daar veelvuldig gebruik van gemaakt (CIJFERS NCTV?)

Q: Is het niet tegenstrijdig dat de regering enerzijds de veiligheid van het internet zegt te willen bevorderen, en anderzijds wel belang heeft bij het open houden van die kwetsbaarheden en ze zelf misbruikt?
Voor de veiligheid van het internet is het van belang dat kwetsbaarheden zo veel mogelijk worden voorkomen of verholpen. Tegelijk is het voor de opsporing van strafbare feiten van belang dat de opsporingsinstanties kunnen beschikken over relevante informatie. Daarvoor is de bevoegdheid tot binnendringen in een geautomatiseerd werk noodzakelijk. Dat is ook van belang voor de opsporing van cybercriminelen. In de meeste gevallen zal het belang van het verhelpen van kwetsbaarheden effectiever zijn voor het voorkomen van criminaliteit dan het in stand houden ervan ten behoeve van de opsporing. Er kunnen zich echter situaties voordoen dat het belang van de bevoegdheid tot binnendringen zo groot is dat een kwetsbaarheid niet wordt gemeld.

12-14

Q: Hoe wordt de afweging gemaakt voor het al dan niet melden van zero-days die in het licht van een opsporingsonderzoek bij de politie aan het licht komen?

12-14

.

Q: Wat betekent “in beginsel direct, of zo spoedig mogelijk” melden in de praktijk?
Soms kan er enige tijd zitten tussen de beslissing van het OM om te melden, en de melding zelf. Bijvoorbeeld omdat nog moet worden uitgezocht wie de fabrikant is, of wanneer melding via het NCSC verloopt.

Q Hoe verloopt het proces van melden?
Het OM kan beslissen om direct aan de fabrikant te melden, of om melding te laten verlopen via het NCSC.

Q: Gaat de politie zich actief begeven op de markt voor zero-days?
12-14

Q: Wanneer de politie software koopt voor het binnendringen, hoe weet de politie dan of deze software gebruik maakt van onbekende kwetsbaarheden? Gaat de politie deze ook melden?
12-14

Q: Als de politie software koopt waarvan de producent niet wil prijsgeven of gebruik wordt gemaakt van zero-days, ziet de politie dan af van het kopen van deze software?
12-14

Q: Gaat de minister/stas van V&J inzicht geven in hoe vaak het OM besluit een kwetsbaarheid niet te melden?
Daar is op dit moment niet toe besloten.
(NB: het is eventueel mogelijk het aantal kwetsbaarheden en het aantal dat daarvan is gemeld jaarlijks bekend te stellen. Hierover is nog geen besluit genomen.)

Van: 10.2.e
Verzonden: donderdag 10 november 2016 13:20
Aan: 10.2.e @politie.nl>
Onderwerp: FW: QenA's kwetsbaarhedenbrief
Bijlagen: Vragen voorlichting over brief kwetsbaarheden (4).docx

Hi 10.2.e ,

Samen even naar kijken? Zit nu op een congres maar kijk er morgen naar.

Groet,
10.2.e

Is gelijk aan doc 450

Is gelijk aan doc 450

Is gelijk aan doc 450

Van: 10.2.e - BD/BSG
Verzonden: woensdag 16 november 2016 17:05
Aan: 10.2.e - BD/BSG/ADVIES; 10.2.e - BD/BSG
CC: 10.2.e . - BD/DCS/ACSB
Onderwerp: FW: Voorbereiding CCIII

Besten,

Zouden jullie ervoor willen zorgen dat dit bij de juiste personen komt? Graag terugkoppeling op de onderstaande punten, zodat ik het gesprek aan kan gaan.

Bij voorbaat dank,

10.2.e

Met een beetje geluk behandelen we volgende week de CCIII. In de PV stonden alle neuzen die kant uit. Nu hangt het af van de plenaire agenda…
Allereerst komt er amendement van Tellegen met Segers over het toestaat van de “chatbot” als lokpuber. Zodra het amendement klaar is, stuur ik je het.
Verder wil ik op de volgende punten kijken wat we kunnen:
- 7-12-14
- Ik wil een punt maken van aangiftebereidheid – die is nu laag maar dat heeft ook te maken met het feit dat slachtoffers vaak niet weten dat ze gehackt zijn of denken dat het geen zin heeft om aangifte te doen. Komt er hier een publiekscampagne? Hoe schroeven we die aangiftebereidheid omhoog? =>DGPOL
- 7-12-14
- Komt het kabinet met een reactie op het rapport “Nederland Digitaal Droge Voeten”. => NCTV
- 7-12-14
- Ik heb mogelijk ook nog 2 vragen t.a.v. medewerkingsplicht telecomproviders en aansprakelijkheid, nl wie draait er nu precies op voor de schade?) DWJZ

Van: 10.2.e BD/BSG/ADVIES
Verzonden: donderdag 17 november 2016 14:04
Aan: 10.2.e - BD/DWJZ/SSR; 10.2.e . - BD/DRC/CV; 10.2.e - BD/DRC/CV
Onderwerp: FW: Voorbereiding CCIII

Hallo 10.2 , 10.2. en 10. ,

Hieronder enkele punten uit de Kamer waar de PA reactie op vraagt. De bullits zijn ook naar de NCTV gestuurd deze geven al aan dat de reactie op het rapport NL droge voeten misschien meer past bij begrotingsbehandeling (immers een extra impuls op een aantal vlakken zit juist al in begroting). Daar ligt al een vraag voor klaar.

Kunnen jullie verder een reactie richting de PA verzorgen?

Met vriendelijke groet,

10.2.e
Adviseur
M 10.2.e
10.2.e @minvenj.nl

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 17 november 2016 14:26
Aan: 10.2.e - BD/DGPOL/PBT/PT; 10.2.e (Parket-Generaal) (10.2.e @om.nl); 10.2.e @klpd.politie.nl); 10.2.e @om.nl'; 10.2.e @om.nl);10.2.e @politie.nl); 10.2.e @klpd.politie.nl)
CC: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e . - BD/DRC/CV;10.2.e . - BD/DCS/ACSB
Onderwerp: CC3 misschien in de Kamer volgende week

Beste collega's,

Vanochtend hoorden wij dat er een kans bestaat dat het wetsvoorstel CC3 volgende week al op de agenda van de Tweede Kamer staat voor plenaire behandeling. Dit is op dit moment nog niet besloten,
en de kans dat het later wordt dan volgende week is groot. Toch moeten we rekening houden met de mogelijkheid, wat betekent dat we morgenmiddag een eerste versie van het dossier voor de staatssecretaris gereed hebben. Zojuist hebben wij hierover overleg gevoerd met DWJZ. Daar kwam het volgende uit:

We maken nu een dossier met spreekteksten, factsheets en Q&A's. Dat dossier moet morgenmiddag 13.00 uur af zijn, inclusief afstemming

Er zijn onderwerpen verdeeld tussen DWJZ en DRC. Van beide kanten kunnen jullie dus benaderd worden voor afstemming.

We streven er naar vanavond een eerste versie van alle stukken af te hebben. Voor onze onderwerpen zullen we deze vanavond aan jullie sturen. Aan jullie de vraag om deze te bezien op onjuistheden e.d. Gezien de korte deadline wil ik jullie vragen VOOR MORGEN 10.30 UUR DAAROP TE REAGEREN. Dat is een veel te korte deadline, en daar kunnen we helaas niets aan veranderen.

De staatssecretaris heeft in het weekend dan de mogelijkheid om eea te lezen, zodat we begin volgende week zijn aanpassingen / aanvullingen / wensen kunnen verwerken.

Voor de plenaire behandeling hebben we jullie hard nodig in de Tweede Kamer om met ons de staatssecretaris te ondersteunen.

Ik hoop dat dit voor jullie duidelijk en werkbaar is. Wij gaan nu aan het werk om het concept
vanavond gereed te hebben. Ik ga bovendien nog contact zoeken met Voorlichting om te bezien of een
werkbezoek nog mogelijk / wenselijk is.

Groet,
10.2.e

From: 10.2.e BD/DRC/CV 10.2.e @minvenj.nl>
Date: 17 November 2016 at 14:47:33 GMT+1
To: 10.2.e @om.nl>, 10.2.e - BD/DCS/ACSB <10.2.e @nctv.minvenj.nl>, 10.2.e @politie.nl>, 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>, 10.2.e @klpd.politie.nl>, 10.2.e om.nl>, 10.2.e (Parket-Generaal) 10.2.e @om.nl
Cc: 10.2.e . - BD/DRC/CV 10.2.e @minvenj.nl>, 10.2.e - BD/DRC/CV <10.2.e @minvenj.nl>, 10.2.e . - BD/DWJZ/SSR <10.2.e @minvenj.nl>, 10.2.e . - BD/DWJZ/SSR 10.2.e @minvenj.nl>
Subject: FW: Voorbereiding CCIII
Importance: High

Collega's, zie hieronder vragen van de PA over CCIII. Ik heb overal achter gezet wie volgens mij de kennis heeft om de vraag te beantwoorden. Kunnen jullie deze asap beantwoorden? Mag via mij, cc aan 10.2.e .

@10.2 /10.2.e , kunnen jullie de laatste vraag beantwoorden?

Groet,

10.2.e

Van: 10.2.e
Verzonden: donderdag 17 november 2016 15:13
Aan: 10.2.e @klpd.politie.nl>; 10.2.e @om.nl>; 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>; 10.2.e @om.nl>; 10.2.e - BD/DCS/ACSB 10.2.e @nctv.minvenj.nl>; 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>; 10.2.e (Parket-Generaal) 10.2.e @om.nl **CC:** 10.2.e . - BD/DRC/CV 10.2.e @minvenj.nl>; 10.2.e - BD/DWJZ/SSR 10.2.e @ minvenj.nl>; 10.2.e - BD/DWJZ/SSR 10.2.e @minvenj.nl>; 10.2.e 10.2.e - BD/DRC/CV <10.2.e @minvenj.nl>
Onderwerp: Re: Voorbereiding CCIII

Hoi 10.2.e

Korte reactie op twee vragen, mocht er behoefte zijn aan meer info, dan hoor ik dat graag

- 7-12-14

- 7-12-14

Groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 17 november 2016 15:50
Aan: 10.2.e
Onderwerp: FW: Voorbereiding CCIII

Ik dacht dat jij in de lijst stond?

Groet,
10.2.e

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 17 november 2016 19:50
Aan: 10.2.e - BD/DGPOL/PBT/PT; 10.2.e (Parket-Generaal) 10.2.e @om.nl)'; 10.2.e @klpd.politie.nl)'; 10.2.e @om.nl'; 10.2.e @om.nl)'; 10.2.e @politie.nl)'; 10.2.e @klpd.politie.nl)'
CC: 10.2.e - BD/DRC/CV; 10.2.e . - BD/DRC/CV; 10.2.e - BD/DCS/ACSB
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Beste collega's, bij deze onze concept-producten tot nu toe.

Groet,
10.2.e

Van: 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>
Verzonden: donderdag 17 november 2016 20:15
Aan: 10.2.e
Onderwerp: FW: CC3 misschien in de Kamer volgende week
Bijlagen: QA.Gegevens van derden Bijvangst.docx; Factsheet De wettelijke regelingen in buurlanden.docx; Factsheet decryptiebevel.docx; Factsheet kwetsbaarheden.docx; QA aangiftebereidheid.docx; QA definitie en pacemaker.docx; QA financien.docx; QA software kopen.docx

En het andere mailadres…

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Beantwoording : DWJZ

Vraag: Hoe kan een privacy inbreuk van niet-verdachte personen worden voorkomen?

Antwoord:

- Inzage in communicatie van andere, niet-verdachte personen kan bij de uitvoering van de bevoegdheid **niet worden uitgesloten**.
- Dit is thans niet anders bij de toepassing van bevoegdheden als het aftappen van communicatie of het direct afluisteren.
- Wel zijn de **wettelijke voorwaarden** voor de uitoefening zodanig dat zoveel mogelijk wordt voorkomen dat de opsporing in aanraking komt met gegevens van derden.
- Dit betreft ten eerste het vereiste dat het geautomatiseerde werk **bij de verdachte in gebruik is**.
- In het bevel van de officier van justitie dient te worden vermeld **welke deel van het geautomatiseerde werk** op afstand wordt binnengedrongen, de **aard van de software** die wordt gebruikt, de **functies van de software** die worden ingeschakeld en de **categorie van gegevens** waar het onderzoek betrekking op heeft.
- Doordat uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier vallen ter beschikking kunnen komen van het **tactisch team**, worden de gegevens van derden **zoveel mogelijk beschermd.**

Factsheet De wettelijke regelingen in buurlanden

Nederland in internationale context

- De dilemma's die het karakter van cyberspace meebrengt voor de taak van de overheid om de rechtsstaat te handhaven spelen niet alleen in Nederland maar evenzeer in andere landen.
- De benadering die in andere Europese landen gekozen wordt is verschillend.
- Grofweg kunnen twee verschillende benaderingen worden onderscheiden. Ten eerste landen die actief inspelen op de huidige ontwikkelingen en met nieuwe wetgevende voorstellen komen om de praktijk duidelijke kaders te bieden. Ten tweede landen die vooralsnog geen additionele handvaten voor de opsporing in het digitale domein bieden of waar de praktijk opereert op basis van een ruime interpretatie van traditionele bevoegdheden.
- De Nederlandse regering geeft de voorkeur aan heldere kaders voor de opsporing en transparantie over hoe met de huidige technologische ontwikkelingen wordt omgegaan.

Landen met vergelijkbare bevoegdheden

- Frankrijk. In juni van dit jaar is een wettelijke regeling aangenomen die toestaat dat, wanneer de behoefte aan informatie met betrekking tot een ernstig misdrijf dit vereist, heimelijk een technisch hulpmiddel wordt geïnstalleerd met het doel toegang te verkrijgen tot elektronische gegevens, deze op te slaan, te bewaren en over te dragen. Waarborgen zijn onder andere:
    - gemotiveerde beslissing van de rechter-commissaris
    - een nauwkeurige omschrijving van het strafbare feit, de exacte locatie of gedetailleerde omschrijving van de geautomatiseerde systemen voor het verwerken van gegevens, en de duur van de maatregel.
    - Het op elektronische wijze aanbrengen en verwijderen van het technische middel gebeurt op gezag en onder toezicht van de rechter-commissaris.
- Verenigd Koninkrijk. Op 2 november 2016 is de Investigatory Powers Bill aangenomen. De wet is een revisie van de bevoegdheden van de inlichtingendiensten en de opsporingsdiensten. Deze wet bevat de bevoegdheid tot binnendringen in geautomatiseerd werk voor de

opsporingsdiensten, in het VK equipment interference genoemd. De mogelijkheden zijn vergelijkbaar met het Nederlandse wetsvoorstel.
- Noorwegen. In juni van dit jaar is een wettelijke regeling aangenomen die het toestaat om met behulp van een technisch hulpmiddel niet-publiekelijke informatie uit een geautomatiseerd werk te lezen wanneer iemand wordt verdacht van een feit dat wordt bestraft met een gevangenisstraf van 10 jaar of meer, of voor een aantal aangewezen strafbare feiten, waaronder witwassen, terrorisme en mensenhandel.

Landen met minder (of minder geëxpliciteerde) bevoegdheden
- Duitsland. Duitsland kent een traditioneel bevel tot doorzoeking en inbeslagname van gegevensdragers. Daarnaast is er een mogelijkheid tot een "verlengd" onderzoek aan de gegevensdrager (StPO sectie 110(3)). Als er een risico is dat bewijs verloren gaat kunnen de Duitse opsporingsdiensten ook een gegevensdrager die fysiek niet verbonden is met de originele gegevensdrager, maar wel via deze gegevensdrager toegankelijk is, doorzoeken. Data die mogelijk belangrijk is voor het onderzoek mag dan worden veiliggesteld. Officieel mag geen onderzoek worden gedaan buiten Duits grondgebied. Voor de uitvoering van deze bevoegdheid wordt daarom steeds aangenomen dat de data waartoe toegang wordt verschaft zich (tevens) ook in Duitsland bevindt. De bewijslast voor het bewijzen dat dit niet het geval is ligt bij de verdachte.
- België. De Belgische wet kent geen bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Bepaalde bevoegdheden die in de Nederlandse wet onder deze bevoegdheid worden geplaatst, kunnen onder de Belgische wet worden geïnterpreteerd als netwerkzoeking. Opsporingsdiensten kunnen een primaire netwerkzoeking verder zetten op eigen informaticasystemen. Zo is het voor hen bijvoorbeeld mogelijk om onder bepaalde voorwaarden gebruik te maken van de gebruikersnaam en het wachtwoord van een Hotmailaccount. Of, wanneer een opsporingsambtenaar via technieken als social engineering een wachtwoord weet te bemachtigen, hiermee onder een valse hoedanigheid of met behulp van een valse sleutel toegang te verkrijgen tot een geautomatiseerd werk.

Factsheet Decryptiebevel

Samenvatting

- Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is het voorstel voor het decryptiebevel aan de verdachte geschrapt
- Met het voorstel voor het decryptiebevel aan de verdachte werd beoogd een extra mogelijkheid (naast de mogelijkheid tot binnendringen) op te nemen om versleutelde gegevens te laten ontsleutelen zodat kennis kan worden genomen van de inhoud van die gegevens met het oog op de waarheidsvinding.
- een decryptiebevel aan de verdachte blijkt zowel juridisch als praktisch nauwelijks haalbaar en komt daarnaast niet voldoende tegemoet aan de behoefte van de opsporingspraktijk.

Bezwaren

- Praktisch: Om het niet uitvoeren van een bevel tot decryptie als misdrijf aan te wijzen is opzet vereist. In de praktijk is dit bijzonder lastig te bewijzen als de verdachte een beroep doet op geheugenverlies of onjuiste gegevens verstrekt
- Technisch: de technische ontwikkeling maakt het mogelijk bestanden op te slaan in het "hidden volume" waarvan de autoriteiten het bestaan niet kunnen bewijzen. Hierdoor kan de verdachte voldoen aan het decryptiebevel zonder alle gegevens beschikbaar te stellen
- Juridisch/Praktisch: Verhouding tot het *nemo tenetur* beginsel (beginsel dat een verdachte niet aan zijn eigen veroordeling hoeft mee te werken).
    - Hier speelt de afweging tussen drie variabelen; (1) de hoogte van de strafbedreiging; (2) de verenigbaarheid met artikel 6 EVRM en (3) het risico van calculerend gedrag door de verdachte.
    - De voorgestelde strafbedreiging van drie jaar gevangenisstraf (zoals in voorgesteld artikel 184b Sv) te riskeren is aanzienlijk hoger dan de zes maanden gevangenisstraf waarover het EHRM zich in de zaak O'Heaney en Mc Guiness tegen Ierland heeft uitgesproken. Verlaging van die strafbedreiging kan bijdragen aan de kans dat het decryptiebevel door het EHRM verenigbaar wordt geacht met artikel 6 EVRM. Echter, een dergelijke verlaging zal het risico op calculerend gedrag door de verdachte navenant doen toenemen.

- In de afweging tussen deze drie variabelen is er geen uitkomst die zowel juridisch als praktisch een gunstige uitkomst heeft voor de in het wetsvoorstel beoogde doel.

Gemaakte afweging en conclusie

- Het decryptiebevel aan de verdachte leidt niet tot het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing, of is niet verenigbaar met art. 6 EVRM.
- De regering geeft daarom de voorkeur aan de bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk. Met behulp van deze bevoegdheid kunnen wachtwoorden en inlogcodes worden achterhaald en vastgelegd, zodat de versleutelde bestanden eenvoudig kunnen worden ontsleuteld en de versleutelde gegevens daadwerkelijk beschikbaar komen voor de opsporing. Bijkomend voordeel is dat deze bevoegdheid heimelijk wordt toegepast, zodat gedurende het opsporingsonderzoek gegevens kunnen worden verzameld.

Factsheet Kwetsbaarheden

Kwetsbaarheden
Hardware en software bevat praktisch altijd kwetsbaarheden die het mogelijk maken het geautomatiseerd werk binnen te dringen. Criminelen en buitenlandse inlichtingendiensten maken hier gebruik van. De overheid heeft belang bij het verhelpen van kwetsbaarheden ter voorkoming van criminaliteit en andere ongewenste activiteiten.

Fabrikanten van hardware en software kunnen kwetsbaarheden verhelpen door voor het product een patch of update beschikbaar te stellen, of een nieuwe versie te maken. Alleen als een kwetsbaarheid bij de fabrikant bekend is, is deze in staat deze te verhelpen. De overheid stimuleert het melden van kwetsbaarheden, onder meer door het beleid voor *responsible disclosure* en de ondersteuning van het NCSC.

Gebruik kwetsbaarheden door overheidsdiensten
De AIVD en de MIVD hebben de bevoegdheid tot binnendringen in een geautomatiseerd werk, en het wetsvoorstel Computercriminaliteit III bevat deze bevoegdheid voor de politie. Voor de inzet van deze bevoegdheid is het gebruik van kwetsbaarheden vaak nodig. De overheid heeft daarom ook een belang bij het bestaan van kwetsbaarheden.

Afweging Kamerbrief
De kern van de Kamerbrief betreft de vraag of de overheid kwetsbaarheden meldt als zij daar kennis van heeft. Dat is alleen van belang als het om *onbekende* kwetsbaarheden gaat, i.e. kwetsbaarheden die nog niet bekend zijn bij de fabrikant. De AIVD en de MIVD zullen volgens de Kamerbrief belangendragers informeren, behoudens wettelijk bepalingen om dat na te laten. Gezien de wettelijke regelingen voor geheimhouding van bronbescherming en werkwijze zullen zij veel kwetsbaarheden niet melden. Voor de opsporing is er voor gekozen kwetsbaarheden in beginsel te melden gezien het belang voor het beperken van criminaliteit. Alleen in uitzonderlijke gevallen kan het OM besluiten het melden van een kwetsbaarheid uit te stellen, bijvoorbeeld in het belang van een specifiek opsporingsonderzoek of omdat het hardware of software betreft die vrijwel alleen door criminelen wordt gebruikt. Dit uitstel is in de Kamerbrief niet aan een termijn gebonden.

De Kamerbrief spreekt overigens over kwetsbaarheden waarvan *aannemelijk* is dat ze onbekend zijn. Het is niet de bedoeling dat de politie voor elke (mogelijke) kwetsbaarheid de opdracht krijgt te onderzoeken of deze bij de fabrikant bekend is. Dat kan de opsporingscapaciteit te zeer belasten. Mocht kennis over een grote hoeveelheid kwetsbaarheden worden gevonden, dan kan er voor worden gekozen deze als geheel voor nadere analyse aan het NCSC of, indien bekend, aan de fabrikanten zelf ter beschikking te stellen.

Het OM werkt aan de inrichting van een proces om het besluit tot het uitstellen van een melding zorgvuldig te nemen. Daarbij is van belang dat het besluit wordt genomen op basis van voldoende kennis en niet alleen op basis van het individuele opsporingsonderzoek waar de kwetsbaarheid in is ontdekt. Het melden van een kwetsbaarheid kan namelijk gevolgen hebben voor andere onderzoeken en voor de werkwijze van de politie. Op dit moment wordt gedacht aan een besluit door de Hoofdofficier van het Landelijk Parket, op basis van adviezen van de Landelijk Officier Cybercrime en de Landelijk Officier voor Opsporingsmiddelen. Ook kan er voor worden gekozen om de melding niet direct aan de fabrikant, maar via het NCSC te doen, 7-12-14

Internationale markt voor kwetsbaarheden
Op het internet wordt kennis over kwetsbaarheden verhandeld. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden. Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Wel kunnen bepaalde softwarepakketten onderhevig zijn aan exportcontrole.

Aankoop van kwetsbaarheden door de overheid
Het is op dit moment niet voorzien dat de politie kennis over specifieke kwetsbaarheden zal aankopen ten behoeve van de bevoegdheid tot binnendringen in geautomatiseerd werk. Eén reden hiervoor is dat na aankoop nog veel specialistische inzet is vereist om daadwerkelijk gebruik daarvan te kunnen maken. Wel is het voorzien dat de politie software aankoopt die gebruik maakt van kwetsbaarheden. Het is niet te verwachten dat de producenten van dergelijke software de broncode en de kwetsbaarheden die worden benut, bekend stellen. Daarom zal het voor de politie onbekend blijven of die software gebruik maakt van *onbekende* kwetsbaarheden.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Aangiftebereidheid

Kamerlid :

Beantwoording : DGPOL

Vraag: De aangiftebereidheid voor cybercrime en gedigitaliseerde criminaliteit moet worden verbeterd. Ik denk dat een publiekscampagne om de awareness bij burgers en bedrijven te vergroten een dringend nodig is. Hoe kijkt de minister hier tegenaan?

Antwoord:

- Ik ben met u van mening dat het voor een effectievere aanpak van criminaliteit een zo hoog mogelijke aangiftebereidheid van groot belang. Dat geldt ook zeker voor cybercrime en gedigitaliseerde criminaliteit.
- In mijn brief van 15 september jl. over de aangiftebereidheid heb ik een aantal maatregelen aangekondigd om het doen van aangifte aan te moedigen.
- Ten eerste moet de dienstverlening van de politie verder verbeterd worden, en moet het aangifteproces zo optimaal mogelijk ingericht worden. Daartoe moeten onder meer laagdrempelige aangiftemogelijkheden worden ontwikkeld en de bekendheid van intake- en servicemedewerkers met cyberdelicten worden verbeterd.
- Daarnaast zijn er specifiek voor cybercrime en gedigitaliseerde criminaliteit verschillende meldpunten

opgericht waarin de politie samenwerkt met partners om vormen van gedigitaliseerde criminaliteit aan te pakken. Voorbeelden hiervan zijn het landelijk meldpunt internetoplichting (LMIO), het meldpunt kinderporno en het centraal meld- en informatiepunt identiteitsfraude en –fouten. Hier worden meldingen en aangiften verzameld en verrijkt met opsporingsinformatie.

- Ook zijn er andere initiatieven zoals bijvoorbeeld de NCSC Handreiking Cybercrime. Met deze handleiding wordt onder meer beoogd de aangiftebereidheid en de aangiftekwaliteit van partijen te verbeteren.
- Het is mijn verwachting dat deze maatregelen rendement opleveren. Het stimuleren van de aangiftebereidheid vereist structurele maatregelen zoals hierboven genoemd. Een meer incidentele actie zoals een publiekscampagne levert op termijn minder op.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Definitie geautomatiseerd werk

Kamerlid :

Beantwoording : DRC

Vraag: Waarom is de definitie van geautomatiseerd werk zo ruim? Gaat de politie pacemakers hacken en auto's tot stoppen dwingen?

Antwoord:

- De definitie van geautomatiseerd werk sluit aan bij de definitie van het Cybercrimeverdrag uit 2001. Deze definitie is overigens minder ruim dan in EU-regelgeving.
- Pacemakers en delen van auto's, zoals navigatiesystemen, vallen onder deze definitie. Dat wil niet zeggen dat we pacemakers gaan binnendringen.
- De regering heeft er voor gekozen geen enkel soort geautomatiseerd werk categorisch uit te sluiten voor onderzoek. Dit kan namelijk leiden tot de situatie dat criminelen vooral deze geautomatiseerde werken gebruiken voor het plegen van strafbare feiten, juist omdat de overheid dan geen bewijs kan vergaren.
- Tevens is een dergelijke inperking in het licht van de snelle technologische ontwikkelingen niet toekomstbestendig.
- Uiteraard vraagt het binnendringen bij bepaalde geautomatiseerde werken een zeer hoge zorgvuldigheid.

De beperkingen in de uitvoering van de bevoegdheid worden voornamelijk bepaald door de proportionaliteit- en subsidiariteitstoets.

- In veel situaties zal worden gekozen voor andere methoden, bijvoorbeeld het vorderen van gegevens, met medewerking van systeembeheerders.
- In de praktijk kan ik me op dit moment geen situatie voorstellen waarin het proportioneel is dat de politie een pacemaker zal binnendringen.
- Wel kan de politie een geautomatiseerd werk in een auto binnendringen, maar niet om deze tot stilstand te dwingen. Dat is namelijk niet genoemd in het wetsvoorstel als mogelijk doel van het binnendringen. Wel kan de politie zo’n werk binnendringen om gegevens over te nemen.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Financiën

Kamerlid :

Beantwoording : DRC

Vraag: Waarom krijgt de politie geen extra middelen voor de uitvoering van het wetsvoorstel?

Antwoord:

- De politie ontvangt een bijzondere bijdrage van € 13,8 mln per jaar voor de verdere professionalisering in een gedigitaliseerde wereld en de bestrijding van cybercrime. Onder meer de aanschaf en implementatie van ICT-hulpmiddelen wordt hieruit gefinancierd.
- Ook de voorbereiding van de implementatie van dit wetsvoorstel wordt hier grotendeels uit bekostigd.
- De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie.
- De nieuwe bevoegdheid leidt derhalve niet tot een structurele toename van de totale opsporingsinspanning.
- Overigens is aan de begroting van de politie een extra bedrag toegevoegd voor het aanpakken van cybercrime. Voor 2017 is dit 1,4 miljoen euro, voor 2018 wordt dit bedrag verhoogd tot 1,5 miljoen euro, ten behoeve van de versterking van de personele en materiële capaciteit.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Kopen software, markt kwetsbaarheden

Kamerlid :

Beantwoording : DRC

Vraag: Gaat de politie software kopen van bedenkelijke bedrijven? Houden we met het kopen van dergelijke software de markt voor onbekende kwetsbaarheden in stand?

Antwoord:

- Voor de selectie van bedrijven van wie software wordt gekocht geldt de **bestaande regelgeving voor inkoop** van de politie.
- Bedrijven die software produceren waarmee kan worden binnengedrongen **vermelden niet van welke kwetsbaarheden die software gebruik maakt** of hoe het bedrijf kennis daarover heeft verkregen.
- Het **beperken van onderzoek** naar kwetsbaarheden wordt **niet wenselijk** geacht. Dergelijke kennis kan bijdragen aan de veiligheid van systemen.

- Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de **verkoop ervan aan bepaalde partijen onwenselijk**.
- De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen,

waardoor het **lastig is deze markt aan controle te onderwerpen**.

- De verkoop van *intrusion software* die gebruik maakt van kwetsbaarheden is in bepaalde omstandigheden onderhevig aan **exportcontrole.**

Onderwerp : WV Computercriminaliteit III

Onderwerp : Financiën

Kamerlid :

Beantwoording : DRC

Vraag: Waarom krijgt de politie geen extra middelen voor de uitvoering van het wetsvoorstel?

Antwoord:

- De politie ontvangt een bijzondere bijdrage van € 13,8 mln per jaar voor de verdere professionalisering in een gedigitaliseerde wereld en de bestrijding van cybercrime. Onder meer de aanschaf en implementatie van ICT-hulpmiddelen kan hieruit worden gefinancierd.
- Ook de voorbereiding van de implementatie van dit wetsvoorstel wordt hier grotendeels uit bekostigd.
- De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie.
- De nieuwe bevoegdheid leidt derhalve niet tot een structurele toename van de totale opsporingsinspanning.
- Overigens is aan de begroting van de politie een extra bedrag toegevoegd voor het aanpakken van cybercrime. Voor 2017 is dit 1,4 miljoen euro, voor 2018 wordt dit bedrag verhoogd tot 1,5 miljoen euro, ten behoeve van de versterking van de personele en materiële capaciteit.

Met opmerkingen 10.2.6 (1): 12-14

Met opmerkingen 10.2.6 (2): 12-14

From 10.2.e @politie.nl>
Subject **RE: CC3 misschien in de Kamer volgende week**
To 10.2.e - BD/DRC/CV" 10.2.e @minvenj.nl>, 10.2.e @om.nl>, 10.2.e @politie.nl>, 10.2.e - BD/DGPOL/PBT/PT" 10.2.e @minvenj.10.2.e @klpd.politie.nl>, 10.2.e @klpd.politie.nl>, 10.2.e @om.nl>, 10.2.e (Parket-Generaal) (10.2.e @om.nl>
Date 18 november 2016 8:55:59 CET

Beste 10.2.e e.a.,

Ik heb er even doorgelezen. Bij de financiën wil ik wel opmerken (wellicht niet voor de QenA) dat we op dit moment gebruik maken van de cybercrime gelden, maar dat dit op het moment dat we echt aan het werk gaan met het team Binnendringen echt niet voldoende gaat zijn. De aanschaf van software (incl. licentiekosten) kan zomaar voor de aanschaf in de 6 euro gaat lopen met de bijbehorende licentiekosten van ongeveer 20% per jaar. Daarnaast hebben we het over geavanceerde hardware die niet in het standaardpakket van de Dienst ICT valt. Neem daarbij hoog technisch gekwalificeerd personeel en dan kom je al gauw op jaarlijkse kosten van minimaal 6 euro per jaar. Om dit op te vangen binnen de reguliere begroting van de NP gaat nog een uitdaging worden. We zullen als politie keuzes moeten gaan maken over wat we wel en niet meer gaan doen en wellicht ook keuzes maken over de manier waarop we bepaalde teams gaan inzetten of niet meer gaan inzetten. 7-12 Dat zou o.a. OT-capaciteit kunnen schelen in de toekomst. Dit soort ideeen zullen worden meegenomen in het PID zoals dat op dit moment door het project CCIII wordt opgesteld. Dit PID zal de basis zijn voor het team Binnendringen en zal beschrijven (o.a.) welk personeel er nodig is, hoe groot zo'n team moet zijn, welke technische middelen nodig zijn, welke opleidingseisen nodig zijn, welke huisvesting noodzakelijk is, hoeveel het gaat kosten en waar we mogelijk kosten kunnen besparen om dit zo budgetneutraal mogelijk in te voeren.
Het vergt ook nog een behoorlijke aanpassing van de werkprocessen bij de politie. Het gaat dus wellicht iets te kort door bocht om te zeggen dat dit niet leidt tot een structurele toename van de opsporingscapaciteit.

Ik kijk straks even verder. Zit zo even in overleg tot 11 uur. Indien snel antwoord nodig is, graag even een sms! Dan loop ik uit de vergadering.
Groet,
10.2.e

10.2.e
9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M: +31 (0)6 10.2.e
E 10.2.e @politie.nl

Van: 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Verzonden: vrijdag 18 november 2016 11:10
Aan: 10.2.e 10.2.e - BD/DRC/CV'; 10.2.e (Parket-Generaal); 10.2.e 10.2.e (Landelijk Parket Rotterdam); 10.2.e 10.2.e 10.2.e 10.2.e - BD/DGPOL/PBT/PT; 10.2.e FP Amsterdam)
CC: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e BD/DCS/ACSB; 10.2.e (Landelijk Parket Rotterdam)
Onderwerp: Input OM op stukken behandeling CCIII
Bijlagen: QA.Gegevens van derden Bijvangst.docx; Factsheet decryptiebevel met aanvullingen.docx; Factsheet kwetsbaarheden met aanvullingen.docx; QA definitie en pacemaker aanpas. OM(3).docx; QA software kopen rev PaG (2).docx

Goedemorgen,

Hierbij de opmerkingen/ tekstwijzigingen op de stukken vanuit het OM.

Gegevens van niet verdachte personen: zie opmerkingen in bijlage
Factsheet decryptiebevel: zie opmerkingen in bijlage
Factsheet kwetsbaarheden: zie opmerkingen in bijlage
QA definitie geautomatiseerd werk/ pacemaker: zie opmerkingen in bijlage
QA software kopen: zie opmerkingen in bijlage
QA aangiftebereidheid: toevoegen in tekst campagneweek Alert Online om awareness bij burger en bedrijf te vergroten
QA financiën: geen opmerkingen, zie opmerking politie
Factsheet de wettelijke regelingen in buurlanden: geen opmerkingen

De beantwoording op de vraag over encryptie 7-12 volgt zo!

Met vriendelijke groet,

10.2.e

9

Openbaar Ministerie
Landelijk Parket
National public prosecutor's office

Postbus/ box 395 - 3000 AJ Rotterdam

✆ *+31 (0) 6 10.2.e*
✉ 10.2.e *@om.nl*

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Beantwoording : DWJZ

Vraag: Hoe kan een privacy inbreuk van niet-verdachte personen worden voorkomen?

Antwoord:

- Inzage in communicatie van andere, niet-verdachte personen kan bij de uitvoering van de bevoegdheid **niet worden uitgesloten**. Op het moment dat een verdachte via zijn geautomatiseerde werk communiceert over strafbare handelingen, is er immers altijd een wederpartij die deze informatie ontvangt en die niet perse al een verdachte is. Die communicatie levert wel relevant bewijsmateriaal op in de zaak van de verdachte
- Dit is thans niet anders bij de toepassing van bevoegdheden als het aftappen van communicatie of het direct afluisteren.
- Wel zijn de **wettelijke voorwaarden** voor de uitoefening van deze bevoegdheid zodanig dat zoveel mogelijk wordt voorkomen dat de opsporing in aanraking komt met gegevens van derden. De voorwaarden zijn strenger dan bijvoorbeeld de bevoegdheid tot tappen waar een niet verdacht persoon ook getapt kan worden.
- Dit betreft ten eerste het vereiste dat het geautomatiseerde werk **bij de verdachte in gebruik is**.

In het bevel van de officier van justitie dient te worden vermeld op welke bevoegdheid het bevel betrekking heeft (bepalen locatie, ter uitvoering van tapbevel of OVC of overname gegevens). ER zal duidelijkheid zijn over de aard en functionaliteit van het technische hulpmiddel waarmee de bevoegdheid wordt uitgevoerd, alsmede het onderdeel van het geautomatiseerde systeem (zoals bijvoorbeeld het besturingssysteem, of bepaalde vormen van communicatiesoftware) waarop het bevel zich richt.

- Daarbij kan in verband met de inzet van een dergelijk middel niet worden aangegeven hoe wordt binnengedrongen, maar wordt wel

Met opmaak: Standaard, Afstand Na: 12 pt, Geen opsommingstekens of nummering, Zwevende regels niet voorkomen, Spatiëring tussen Aziatische en Latijnse tekst niet aanpassen, Spatiëring tussen Aziatische tekst en nummers niet aanpassen

Met opmaak: Lettertype: Verdana

Met opmaak: Tekstkleur: Aangepaste kleur (RGB(26;23;24)), Engels (Verenigde Staten)

aangegeven op welke wijze uitvoering aan het bevel wordt gegeven en waar het bevel in wordt beperkt, gelet op de privacyrechten van de gebruiker(s) van het geautomatiseerde werk en/of derden waarmee wordt gecommuniceerd. ~~**welke deel van het geautomatiseerde werk** op afstand wordt binnengedrongen, de **aard van de software** die wordt gebruikt, de **functies van de software** die worden ingeschakeld en de **categorie van gegevens** waar het onderzoek betrekking op heeft.~~

- Doordat slechts~~uitsluitend~~ de gegevens die binnen de reikwijdte van het bevel van de officier vallen ter beschikking kunnen komen van het **tactisch team**, worden de gegevens van derden **zoveel mogelijk beschermd.**

Factsheet Decryptiebevel

Samenvatting

- Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is het voorstel voor het decryptiebevel aan de verdachte geschrapt
- Met het voorstel voor het decryptiebevel aan de verdachte werd beoogd een extra mogelijkheid (naast de mogelijkheid tot binnendringen) op te nemen om versleutelde gegevens te laten ontsleutelen zodat kennis kan worden genomen van de inhoud van die gegevens met het oog op de waarheidsvinding.
- een decryptiebevel aan de verdachte blijkt zowel juridisch als praktisch ~~nauwelijks~~ moeilijk haalbaar en komt daarnaast niet voldoende tegemoet aan de behoefte van de opsporingspraktijk.

Bezwaren

- Praktisch: Om het niet uitvoeren van een bevel tot decryptie als misdrijf aan te wijzen is opzet vereist. In de praktijk is dit bijzonder lastig te bewijzen als de verdachte een beroep doet op geheugenverlies of onjuiste gegevens verstrekt
- Technisch: de technische ontwikkeling maakt het mogelijk bestanden op te slaan in het "hidden volume" waarvan de autoriteiten het bestaan ~~niet~~ moeilijk kunnen bewijzen. Hierdoor kan de verdachte voldoen aan het decryptiebevel zonder alle gegevens beschikbaar te stellen
- Juridisch/Praktisch: Verhouding tot het *nemo tenetur* beginsel (beginsel dat een verdachte niet aan zijn eigen veroordeling hoeft mee te werken).
    - Hier speelt de afweging tussen drie variabelen; (1) de hoogte van de strafbedreiging; (2) de verenigbaarheid met artikel 6 EVRM en (3) het risico van calculerend gedrag door de verdachte.
    - De voorgestelde strafbedreiging van drie jaar gevangenisstraf (zoals in voorgesteld artikel 184b Sv) te riskeren is aanzienlijk hoger dan de zes maanden gevangenisstraf waarover het EHRM zich in de zaak O'Heaney en Mc Guiness tegen Ierland heeft uitgesproken. Verlaging van die strafbedreiging kan bijdragen aan de kans dat het decryptiebevel door het EHRM verenigbaar wordt geacht met artikel 6 EVRM. Echter, een dergelijke verlaging zal het risico op calculerend gedrag door de verdachte navenant doen toenemen.

- In de afweging tussen deze drie variabelen is er geen uitkomst die zowel juridisch als praktisch een gunstige uitkomst heeft voor de in het wetsvoorstel beoogde doel.

Gemaakte afweging en conclusie

- Het decryptiebevel aan de verdachte leidt niet tot het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing, of is niet verenigbaar met art. 6 EVRM.
- De regering geeft daarom de voorkeur aan de bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk. Met behulp van deze bevoegdheid kunnen wachtwoorden en inlogcodes worden achterhaald en vastgelegd, zodat de versleutelde bestanden eenvoudig kunnen worden ontsleuteld en de versleutelde gegevens daadwerkelijk beschikbaar komen voor de opsporing. Bijkomend voordeel is dat deze bevoegdheid heimelijk wordt toegepast, zodat gedurende het opsporingsonderzoek gegevens kunnen worden verzameld.

12-14

Met opmaak: Onderstrepen

Met opmaak: Standaard, Geen opsommingstekens of nummering

Met opmaak: Lettertype: Verdana, 12 pt

Factsheet Kwetsbaarheden

Kwetsbaarheden
Hardware en software bevat praktisch altijd kwetsbaarheden die het mogelijk maken het geautomatiseerd werk binnen te dringen. 12-14

Criminelen en buitenlandse inlichtingendiensten maken hier gebruik van. De overheid heeft belang bij het verhelpen van kwetsbaarheden ter voorkoming van criminaliteit en andere ongewenste activiteiten.

Fabrikanten van hardware en software kunnen kwetsbaarheden verhelpen door voor het product een patch of update beschikbaar te stellen, of een nieuwe versie te maken. ~~Alleen~~ Aals een kwetsbaarheid bij de fabrikant bekend is of kan zijn, is deze in staat deze te verhelpen. (opm 9, ik heb alleen weggehaald. 12-14 De overheid stimuleert het melden van kwetsbaarheden, onder meer door het beleid voor *responsible disclosure* en de ondersteuning van het NCSC.

Gebruik kwetsbaarheden door overheidsdiensten
De AIVD en de MIVD hebben de bevoegdheid tot binnendringen in een geautomatiseerd werk, en het wetsvoorstel Computercriminaliteit III bevat deze bevoegdheid voor de politie. Voor de inzet van deze bevoegdheid is het gebruik van kwetsbaarheden vaak nodig. ~~De overheid heeft daarom ook een belang bij het bestaan van kwetsbaarheden~~. De inschatting is dat door de politie gebruik kan worden gemaakt van bekend geworden kwetsbaarheden die -vanwege velerlei redenen- door een fabrikant (nog) niet zijn gepatcht.

Opm9

7-12-14

Afweging Kamerbrief
De kern van de Kamerbrief betreft de vraag of de overheid kwetsbaarheden meldt als zij daar kennis van heeft. Dat is alleen van belang als het om *onbekende* kwetsbaarheden gaat, i.e. kwetsbaarheden die nog niet bekend zijn bij de fabrikant. De AIVD en de MIVD zullen volgens de Kamerbrief belangendragers informeren, behoudens wettelijk bepalingen om dat na te laten. Gezien de wettelijke regelingen voor geheimhouding van bronbescherming en werkwijze zullen zij veel kwetsbaarheden niet melden. Voor de opsporing is er voor gekozen kwetsbaarheden in beginsel te melden gezien het belang voor het beperken van criminaliteit. Alleen in uitzonderlijke gevallen kan het OM besluiten het melden van een onbekende kwetsbaarheid uit te stellen, bijvoorbeeld in het belang van een specifiek opsporingsonderzoek of omdat het hardware of software betreft die vrijwel alleen door criminelen wordt gebruikt. Dit uitstel is in de Kamerbrief niet aan een termijn gebonden.

De Kamerbrief spreekt overigens over kwetsbaarheden waarvan *aannemelijk* is dat ze onbekend zijn. Het is niet de bedoeling dat de politie voor elke (mogelijke) kwetsbaarheid de opdracht krijgt te onderzoeken of deze bij de fabrikant bekend is of hoort te zijn. Dat is niet de taak van een opsporingsapparaat, maar van de cybersecurityindustrie en ~~Dat~~zal ~~kan~~ de opsporingscapaciteit te zeer belasten. Mocht kennis over een grote hoeveelheid kwetsbaarheden worden gevonden, dan kan er voor worden gekozen deze als geheel voor nadere analyse aan het NCSC of, indien bekend, aan de fabrikanten zelf ter beschikking te stellen.

Het OM werkt aan de inrichting van een proces om het besluit tot het uitstellen van een melding van een onbekende kwestbaarheid zorgvuldig te nemen. Daarbij is van belang dat het besluit wordt genomen op basis van voldoende kennis van de kwetsbaarheid en niet alleen op basis van het individuele opsporingsonderzoek waar de onbekende kwetsbaarheid in is ontdekt. Het melden van een onbekende kwetsbaarheid kan namelijk gevolgen hebben voor andere onderzoeken en voor de werkwijze van de politie. Op dit moment wordt gedacht aan een besluit door de Hoofdofficier van het Landelijk Parket, op basis van adviezen van de Landelijk Officier Cybercrime en de Recherche Officier van het Landelijk Parket~~Landelijk Officier voor Opsporingsmiddelen~~.
Ook kan er voor worden gekozen om de melding niet direct aan de fabrikant, maar via het NCSC te doen.~~, bijvoorbeeld indien de herkomst van de kennis van de kwetsbaarheid onbekend dient te blijven.~~

Internationale markt voor kwetsbaarheden
Op het internet wordt kennis over kwetsbaarheden verhandeld. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden. Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Er is immers ook een groeiende industrie die zich richt op het ontdekken van onbekende kwestbaarheden, waarna die in het kader van een responsible disclosure-programma worden gemeld aan de fabrikanten. Vele grote bedrijven zijn bereid om een vergoeding te betalen aan ethisch hackers om geattendeerd te worden op kwestbaarheden en die ontwikkeling moet niet worden beperkt.

Om te voorkomen dat ~~Wel kunnen~~ bepaalde softwarepakketten in handen komen van verkeerde bedrijven of regimes, kunnen sommige softwarepakketten reeds onderhevig ~~zijn~~ zijn aan exportcontrole.

Aankoop van kwetsbaarheden door de overheid
Het is op dit moment niet voorzien dat de politie kennis over specifieke kwetsbaarheden zal aankopen ten behoeve van de bevoegdheid tot binnendringen in geautomatiseerd werk. Eén reden hiervoor is dat na aankoop nog veel specialistische inzet is vereist om daadwerkelijk gebruik daarvan te kunnen maken. Wel is het voorzien dat de politie software aankoopt die in zijn algemeenheid (ook) gebruik maakt van kwetsbaarheden. Het is niet te verwachten dat de producenten van dergelijke software de broncode en de kwetsbaarheden die worden benut,

bekend stellen. Daarom zal het voor de politie onbekend blijven of die software gebruik maakt van *onbekende* kwetsbaarheden.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Definitie geautomatiseerd werk

Kamerlid :

Beantwoording : DRC

Vraag: Waarom is de definitie van geautomatiseerd werk zo ruim? Gaat de politie pacemakers hacken en auto's tot stoppen dwingen?

Antwoord:

- De definitie van geautomatiseerd werk sluit aan bij de definitie van het Cybercrimeverdrag uit 2001. Deze definitie is overigens minder ruim dan in EU-regelgeving.
- Pacemakers en delen van auto's, zoals navigatiesystemen, vallen strikt genomen onder deze definitie. Dat wil uiteraard niet zeggen dat we pacemakers gaan binnendringen.
- De regering heeft er voor gekozen geen enkel soort geautomatiseerd werk categorisch uit te sluiten voor onderzoek. Dit kan namelijk leiden tot de situatie dat criminelen vooral deze geautomatiseerde werken gebruiken voor het plegen van strafbare feiten, juist omdat de overheid dan geen bewijs kan vergaren.
- Tevens is een dergelijke inperking in het licht van de snelle technologische ontwikkelingen niet toekomstbestendig.

- Uiteraard vraagt het binnendringen bij bepaalde geautomatiseerde werken een zeer hoge zorgvuldigheid. De ~~beperkingen in de~~ uitvoering van de bevoegdheid word~~ten voornamelijk bepaald~~ al beperkt door de proportionaliteit- en subsidiariteitstoets.
- In veel situaties zal moeten worden gekozen voor andere methoden, bijvoorbeeld het vorderen van gegevens, met medewerking van systeembeheerders.
- In de praktijk kan ik me op dit moment geen situatie voorstellen waarin het proportioneel is dat de politie een pacemaker zal binnendringen.
- ~~Wel kan d~~De politie kan wel een geautomatiseerd werk in een auto binnendringen, maar heeft niet de bevoegdheid ~~niet~~ om deze tot stilstand te dwingen. ~~Dat is~~ Die bevoegdheid is namelijk niet genoemd in het wetsvoorstel als mogelijk doel van het binnendringen. Wel kan de politie zo'n werk binnendringen om de locatie te bepalen of gegevens over te nemen.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Kopen software, markt kwetsbaarheden

Kamerlid :

Beantwoording : DRC

Vraag: Gaat de politie software kopen van bedenkelijke bedrijven? Houden we met het kopen van dergelijke software de markt voor onbekende kwetsbaarheden in stand?

Antwoord:

- Voor de selectie van bedrijven van wie software wordt gekocht geldt de **bestaande regelgeving voor inkoop** van de politie. 12-14
- Bedrijven die software produceren waarmee kan worden binnengedrongen **vermelden niet van welke kwetsbaarheden die software gebruik maakt** of hoe het bedrijf kennis daarover heeft verkregen.
- Het **beperken van onderzoek** naar kwetsbaarheden wordt **niet wenselijk** geacht. Dergelijke kennis kan bijdragen aan de veiligheid van systemen. 12-14

Met opmerkingen 10.2.e 1]: 12-14

7-12-14

12-14

Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de **verkoop ervan aan bepaalde partijen onwenselijk**.12-14

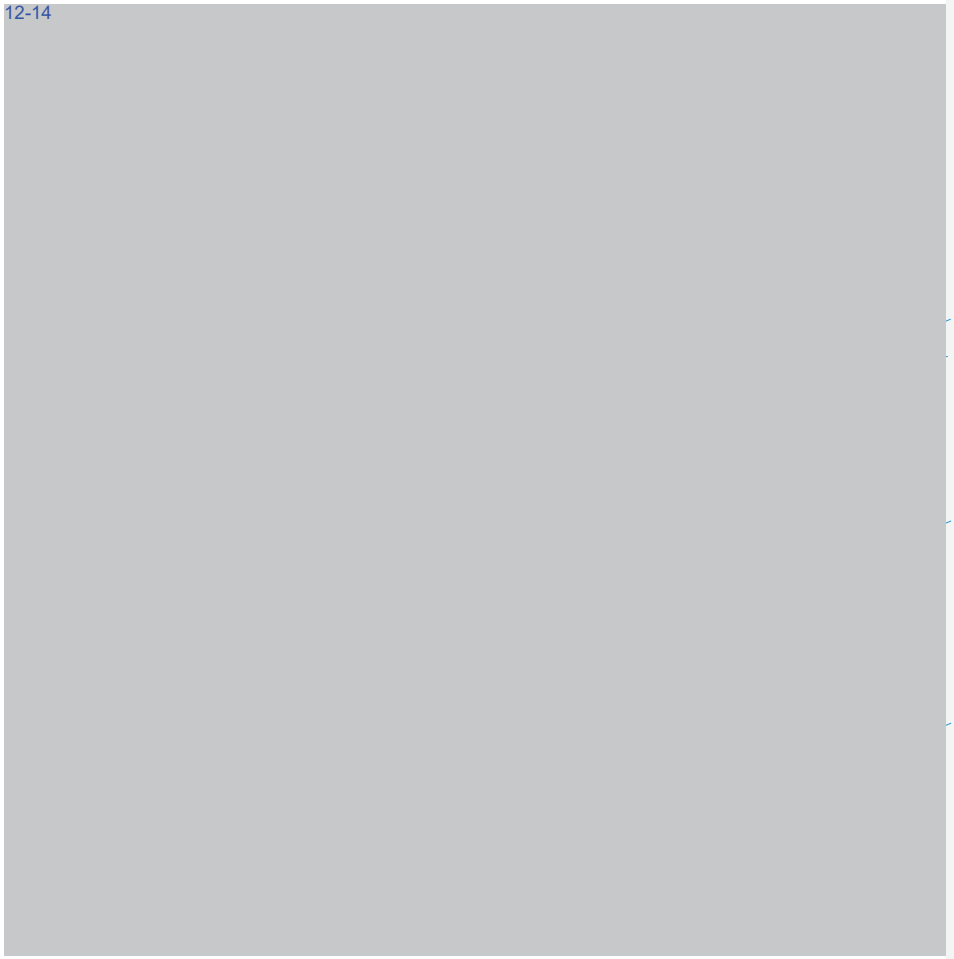
Met opmaak: Lettertype: Verdana, 14 pt

Met opmaak: Standaard, Geen opsommingstekens of nummering

Met opmaak: Lettertype: Verdana, 14 pt

Met opmaak: Standaard, Geen opsommingstekens of nummering

12-14



Met opmaak: Lettertype: Verdana, 14 pt

Met opmaak: Standaard, Inspringing: Links: 0,63 cm, Geen opsommingstekens of nummering

Met opmaak: Lettertype: Verdana, 14 pt

Met opmaak: Lettertype: Verdana, 14 pt

Van: 10.2.e
Verzonden: vrijdag 18 november 2016 11:57
Aan: 10.2.e @politie.nl>
Onderwerp: QA software kopen rev PaG (2).docx

Hallo 10.2.e

Hierbij zoals beloofd de concept Q&A.

Groet,

10.2.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Kopen software, markt kwetsbaarheden

Kamerlid :

Beantwoording : DRC

Vraag: Gaat de politie software kopen van bedenkelijke bedrijven? Houden we met het kopen van dergelijke software de markt voor onbekende kwetsbaarheden in stand?

Antwoord:

- Voor de selectie van bedrijven van wie software wordt gekocht geldt de **bestaande regelgeving voor inkoop** van de politie.
- Bedrijven die software produceren waarmee kan worden binnengedrongen **vermelden niet van welke kwetsbaarheden die software gebruik maakt** of hoe het bedrijf kennis daarover heeft verkregen.
- Het **beperken van onderzoek** naar kwetsbaarheden wordt **niet wenselijk** geacht. Dergelijke kennis kan bijdragen aan de veiligheid van systemen.

- Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de **verkoop ervan aan bepaalde partijen onwenselijk**.
- De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen,

waardoor het **lastig is deze markt aan controle te onderwerpen**.

- De verkoop van *intrusion software* die gebruik maakt van kwetsbaarheden is in bepaalde omstandigheden onderhevig aan **exportcontrole.**

Van: 10.2.e
Verzonden: vrijdag 18 november 2016 12:26
Aan: 10.2.e . - BD/DGPOL/PBT/PT; 10.2.e Parket-Generaal) 10.2.e @om.nl)';10.2.e @klpd.politie.nl)';
10.2.e @om.nl';10.2.e @om.nl)';10.2.e @politie.nl)'; 10.2.e @klpd.politie.nl)'
CC:10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DCS/ACSB
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Beste collega's,

Zojuist hebben we vernomen dat CC3 NIET op de plenaire agenda voor volgende week staat.Veel dank voor

jullie snelle bijdragen. Komende tijd werken we verder aan het dossier.

Groet,
10.2.e

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl]
Verzonden: vrijdag 18 november 2016 12:28
Aan: 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>
CC: 10.2.e @politie.10.2.e BD/DGPOL/PBT/PT10.2.e @minvenj.nl>
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Dat geeft ruimte!
Ook om die financien eens goed te bespreken.

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
SBA
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nl
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 10.2.e @politie.nl]
Verzonden: vrijdag 18 november 2016 12:38
Aan: 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Hoi 10.2.e

Wij gaan ook nog een Q&A maken voor : Hoe gaat de politie dit organiseren?/Gaat het THTC dit uitvoeren?
Lijkt ons goed dat de STAS dat ook voorbereid heeft omdat er nogal eens verwarring over is. Of maken jullie die zelf al?

Groet.
10.2.e

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl]
Verzonden: vrijdag 18 november 2016 12:50
Aan: 10.2.e @politie.nl>
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Ha 10.2.e
Volgens mij ligt daar al een tekstje voor nav vraag uit Kamer via politiek assistent. 10.2.e had input geleverd. Daar is dan een QenA van te maken.
Nu de druk op dit dossier even van de ketel is, ga ik nu even andere dingen doen. Zullen we volgende week alles bij elkaar brengen? We zien elkaar in elk geval de 22 ste toch?

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
SBA
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 10.2.e @politie.nl]
Verzonden: vrijdag 18 november 2016 12:53
Aan: 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: RE: CC3 misschien in de Kamer volgende week

Hi 10.2.e

Zou je die dan kunnen delen? Goed om een tekst voor te bereiden hierop.

We zien elkaar dinsdag. Misschien wel zsm. Fin aanhaken inderdaad. Is het cybercrime overleg nu 14.00 uur dus?
Willen we dat gebruiken voor afstemming?
Dan kan ik 9 vragen aan te haken daarvoor.

Groet,
10.2.e

From 10.2.e - BD/DGPOL/PBT/PT" 10.2.e @minvenj.nl>
Subject **RE: CC3 misschien in de Kamer volgende week**
To 10.2.e - BD/DRC/CV" 10.2.e @minvenj.nl>, 10.2.e @politie.nl>
Date 18 november 2016 13:00:12 CET

Ik vraag 10.2.e (bij deze 10.2.e om laatste versie van de tekst over thtc en functiescheiding etc.

10.2.e willen/kunnen we cc overleg ook gebruiken om cc3 te bespreken? Of past dat niet op de agenda? We hebben dan wel de juiste personen aan de tafel toch?

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
SBA
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 10.2.e
Verzonden: vrijdag 18 november 2016 13:13
Aan: 10.2.e
Onderwerp: RE: QA software kopen rev PaG (2).docx

Hoi 10.2. ,

Onderstaande hebben we destijds geantwoord op de vraag m.b.t. geheimhouding tapsysteem.
Ik zie dat de vraag eigenlijk gaat over hoe je de betrouwbaarheid van het bedrijf toetst met wie je zaken doet.
Voor een antwoord op die vraag kun je denk ik het best bij Inkoop terecht, bijvoorbeeld bij 9

Groeten,

10.2.e

11.
Met betrekking tot het beheer van het tapsysteem vragen de leden van de SP-fractie waarom en op basis waarvan de leverancier van het tapsysteem geheim moet blijven. Sinds wanneer is dat? Wie heeft dat op welk moment bedongen? Welk belang is er met geheimhouding gediend?
De keuze voor geheimhouding van de naam van de huidige leverancier is uit veiligheidsoverwegingen en afgesproken ten tijde van het aangaan van het contract. Achtergrond is kwaadwillenden zo min mogelijk handvatten te geven om het tapproces te frustreren.
In het kader van de komende aanbesteding zal ik heroverwegen of en in welke mate geheimhouding in relatie tot de leverancier noodzakelijk is.

Van: 10.2.e
Verzonden: vrijdag 18 november 2016 13:51
Aan: 10.2.e @politie.nl>
CC: 10.2.e @klpd.politie.nl>
Onderwerp: FW: QA software kopen rev PaG (2).docx

Hi 10.2.e

Ter info. Mbt. geheimhouding tapsysteem is onderstaande geantwoord.

Groet,
10.2.e

Spreektekst wetvoorstel computercriminaliteit III (34 372)

- Ik stel het zeer op prijs dat wij reeds vandaag kunnen spreken over het wetsvoorstel computercriminaliteit III. Dit wetsvoorstel bevat namelijk verschillende onderdelen die voor de opsporing van cybercrime van bijzonder groot belang zijn. Tegelijkertijd is dit ook een wetsvoorstel dat letterlijk veel vragen heeft opgeroepen. In het Verslag hebben de leden van de fracties van Uw Kamer maar liefst ruim 300 vragen gesteld over dit wetsvoorstel. Een groot deel van de vragen had betrekking op het op afstand binnendringen in een geautomatiseerd werk, met het oog op het verrichten van bepaalde onderzoekshandelingen. Deze combinatie van bevoegdheden, dus het binnendringen en het vervolgens uitvoeren van bepaalde onderzoekshandelingen, wordt ~~ook wel~~ aangeduid als het onderzoek in een geautomatiseerd werk.

- Het wetsvoorstel is een reactie op~~sluit aan bij~~ de snelle ontwikkelingen van de technologie en het internet. Helaas heeft de criminaliteit die ontwikkeling beter kunnen bijhouden dan de wetgever. De Wet computercriminaliteit I dateert alweer van 1993 12-14 Die~~ze~~ wet gaf politie en justitie de mogelijkheid om, in het kader van de doorzoeking van een besloten plaats, gegevens vast te leggen van een aldaar aanwezig geautomatiseerd werk. Daarbij was tevens voorzien in de mogelijkheid gegevens van een ander geautomatiseerd werk vast te leggen, dat met het geautomatiseerde werk in verbinding staat. Dit wordt ook wel de netwerkzoeking genoemd. Toentertijd werd aan bedrijfsnetwerken gedacht. De wetgever had echter een vooruitziende blik, want in het licht van de ontwikkeling van cloudcomputing blijkt de netwerkzoeking van bijzondere betekenis voor de bestrijding van cybercrime. En bij de netwerkzoeking is het eigenlijk gebleven. Want ~~Met~~ de ~~w~~Wet computercriminaliteit II, die in 2006 van kracht is geworden, betrof voornamelijk de aanpassing van definities en de verhoging van de straffen. Dit ter implementatie van~~is~~ het Cybercrimeverdrag van de Raad van Europa ~~in de~~ 12-14

- De ontwikkeling van de informatie- en communicatietechnologie heeft echter niet stil gestaan. Het internet is in onze samenleving inmiddels een basisbehoefte geworden, bijna vergelijkbaar met gas en licht. Of het nu gaat om het overmaken van geld, het boeken van een reis of het bestellen van kaartjes voor een concert, we

zijn inmiddels in ons dagelijks handelen vrijwel volledig afhankelijk van internet. En het internet is mobiel geworden, het is niet meer aan huis gebonden. Deze ontwikkelingen bieden helaas ook nieuwe mogelijkheden voor de criminaliteit. Het is enerzijds eenvoudig om via internet in contact te komen mogelijke slachtoffers. Het is anderzijds eenvoudig om het strafbare handelen af te schermen voor de overheid, bijvoorbeeld door gebruik te maken van encryptie, ofwel het versleutelen van gegevens. De wetgever heeft deze ontwikkeling niet kunnen bijhouden. Daarom is het van belang, ruim twintig jaar na de invoering van de Wet computercriminaliteit, dat de bevoegdheden van politie en justitie op peil worden gebracht. 12-14

Met opmaak: Inspringing: Links: 0,63 cm

- Een belangrijk onderdeel van het wetsvoorstel betreft de bevoegdheid om op afstand, dus via het internet, binnen te dringen in een geautomatiseerd werk. In de publiciteit rond dit wetsvoorstel wordt dit ook wel aangeduid als een hackbevoegdheid. De politie heeft vanwege verschillende redenen dringend behoefte aan een hackbevoegdheid. Digitale gegevens worden steeds vaker versleuteld. Kwaadwillenden kunnen ervoor kiezen om gegevens te versleutelen door het gebruik van speciale software. Maar versleuteling vindt ook plaats zonder dat de gebruiker daar invloed heeft, doordat een fabrikant versleuteling als standaard inbouwt in de hard- en software die aan de gebruiker wordt aangeboden. Het ontsleutelen van gegevens wordt steeds lastiger, niet alleen doordat de software steeds geavanceerder wordt maar ook doordat een aanbieder meestal zelf niet in staat is om de encryptie ongedaan te maken. Daardoor is de communicatie van de criminaliteit voor de overheid niet meer toegankelijk, en komt de functie van de staat als hoeder van de veiligheid van burgers in het gedrang. Dit probleem speelt niet alleen bij het aftappen van telecommunicatie. Dit is ook aan de orde bij het opnemen van emailverkeer tussen computers, met behulp van een zogenaamde IP-tap.

- Met de voorgestelde bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk wordt de achterstand dus enigszins 12-14 . Daarbij wordt uiteraard rekening gehouden met de privacy van burgers. 12-14 Het recht op privacy is een heel belangrijk recht, maar het is geen absoluut recht. In bepaalde gevallen moet het ~~echter~~ mogelijk zijn dat de overheid kennis neemt van de communicatie van burgers in het belang van algemeen aanvaarde belangen, zoals de opsporing van strafbare feiten. Een goed voorbeeld is het aftappen van telecommunicatie, als we zouden uitgaan

van een absoluut recht op privacy dan zou dat ook niet mogelijk zijn.

-In dit wetsvoorstel worden ~~U~~uiteraard worden ~~hierbij~~ de waarborgen van de rechtstaat gerespecteerd. Zo moet het gaan om ernstige strafbare feiten. Verder is het binnendringen van een geautomatiseerd werk slechts mogelijk met het oog op het verrichten van bepaalde onderzoeksbevoegdheden. Dit betreft deels bestaande bevoegdheden, zoals het aftappen van telecommunicatie en het direct afluisteren. Dit betreft deels nieuwe bevoegdheden, zoals het overnemen van gegevens.

-Daarbij is voorzien in een voorafgaande rechterlijke toetsing, zodat een adequate rechterlijke controle verzekerd is.

- Door critici dat er geen noodzaak ~~n~~is voor een dergelijke bevoegdheid. Dat is~~, zoals ik hierboven reeds heb aangegeven,~~ echter een ontkenning van de realiteit. Het internet biedt mogelijkheden tot het afschermen van communicatie, die tot nu toe ongekend zijn. Encryptie wordt eerder standaard dan uitzondering. Verder wordt bezwaar gemaakt tegen het gebruik van kwetsbaarheden door de politie. Die kwetsbaarheden zijn er echter al, en ook in ruime mate. Er zijn tal van trojaanse paarden en virussen in omloop waarmee computers en laptops worden geïnfecteerd. Daarvoor wordt ook gebruik gemaakt van emailberichten. De gebruikers weten vaak zelf niet wie er allemaal meekijk~~t~~en. De politie stimuleert god hang- en sluitwerk. Betekent dit nu dat de politie geen gebruik mag maken van een valse sleutel om een woning binnen te dringen? Dat kan de bedoeling toch niet zijn.

  -Als de politie in aanraking komt met een kwetsbaarheid, dan zal dat aan de fabrikant worden gemeld. In uitzonderlijke gevallen moet de mogelijkheid bestaan om een kwetsbaarheid te blijven gebruiken. ~~, b~~Bijvoorbeeld als het gaat om software die vrijwel alleen door criminelen wordt gebruikt of zelfs door hen is geproduceerd. Of om het opsporingsonderzoek niet te frustreren. Dit is alleen mogelijk na een zorgvuldige afweging door het Openbaar Ministerie. Maar we laten de burgers natuurlijk geen onnodig risico lopen. Daarom is het uitgangspunt dat ~~we~~ de kwetsbaarheden aan de leverancier worden gemeld~~en~~, en snel ook.

—

12-14 [redacted]

- Verschillende fracties hebben tijdens de schriftelijke ronde over het wetsvoorstel aangedrongen op toezicht op de uitvoering van de bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk. De regering is voorstander van toezicht, in aanvulling op de rechterlijke toetsing. Vanwege de positie van de rechter spreek ik dan ook liever over 12-14 systeemtoezicht. De Inspectie Veiligheid en Justitie is als rijksinspectie belast met toezicht op de kwaliteit van de taakuitvoering door politie (en Kmar), op basis van de Politiewet 2012. Dit toezicht strekt zich van rechtswege uit over de uitvoering van een bevel tot het op afstand binnendringen van een geautomatiseerd werk. De inspecteurs beschikken over de nodige toezichtbevoegdheden, op basis van de Algemene wetbestuursrecht. Bij nota van wijziging is toezicht door de Inspectie VenJ ook van toepassing verklaard op de taakuitvoering door de ambtenaren van de bijzondere opsporingsdiensten, die niet onder de reikwijdte van de Politiewet 2012 vallen.

- Verder voorziet dit wetsvoorstel in de aanpassing van de strafbaarstelling van het langs digitale weg verleiden van minderjarigen tot ontucht. Soms wordt geprobeerd via de computer een afspraak te maken met een minderjarige. Dit wordt ook wel aangeduid als grooming. Tot voor kort maakte de politie gebruik van de zogenaamde lokpubers. Dat iszij een opsporingsambtenaarren die zich op het internet voordoen als jongere. Inmiddels heeft de rechter geoordeeld dat de tekst van de wet geen ruimte laat voor de inzet van een oudere opsporingsambtenaar als lokpuber. Voorgesteld wordt de 12-14 [redacted] wet aan te passen, zodat deze praktijk weer mogelijk wordt. Daarbij is uiteraard rekening gehouden met het zogenaamde Tallon-criterium. Dit betekent dat de politie zich op geen enkele wijze schuldig maakt aan uitlokking.

- Dan kom ik nu aan de ingediende amendementen. Allereerst behandel ik het amendement met nr. 9 dat is ingediend door de heer Verhoeven van de fractie van D66. Met het amendement wordt beoogd om alle misdrijven waarvoor de bevoegdheid tot het binnendringen in een geautomatiseerd in de wet te regelen. Dit amendement ontraad ik.
  Het gevolg van het amendement is dat het niet mogelijk is om de binnendring- en onderzoeksbevoegdheid in te zetten met het oog op het overnemen van gegevens of ontoegankelijkheid van gegevens voor de opsporing van computercriminaliteit in enge zin. Het gaat hier om ernstige strafbare feiten waarop weliswaar een vrijheidsstraf van minder dan acht jaar is gesteld maar die naar hun aard worden gepleegd met behulp van een geautomatiseerd werk, waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders, en de inzet van andere opsporingsbevoegdheden onvoldoende zicht op resultaat biedt. Het gaat hier om misdrijven als het gebruik van een botnet (art. 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (art. 240b Sr), de verleiding van een minderjarige tot ontucht (art. 248a Sr) de «grooming» (art. 248e Sr).
- Dan kom ik nu toe aan de beantwoording van de vragen.

++

Met opmaak: Lettertype: 12 pt
Met opmaak: Lijstalinea, Met opsommingstekens + Niveau: 1 + Uitgelijnd op: 0,63 cm + Inspringen op: 1,27 cm
Met opmaak: Lettertype: 12 pt
Met opmaak: Lettertype: 12 pt
Met opmaak: Lettertype: 12 pt
Met opmaak: Lettertype: 12 pt
Met opmaak: Lettertype: 12 pt


Niet onder reikwijdte

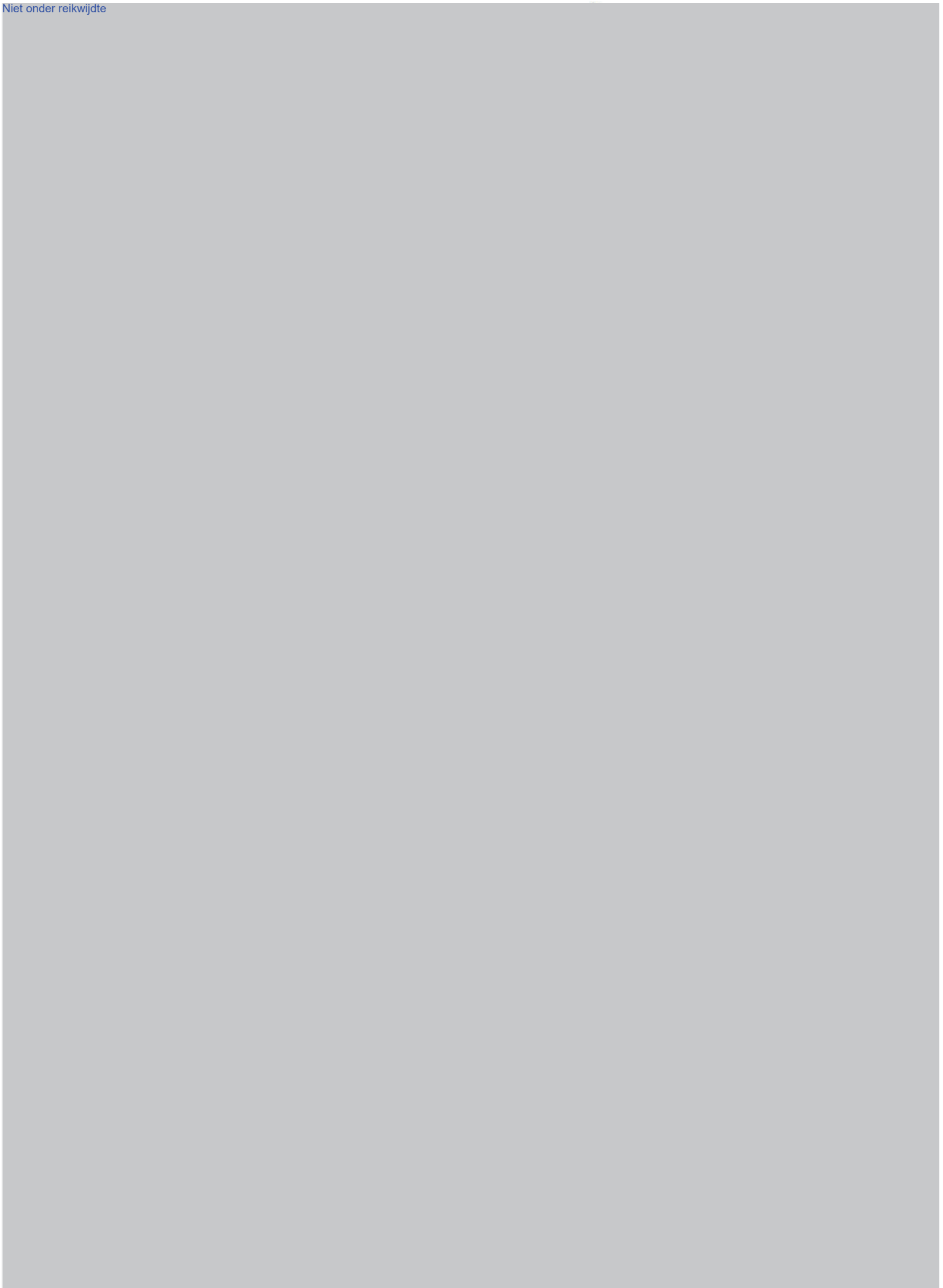

Niet onder reikwijdte


Niet onder reikwijdte


Niet onder reikwijdte


Niet onder reikwijdte

Niet onder reikwijdte


Niet onder reikwijdte

Van: 10.2.e - BD/DRC/CV <10.2.e @minvenj.nl>
Verzonden: maandag 28 november 2016 09:58
Aan: 10.2.e @om.nl); 10.2.e 10.2.e 10.2.e (Parket-Generaal) 10.2.e @om.nl); 10.2.e
CC: 10.2.e - BD/DGPOL/PBT/PT; 10.2.e . - BD/DGPOL/PBT/PT
Onderwerp: CC III

Kamerstukken voor behandeling CC III
https://www.tweedekamer.nl/vergaderingen/plenaire_vergaderingen/details/activiteit?id=2016A04779

10.2.e
9
.....
Ministry of Security and Justice of The Netherlands
Law Enforcement Department
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag | The Netherlands
Postbus 20301 | 2500 EH | Den Haag | The Netherlands
.....
M 10.2.e
10.2.e @minvenj.nl
www.rijksoverheid.nl/venj

.....

From: 10.2.e (Parket-Generaal) [mailto 10.2.e @om.nl]
Sent: Monday, November 28, 2016 11:19 AM
To: 10.2.e
Cc: 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Subject: bespreken QenAs debat CCIII

Hoi 10.2.e,

Zoals besproken zouden wij en petit comité nog de QenA's doornemen.
10.2.e en ik zouden woensdag tussen 14u en 16u kunnen. Heb jij dan tijd? Zo niet: wat zou jou uit komen?

Gr 10.2

Met vriendelijke groet,

10.2.e
Openbaar Ministerie
Parket-Generaal
Afdeling Beleid en Strategie
10.2.e
10.2.e
10.2.e @om.nl
www.om.nl

Van: 10.2.e @politie.nl>
Datum: 28 november 2016 20:53:45 CET
Aan: 10.2.e (Parket-Generaal) 10.2.e @om.nl>
CC: 10.2.e @politie.nl>,10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Onderwerp: Re: bespreken QenAs debat CCIII

Hi 10.2,

Ik heb deze week alleen donderdag nog. Van 14.15 tot 15.30 of na 17.00 uur.
Een alternatief is dat jullie met 10.2.e afstemmen en dat ik meelees?

Met vriendelijke groet,

10.2.e
Staf Korpsleiding Politie
Directie Operatien

Van: 10.2.e (Parket-Generaal) [mailto:10.2.e @om.nl]
Verzonden: dinsdag 29 november 2016 12:05
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Onderwerp: Re: bespreken QenAs debat CCIII

Hoi 10.2.e ,

Donderdag gaat ons niet lukken.
@10.2.e , Kun jij woensdag 14u?

Groet 10.2

Van: 10.2.e @politie.nl>
Datum: 29 november 2016 12:56:46 CET
Aan: 10.2.e (Parket-Generaal) 10.2.e @om.nl>, 10.2.e @politie.nl>
CC: 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Onderwerp: RE: bespreken QenAs debat CCIII

Hoi 10. ,

Helaas niet niet… Ik zit op de themadagen Digitale Opsporing. Anders afstemmen via de mail?

Gr.
10.2.e

Van: 10.2.e (Parket-Generaal) 10.2.e @om.nl]
Verzonden: dinsdag 29 november 2016 13:10
Aan: 10.2.e @politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Onderwerp: RE: bespreken QenAs debat CCIII

Hoi 10.2.e

Dat is dan idd het beste. Ik had politie gevraagd aan te haken omdat ik begreep dat er vanuit jullie enkele suggesties waren tav input op de q&a's. Is het mogelijk deze met ons te delen?

Gr 10.

Van: 10.2.e @politie.nl>
Datum: 1 december 2016 14:56:27 CET
Aan: 10.2.e @politie.nl>,10.2.e (Parket-Generaal)'
<10.2.e @om.nl>
CC:10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>
Onderwerp: RE: bespreken QenAs debat CCIII

Beste 10. ,

Zojuist even met 10.2.e de QenA's besproken. Bijgevoegd zijn de versies waarin onze aanpassingen zijn verwerkt.

- In de QenA over de pacemakers hebben we al jullie opmerkingen geaccepteerd.
- In de QenA over de bijvangst hebben we jullie opmerkingen ook geaccepteerd, met uitzondering van de uitgebreide toelichting over wat niet in het bevel staat.
- In de QenA over de aanschaf van software is het ons voorstel om te blijven bij de originele versie. De input van jullie kan dat gebruikt worden voor een additionele QenA of als achtergrondinformatie worden gebruikt. We zijn het namelijk niet oneens met jullie aanvullingen, maar het lijkt beter om alles zo kort en bondig mogelijk te houden.

10.2.e probeert je nog wel even te bellen.

We horen graag jullie reactie voordat we dit met het departement gaan delen.

Met groet,
10.2.e en 10.2.

From: 10.2.e (Landelijk Parket Rotterdam)" 10.2.e @om.nl>
Subject: **RE: bespreken QenAs debat CCIII**
To: 10.2.e @politie.nl>; 10.2.e @politie.nl>, 10.2.e (Parket-Generaal)" 10.2.e @om.nl>
Date: 2 december 2016 11:49:11 CET

Hoi 10.2.e en 10.2.e

10.2.e en ik zijn akkoord met jullie aanpassingen en opmerkingen. Het mag op deze manier naar het Departement. Ben jij daar ook mee akkoord 10.2.e

Met vriendelijke groet,

10.2.e
9

Openbaar Ministerie
Landelijk Parket
06 – 10.2.e
www.om.nl

Van: 10.2.e
Verzonden: vrijdag 2 december 2016 12:32
Aan: 10.2.e BD/DRC/CV; 10.2.e - BD/DGPOL/PBT/PT; 10.2.e (Parket-Generaal)
CC: 10.2.e
Onderwerp: Doorst: bespreken QenAs debat CCIII
Bijlagen: QA software kopen aanpassingen politie.docx; QA definitie en pacemaker aanpas OM(3) aanpassingen politie.docx; QA Gegevens van derden Bijvangst aangepast Politie.docx
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hallo 10.2.e en 10. ,10.2.

In overleg met het OM hebben we definitieve teksten gemaakt voor de QenA's. Zie bijlagen.

We hebben enkele aanvullingen van 10.2.e verwijderd omdat we denken dat we die beter achter de hand kunnen houden voor als er vervolgvragen komen. Een heel uitgebreid antwoord roept juist vragen op.

Gisteren heeft 10.2.e . mij ook al het antwoord mbt. de financiering gestuurd.
Kunnen jullie mij svp meenemen in de ontwikkelingen mbt. toets op niet melden 0days? Ik heb alleen via DGoverleg gehoord dat dit speelt, maar verder geen informatie.

Dank vast,

10.2.

Onderwerp : WV Computercriminaliteit III

Onderwerp : Kopen software, markt kwetsbaarheden

Kamerlid :

Beantwoording : DRC

Vraag: Gaat de politie software kopen van bedenkelijke bedrijven? Houden we met het kopen van dergelijke software de markt voor onbekende kwetsbaarheden in stand?

Antwoord:

- Voor de selectie van bedrijven van wie software wordt gekocht geldt de **bestaande regelgeving voor inkoop** van de politie.
- Bedrijven die software produceren waarmee kan worden binnengedrongen **vermelden niet van welke kwetsbaarheden die software gebruik maakt** of hoe het bedrijf kennis daarover heeft verkregen.
- Het **beperken van onderzoek** naar kwetsbaarheden wordt **niet wenselijk** geacht. Dergelijke kennis kan bijdragen aan de veiligheid van systemen.

- Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de **verkoop ervan aan bepaalde partijen onwenselijk**.
- De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen,

waardoor het **lastig is deze markt aan controle te onderwerpen**.

- De verkoop van *intrusion software* die gebruik maakt van kwetsbaarheden is in bepaalde omstandigheden onderhevig aan **exportcontrole.**

Onderwerp : WV Computercriminaliteit III

Onderwerp : Definitie geautomatiseerd werk

Kamerlid :

Beantwoording : DRC

Vraag: Waarom is de definitie van geautomatiseerd werk zo ruim? Gaat de politie pacemakers hacken en auto's tot stoppen dwingen?

Antwoord:

- De definitie van geautomatiseerd werk sluit aan bij de definitie van het Cybercrimeverdrag uit 2001. Deze definitie is overigens minder ruim dan in EU-regelgeving.
- Pacemakers en delen van auto's, zoals navigatiesystemen, vallen strikt genomen onder deze definitie. Dat wil uiteraard niet zeggen dat we pacemakers gaan binnendringen.
- De regering heeft er voor gekozen geen enkel soort geautomatiseerd werk categorisch uit te sluiten voor onderzoek. Dit kan namelijk leiden tot de situatie dat criminelen vooral deze geautomatiseerde werken gebruiken voor het plegen van strafbare feiten, juist omdat de overheid dan geen bewijs kan vergaren.
- Tevens is een dergelijke inperking in het licht van de snelle technologische ontwikkelingen niet toekomstbestendig.

- Uiteraard vraagt het binnendringen bij bepaalde geautomatiseerde werken een zeer hoge zorgvuldigheid. De uitvoering van de bevoegdheid wordt al beperkt door de proportionaliteit- en subsidiariteitstoets.
- In veel situaties zal moeten worden gekozen voor andere methoden, bijvoorbeeld het vorderen van gegevens, met medewerking van systeembeheerders.
- In de praktijk kan ik me op dit moment geen situatie voorstellen waarin het proportioneel is dat de politie een pacemaker zal binnendringen.
- De politie kan wel een geautomatiseerd werk in een auto binnendringen, maar heeft niet de bevoegdheid om deze tot stilstand te dwingen. Die bevoegdheid is namelijk niet genoemd in het wetsvoorstel als mogelijk doel van het binnendringen. Wel kan de politie zo'n werk binnendringen om de locatie te bepalen of gegevens over te nemen.

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Beantwoording : DWJZ

Vraag: Hoe kan een privacy inbreuk van niet-verdachte personen worden voorkomen?

Antwoord:

- Inzage in communicatie van andere, niet-verdachte personen kan bij de uitvoering van de bevoegdheid **niet worden uitgesloten**. Op het moment dat een verdachte via zijn geautomatiseerde werk communiceert over strafbare handelingen, is er immers altijd een wederpartij die deze informatie ontvangt en die niet perse al een verdachte is. Die communicatie levert wel relevant bewijsmateriaal op in de zaak van de verdachte
- Dit is thans niet anders bij de toepassing van bevoegdheden als het aftappen van communicatie of het direct afluisteren.
- Wel zijn de **wettelijke voorwaarden** voor de uitoefening van deze bevoegdheid zodanig dat zoveel mogelijk wordt voorkomen dat de opsporing in aanraking komt met gegevens van derden. De voorwaarden zijn strenger dan bijvoorbeeld de bevoegdheid tot tappen waar een niet verdacht persoon ook getapt kan worden.
- Dit betreft ten eerste het vereiste dat het geautomatiseerde werk **bij de verdachte in gebruik is**.
- In het bevel van de officier van justitie dient te worden vermeld op welke bevoegdheid het bevel betrekking heeft (bepalen locatie, ter uitvoering van tapbevel of OVC of overname gegevens). ER zal duidelijkheid zijn over de aard en functionaliteit van het technische hulpmiddel waarmee de bevoegdheid wordt uitgevoerd, alsmede het onderdeel van het geautomatiseerde systeem (zoals bijvoorbeeld het besturingssysteem, of bepaalde vormen van communicatiesoftware) waarop het bevel zich richt.

- Doordat slechts de gegevens die binnen de reikwijdte van het bevel van de officier vallen ter beschikking kunnen komen van het **tactisch team**, worden de gegevens van derden **zoveel mogelijk beschermd.**

Van: 10.2.e - BD/DWJZ/SSR
Verzonden: dinsdag 6 december 2016 12:43
Aan: 10.2.e - BD/DRC/CV; 10.2.e . - BD/DRC/CV
CC: 10.2.e - BD/DWJZ/SSR
Onderwerp: Dossier CC III

Dag 10.2. en 10.2.e , het lukt mij niet jullie te machtigen voor mijn k-schijf dus moet ik het toch maar zo doen. Hierbij aangepaste en aangevulde teksten dossier, zouden jullie willen meelezen.

Gr. 10.2.e

Van: 10.2.e
Verzonden: woensdag 7 december 2016 12:13
Aan: 10.2.e
CC: Bestuursondersteuning
Onderwerp: amendementen CIII
Bijlagen: 34372-9.pdf; 34372-8.pdf

En bij deze de (tot nu toe) ingediende amendementen voor CCIII

Gr.,

10.2.

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 8 **AMENDEMENT VAN DE LEDEN VERHOEVEN EN VAN TONGEREN**

Ontvangen 1 december 2016

De ondergetekenden stellen het volgende amendement voor:

In artikel II, onderdeel G, wordt in artikel 126nba in het eerste lid, aanhef, «binnendringt in een geautomatiseerde werk dat bij de verdachte in gebruik is» vervangen door: zonder gebruik te maken van kwetsbaarheden in software een geautomatiseerd werk dat bij de verdachte in gebruik is binnendringt.

Toelichting

Dit amendement beperkt de bevoegdheid voor de politie om geautomatiseerde werken binnen te dringen, er mag namelijk geen gebruik worden gemaakt van kwetsbaarheden in software. Het binnendringen van geautomatiseerde werken zonder gebruik van kwetsbaarheden in software kan bijvoorbeeld door middel van (spear)phishing technieken, oftewel het sturen van een misleidende email of bericht waarmee een verdachte verleid kan worden om een wachtwoord of logingegevens prijs te geven of om een technisch hulpmiddel zoals een keylogger of andere software te installeren, mits zonder het gebruik van kwetsbaarheden, waarmee vervolgens inloggegevens buitgemaakt kunnen worden. Een andere techniek is social engineering, waarmee door middel van psychologische manipulatie het uitvoeren van handelingen of het openbaar maken van vertrouwelijke informatie, zoals een wachtwoord of inloggegevens, uitgelokt kan worden. Daarnaast zijn technieken mogelijk als brute forcing, dictionary attacks of shoulder surfing.

Cybersecurity experts benadrukken vaak het feit dat de mens de zwakste schakel in ICT-systemen is. Volgens de «Cyber Security Intelligence Index 2015» komt 95 procent van alle beveiligingsincidenten voort uit menselijke fouten. Uit meerdere onderzoeken blijkt dat ook de criminelen die zich goed beveiligen steken laten liggen. Een sprekend voorbeeld daarvan is de uitbater van de ondergrondse digitale markt Silk Road.

kst-34372-8
ISSN 0921 - 7371
's-Gravenhage 2016

Het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software is een extra bevoegdheid waarvan de noodzaak niet voldoende aangetoond is. Bovendien is het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software een onwenselijke bevoegdheid. Het maakt mensen onveilig omdat kwetsbaarheden in telefoons, tablets en andere apparaten blijven bestaan, waardoor mensen makkelijker slachtoffer kunnen worden van cybercrime. Hiermee zou de overheid een belang krijgen bij onveilige apparaten, zoals laptops, smartphones, wearables en computers en, gezien de brede definitie van «geautomatiseerde werken», ook pacemakers, auto's en medische apparatuur. Dit zorgt ervoor dat hackers die fouten in software vinden eerder geneigd zullen zijn om gevonden fouten te verkopen aan bedrijven als HackingTeam of Gamma International dan ze te melden aan de maker van de software zodat ze gedicht kunnen worden. Dit kan bijvoorbeeld gaan om een fout in het besturingssysteem van smartphones.

In een tijd waarin vrijwel elk apparaat op het internet wordt aangesloten en onze veiligheid en onze economie steeds meer afhankelijk zijn van veilige ICT-systemen is het belangrijk dat de overheid zich juist inzet voor een veiliger internet. Deze bevoegdheid zou grote schade toebrengen aan onze economie en aan ons vestigingsklimaat. Daarnaast maakt het iedereen gevoeliger voor hacks door criminelen en landen als Rusland en China. Criminelen zullen makkelijker gegevens, zoals medische data, creditcardgegevens of inloggegevens, van gewone mensen buit kunnen maken. Daarom willen de indieners dat de overheid blijft werken aan een veiliger internet, veiligere software en sterke encryptie, alleen dan kunnen mensen veiliger gemaakt worden tegen criminelen en buitenlandse mogendheden.

Verhoeven
Van Tongeren

Vergaderjaar 2016-2017

34 372 **Wijziging van het Wetboek van Strafrecht en het Wetboek van strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)**

Nr. 9 **AMENDEMENT VAN HET LID VERHOEVEN**
Ontvangen 5 december 2016

De ondergetekende stelt het volgende amendement voor:

I

In artikel II, onderdeel G, vervalt in artikel 126nba, eerste lid, onderdeel c: , dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

II

In artikel II, onderdeel L, vervalt in artikel 126uba, eerste lid, onderdeel c: , dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

III

In artikel II, onderdeel Q, vervalt in artikel 126zpa, eerste lid, onderdeel c: , dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

Toelichting

Indiener stelt voor om alle misdrijven waarvoor de bevoegdheid tot binnendringen van een geautomatiseerd werk kan worden afgegeven, te regelen in de wet en niet deels bij algemene maatregel van bestuur.

De bevoegdheid tot het binnendringen van een geautomatiseerd werk betreft een vergaande bevoegdheid. Bij de toepassing van dergelijke bevoegdheden geldt dat zij voorzienbaar en controleerbaar dienen te zijn. Zodoende past het niet om ook bij algemene maatregel van bestuur misdrijven aan te wijzen waarvoor deze bevoegdheid kan worden ingezet. Dat dient bij wet geregeld te zijn om de voorzienbaarheid en controleerbaarheid te waarborgen.

Verhoeven

Van: 10.2.e
Verzonden: woensdag 7 december 2016 14:58
Aan: 10.2.e @politie.nl>
Onderwerp: CCIII - D66 verzoekt uitstel plenaire behandeling

t.i. er ligt bij de cie VenJ een verzoek van D66 voor het uitstellen van het plenair debat CCIII. De commissie heeft tot vandaag 17.00 uur de tijd om wel of niet in te stemmen met het verzoek.
Gr.,
10.2.e

E-mailprocedure

Wijziging volgorde behandeling plenair aangemelde wetsvoorstellen

Van: Commissie V&J
Verzonden: dinsdag 6 december 2016 17:07
Aan: GC-Commissie-V&J
Onderwerp: V&J: SPOED e-mailprocedure wijziging volgorde behandeling plenair aangemelde wetsvoorstellen
Urgentie: Hoog

Geachte (plv.) leden van de vaste commissie voor Veiligheid en Justitie,
Hieronder treft u aan een verzoek van het lid Verhoeven (D66-fractie).
Ik verzoek u **uiterlijk morgen, woensdag 7 december 2016, om 17.00 uur** kenbaar te maken of u al dan niet met dit voorstel kunt instemmen.

Met vriendelijke groet,

10.2.e
9

Van: 10.2.e
Verzonden: dinsdag 6 december 2016 16:56
Aan: Commissie V&J
Onderwerp: Verzoek D66 over wvst CC3
Urgentie: Hoog

Beste griffier,

Volgende week staat de wet Computercriminaliteit III (34 372) ingepland voor plenaire behandeling. In dit wetsvoorstel komt ook het verschoningsrecht aan de orde. Voor bescherming van het verschoningsrecht bij de toepassing van de bevoegdheid tot het op afstand binnendringen in een geautomatiseerd werk wordt volgens het Kabinet aangesloten bij bestaande wetgeving. Alleen, journalisten worden daarmee niet beschermd. Daarvoor ligt nu juist een wetsvoorstel voor bronbescherming in strafzaken (34032) aan de Kamer voor.

Nu blijkt uit de Nota naar aanleiding van het verslag die we onlangs hebben ontvangen bij het wetsvoorstel Computercriminaliteit III, dat het Kabinet ervanuit gaat dat de Kamer eerst het wetsvoorstel bronbescherming in strafzaken zal behandelen alvorens de wet Computercriminaliteit III aan de orde komt. In die volgordelijkheid is verandering gebracht doordat een aantal partijen in een eerdere procedure vergadering te kennen gaven de Wet Computercriminaliteit III met hoogste prioriteit te willen behandelen. D66 stemt in met snelle behandeling, maar dat cie-besluit is genomen voordat de nota naar aanleiding van het verslag bij de Kamer binnen kwam en de Kamer er nota van kon nemen dat het Kabinet uitgaat van een andere volgorde.

Daarom het voorstel van de D66-fractie om toch eerst de wet bronbescherming in strafzaken plenair te behandelen en daarna de Wet Computercriminaliteit III.

Bij deze het verzoek dit voorstel zsm aan de leden van de commissie VenJ voor te leggen zodat een mogelijk positieve uitkomst tijdig

aan de plenaire griffie doorgegeven kan worden.
Alvast dank!

Met vriendelijke groet,

Kees Verhoeven

Van: 10.2.e BD/DRC/CV [10.2.e @minvenj.nl]
Verzonden: woensdag 7 december 2016 15:22
Aan: 1 @politie.nl>
CC: 10.2.e BD/DRC/CV 10.2.e @minvenj.nl>
Onderwerp: FW: Dossier CC III

Hoi 10.2.e bij deze het dossier op dit moment. De teksten zijn erg ingekort, het is al een enorm pakket. Moet morgen af zijn, dus svp vooral letten op feitelijke onjuistheden.

Groet,

10.2.e

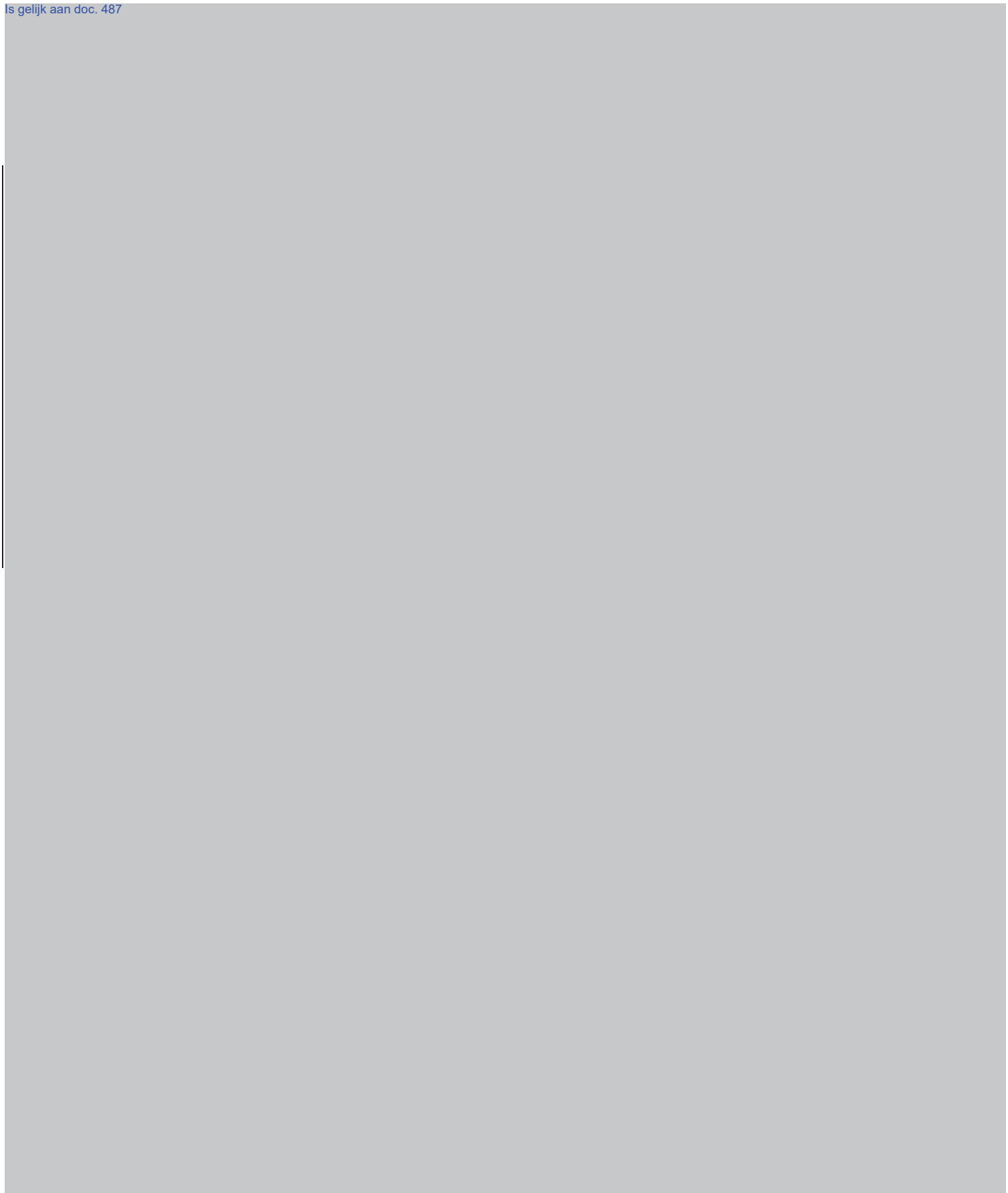
Is gelijk aan doc. 487

Is gelijk aan doc. 487

Is gelijk aan doc. 487

Is gelijk aan doc. 487

Is gelijk aan doc. 487



Inhoudsopgave dossier wetsvoorstel Computercriminaliteit III (34 372)

1. SPREEKTEKST

Voorzitter,

P.M.

- Dan kom ik nu toe aan de behandeling van de vragen.

2. SCHEMA'S

Schema1: wettelijke regeling

Schema 2: nut en noodzaak

Schema 3: amendementen

3. FACTHEETS

1. Onderzoek in geautomatiseerd werk (126nba Sv)

1.1 Wettelijke regeling en waarborgen

1.2 Gebruik van kwetsbaarheden

1.3 Binnendringen en loggen

1.4 Toezicht

1.5 Algemene maatregel van bestuur

1.6 Gebruik technisch hulpmiddel

1.7 Verschoningsrecht

1.8 De wettelijke regeling in buurlanden

1.9 Rechtsmacht

1.10 Europese jurisprudentie

1.11 Verhouding met de Wiv

2. Ontoegankelijk maken gegevens (125p Sv)

3. Overnemen en helen gegevens (138c en 139g Sr)

4. Grooming (248a en 248e Sr)

4.1 Strafbaarstelling van grooming en verleiding

4.2. Inzet (virtuele) lokmiddelen

5. Online handelsfraude (326d Sr)

6. Decryptiebevel (geschrapt)

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.1 Wettelijke regeling en waarborgen

Wettelijke regeling

- Het begrip onderzoek in een geautomatiseerd werk omvat (1) het op afstand heimelijk binnendringen in een geautomatiseerd werk en (2) het verrichten van bepaalde onderzoekshandelingen.

- Het binnendringen van een geautomatiseerd werk vindt plaats ter voorbereiding van het onderzoek al dan niet met een technisch hulpmiddel (met behulp waarvan gegevens kunnen worden vastgelegd).

- De onderzoekshandelingen betreffen:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;

b. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;

c. de ontoegankelijkmaking van gegevens;

d. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie (richtmicrofoon);

e. de uitvoering van een bevel tot stelselmatige observatie.

- Het aftappen, direct afluisteren en de observatie (punten d en e) zijn bestaande Bob-bevoegdheden, het identificatie van het werk of van de gebruiker (punt a), de vastlegging van gegevens (punt b) is nieuw en met de ontoegankelijkmaking

van gegevens (punt c) wordt aangesloten bij de bestaande regeling in Sv.

Waarborgen

- Een bevel van de officier van justitie. In het bevel moeten bepaalde gegevens worden opgenomen (misdrijf en feiten en omstandigheden die ten grondslag liggen aan verdenking, zo mogelijk nummer of andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd (bijv. IP- of MAC-adres, IMEI-nummer), dat de gegevens niet in Nederland zijn opgeslagen, aanduiding technisch hulpmiddel, aanduiding welk deel van het werk het betreft en tijdsduur inzet).

- Toestemming van het College van procureurs-generaal Het College laat zich daarbij adviseren door de Centrale Toetsingscommissie (CTC).

- Vereiste vaneen dringend onderzoeksbelang: hiermee wordt tot uitdrukking gebracht dat de gegevens niet op een minder ingrijpende wijze kunnen worden verkregen, waarbij rekening wordt gehouden met de gevolgen voor het geautomatiseerde werk en de betrokken personen.

- Een voorafgaande machtiging van de rechter-commissaris.

- Voor de bevoegdheden, genoemd in de punten a., d. en e. geldt het vereiste van een feit waarvoor voorlopige hechtenis mogelijk is.

- Voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens (punten b en c) geldt het vereiste van een feit waarvoor gevangenisstraf van acht jaar of meer kan worden opgelegd of dat bij AMvB is aangewezen.

- Bij AMvB worden aangewezen bepaalde misdrijven die worden gepleegd met behulp van een geautomatiseerd werk en.

- De drempel van acht jaar voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens is opgenomen n.a.v. advies Raad van State. In de AMvB worden de delicten opgenomen waarbij het gebruik van een computer instrumenteel is voor het plegen van et delict en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders (bijv. gebruik van botnet, aanbieden of verspreiden kinderpornografie of grooming).

- Het binnendringen is beperkt tot de daartoe aangewezen opsporingsambtenaren van het technische team. Dit betreft de door de korpschef aangewezen en ter zake deskundige opsporingsambtenaren die over specialistische kennis beschikken op het gebied van ICT.

- De opsporingsambtenaren van het technische team behoren niet tot het opsporingsteam dat het tactische onderzoek verricht (functiescheiding, vermindert risico tunnelzicht).

- De in het kader van de onderzoekshandelingen verrichte handelingen in geautomatiseerde werk worden gelogd. Daardoor kan later worden nagegaan wat er in dat kader precies is gedaan en kan de integriteit van de bewijsverkrijging worden verzekerd.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.2 Gebruik van kwetsbaarheden

Kwetsbaarheden

- Hardware en software bevat praktisch altijd kwetsbaarheden die het mogelijk maken het geautomatiseerd werk binnen te dringen.

- Criminelen en buitenlandse inlichtingendiensten maken hier gebruik van. De overheid heeft belang bij het verhelpen van kwetsbaarheden ter voorkoming van criminaliteit en andere ongewenste activiteiten.

- Fabrikanten van hardware en software kunnen kwetsbaarheden verhelpen door voor het product een patch of update beschikbaar te stellen, of een nieuwe versie te maken. Alleen als een kwetsbaarheid bij de fabrikant bekend is, is deze in staat deze te verhelpen.

- De overheid stimuleert het melden van kwetsbaarheden, onder meer door het beleid voor ‘responsible disclosure’ en de ondersteuning van het NCSC.

Gebruik kwetsbaarheden door overheidsdiensten

- De AIVD en de MIVD hebben de bevoegdheid tot binnendringen in een geautomatiseerd werk, en dit wetsvoorstel bevat deze bevoegdheid voor de politie.

- Voor de inzet van deze bevoegdheid is het gebruik van kwetsbaarheden vaak nodig. De overheid heeft daarom ook een belang bij het bestaan van kwetsbaarheden.

Afweging Kamerbrief (26 643, nr. 428)

- De kern van de Kamerbrief betreft de vraag of de overheid kwetsbaarheden meldt als zij daar kennis van heeft. Dat is alleen van belang als het om onbekende kwetsbaarheden gaat, i.e. kwetsbaarheden die nog niet bekend zijn bij de fabrikant.

- De AIVD en de MIVD zullen volgens de Kamerbrief belangendragers informeren, behoudens wettelijk bepalingen om dat na te laten. Gezien de wettelijke regelingen voor geheimhouding van bronbescherming en werkwijze zullen zij veel kwetsbaarheden niet melden.

- Voor de opsporing is er voor gekozen kwetsbaarheden in beginsel te melden gezien het belang voor het beperken van criminaliteit. In uitzonderlijke gevallen kan het OM besluiten het melden van een kwetsbaarheid uit te stellen, bijvoorbeeld in het belang van een specifiek opsporingsonderzoek of omdat het hardware of software betreft die vrijwel alleen door criminelen wordt gebruikt. Dit uitstel is in de Kamerbrief niet aan een termijn gebonden.

- De Kamerbrief spreekt overigens over kwetsbaarheden waarvan aannemelijk is dat ze onbekend zijn.

- Het is niet de bedoeling dat de politie voor elke (mogelijke) kwetsbaarheid de opdracht krijgt te onderzoeken of deze bij de fabrikant bekend is. Dat kan de opsporingscapaciteit te zeer belasten.

- Mocht kennis over een grote hoeveelheid kwetsbaarheden worden gevonden, dan kan er voor worden gekozen deze als geheel voor nadere analyse aan het NCSC of, indien bekend, aan de fabrikanten zelf ter beschikking te stellen.

- Het OM werkt aan de inrichting van een proces om het besluit tot het uitstellen van een melding zorgvuldig te nemen. Daarbij is van belang dat het besluit wordt genomen op basis van voldoende kennis en niet alleen op basis van het

individuele opsporingsonderzoek waar de kwetsbaarheid in is ontdekt.

- Het melden van een kwetsbaarheid kan namelijk gevolgen hebben voor andere onderzoeken en voor de werkwijze van de politie. Ook kan er voor worden gekozen om de melding niet direct aan de fabrikant, maar via het NCSC te doen, bijvoorbeeld indien de herkomst van de kennis van de kwetsbaarheid onbekend dient te blijven.

Internationale markt voor kwetsbaarheden

- Op het internet wordt kennis over kwetsbaarheden verhandeld. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden.

- Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Wel kunnen bepaalde softwarepakketten onderhevig zijn aan exportcontrole.

Aankoop van kwetsbaarheden door de overheid

- Het is op dit moment niet voorzien dat de politie kennis over specifieke kwetsbaarheden zal aankopen ten behoeve van de bevoegdheid tot binnendringen in geautomatiseerd werk.

- Eén reden hiervoor is dat na aankoop nog veel specialistische inzet is vereist om daadwerkelijk gebruik daarvan te kunnen maken. Wel is het voorzien dat de politie software aankoopt die gebruik maakt van kwetsbaarheden.

- Het is niet te verwachten dat de producenten van dergelijke software de broncode en de kwetsbaarheden die worden benut, bekend maken. Daarom zal het voor de politie onbekend blijven of die software gebruik maakt van onbekende kwetsbaarheden.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.3 Binnendringen en loggen

Binnendringen

In het wetsvoorstel wordt de wijze van binnendringen niet geregeld. Dit is aan de politie zelf om te bepalen.

De politie kan voor het binnendringen gebruik maken van bekende kwetsbaarheden, onbekende kwetsbaarheden of zwakheden bij de gebruikers (‘social engineering’).

De wijze van binnendringen wordt niet gelogd. De wijze van binnendringen wordt niet bij proces-verbaal vastgelegd.

De wijze van binnendringen is niet van invloed op de kwaliteit van het vervolgens verzamelde bewijsmateriaal. Als ter zitting vragen zouden rijzen over de wijze van binnendringen, dan zal de rechter de opsporingsambtenaar van het technische team als getuige kunnen horen.

Logging

De loggingplicht geldt voor de toepassing van de opsporingshandelingen, *nadat* is binnengedrongen. De logging maakt controle mogelijk op de integriteit en kwaliteit van het bewijsmateriaal.

De handelingen die worden verricht tijdens het onderzoek worden doorlopend en automatisch op de politieserver vastgelegd, zodat controle op de uitvoering van het bevel van de officier van justitie mogelijk is.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.4 Toezicht

College van procureurs-generaal (vooraf)

- De officier van justitie legt de voorgenomen beslissing tot het onderzoek in een geautomatiseerd werk voor aan het College van procureurs-generaal, dat zich daarbij laat adviseren door de CTC.

Rechter-commissaris (vooraf)

- De rechter-commissaris toetst het bevel van de officier van justitie in het individuele geval, vanwege het vereiste van een RC-machtiging. Toetsing onder meer aan de proportionaliteit en subsidiariteit.

Inspectie VenJ (achteraf)

- De Inspectie Veiligheid en Justitie is belast met het toezicht op de kwaliteit van de taakuitvoering door de politie (art. 57, eerste lid, onderdeel d, Wet veiligheidsregio's). Dit betreft de naleving van de wet- en regelgeving rond de toepassing van die bevoegdheden en de kwaliteit van de uitvoering. Waar nodig signaleert de Inspectie VenJ risico's.

- Op basis van de in de wet vastgelegde positie en taken is de Inspectie VenJ de aangewezen instantie voor de uitoefening van het toezicht op de uitvoering van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris.

- Dit toezicht omvat zowel de gevallen die, in het kader van de door het openbaar ministerie ingestelde strafvervolging jegens een verdachte, aan het oordeel van de rechter worden voorgelegd als de gevallen die niet tot strafvervolging jegens een verdachte leiden.

- De Inspectie VenJ is een rijksinspectie. Een rijksinspectie heeft de ruimte om zelf, op basis van een werkprogramma en zijn professionele deskundigheid, informatie te verzamelen, daarover een oordeel te vormen, en daarover te rapporteren en te adviseren. Er is sprake van onafhankelijke oordeelvorming.

- De inspecteurs beschikken over de nodige wettelijke toezichtbevoegdheden, op grond van de Algemene wet bestuursrecht (art. 5:12 tot en met 5:20 Awb).

- Het toezicht door de Inspectie VenJ zal betrekking hebben op de naleving van de wettelijke regels en voorschriften rond de toepassing van het onderzoek in een geautomatiseerd werk die zijn neergelegd in het Wetboek van Strafvordering en in het Besluit technische hulpmiddelen Strafvordering. Meer concreet heeft het toezicht betrekking op aspecten als de autorisaties van de bevoegde opsporingsambtenaren voor de uitvoering van het bevel van de officier van justitie voor het onderzoek in een geautomatiseerd werk, de expertise en kennis van de betrokken opsporingsambtenaren, de inzet van het technische hulpmiddel (kwaliteit en betrouwbaarheid), de vastlegging van gegevens over de werking van het technische hulpmiddel en over de toepassing van onderzoekshandelingen in het geautomatiseerde werk (logging), de beveiliging van de vastgelegde gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan.

- Het toezicht van de Inspectie VenJ is aldus gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk (systeemtoezicht). Het kader voor

het toezicht wordt gevormd door de grenzen van het bevel en de machtiging voor het onderzoek in een geautomatiseerd werk.

- De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit kader.

- De Inspectie VenJ werkt op basis van een werkprogramma dat jaarlijks door het hoofd van de Inspectie VenJ wordt vastgesteld en door de Minister van Veiligheid en Justitie aan de Staten-Generaal wordt aangeboden. Na afloop van een onderzoek wordt een rapport opgesteld. Het vastgestelde inspectierapport wordt door het hoofd van de Inspectie aan de Minister van Veiligheid en Justitie aangeboden en door die Minister openbaar gemaakt.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.5 Algemene maatregel van bestuur

Algemeen

- Het wetsvoorstel bevat een drietal (deels verplichte, deels facultatieve) delegatiegrondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de uitoefening van de binnendringbevoegdheid.

- Ter uitvoering hiervan wordt één allesomvattend besluit opgesteld, met als (werk)titel Besluit onderzoek in een geautomatiseerd werk, dat volledig wordt toegespitst op het werken in een digitale omgeving.

- De eerder aangekondigde wijziging van het reeds bestaande Besluit technische hulpmiddelen strafvordering dat primair betrekking heeft op fysieke hulpmiddelen bij de opsporing (camera's, richtmicrofoons) wordt niet meer overwogen.

Delegatiegrondslagen

<u>1. Aanwijzing misdrijven waarvoor bevoegdheid tot vastleggen/ontoegankelijkmaken gegevens mag worden ingezet (126nba, eerste lid, Sv)</u>

- In beginsel is voor het verrichten van het vastleggen en ontoegankelijkmaken van gegevens, gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer, een verdenking van een misdrijf vereist waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld.

- Deze eis is opgenomen naar aanleiding van het advies van de Afdeling advisering Raad van State.

- Artikel 126nba, eerste lid, Sv bevat een grondslag om de inzet van de bevoegdheid voor de toepassing van deze onderzoekshandelingen ook mogelijk te maken bij verdenking van een bij algemene maatregel van bestuur aangewezen misdrijf dat een ernstige inbreuk op de rechtsorde oplevert.

- Het gaat hier om misdrijven die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.

- Voorbeelden van dergelijke misdrijven zijn: het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) en 'grooming' (artikel 248e Sr).

- Er is dan vaak geen ander aangrijpingspunt voor de opsporing dan via het geautomatiseerde werk waarmee het misdrijf gepleegd wordt.

- Door de aanwijzing bij algemene maatregel van bestuur van de deze delicten kan flexibeler ingespeeld kan worden op ontwikkelingen in de computercriminaliteit dan wanneer aanwijzing bij wet zou plaatsvinden.

2. Eisen aan technische hulpmiddelen, deskundigheidseisen opsporingsambtenaren (126ee Sv, 126nba, zevende lid, Sv)

- Artikel 126ee Sv bevat een grondslag om bij algemene maatregel van bestuur regels te stellen aan de technische hulpmiddelen (software) die gebruikt worden bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk.

- Het betreft technische en procedure eisen (keuring, beheer, verstrekking, plaatsing en verwijdering van technische hulpmiddelen en vastlegging van gegevens (logging) tijdens het onderzoek.

3. Gegevens op onbekende locatie, stapsgewijze aanpak (126nba, achtste lid, Sv)

- Op grond van artikel 126nba, achtste lid, Sv kunnen bij algemene maatregel van bestuur regels worden gesteld over de toepassing van de binnendringbevoegdheid in de gevallen waarin niet bekend is op welke locatie de gegevens zijn opgeslagen.

- Een dergelijk zelfstandig optreden dient zeer zorgvuldig te worden ingekaderd, op basis van een zoveel mogelijk stapsgewijze aanpak.

- Het betreft een facultatieve delegatiegrondslag. Het heeft de voorkeur dat deze aanpak wordt uitgewerkt in een OM-aanwijzing, zo niet, dan kunnen alsnog regels in een AMvB worden gesteld.

Voorhang besluit

- Het besluit stelt technische en procedurele eisen aan het verrichten van onderzoek in een geautomatiseerd werk.

- Het besluit bevat geen voorhangbepaling. Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen (Aanwijzingen voor de regelgeving, Aanwijzing 35).

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.6. Gebruik technisch hulpmiddel

Technisch hulpmiddel

- Het onderzoek in een geautomatiseerd werk vindt in beginsel plaats met behulp van een technisch hulpmiddel, dat gegevens detecteert, registreert en opslaat.

- Een technisch hulpmiddel bestaat uit een softwareapplicatie die functionaliteiten bevat waarmee onderzoekshandelingen verricht kunnen worden.

- De inzet van een technisch hulpmiddel vindt plaats binnen de grenzen van het bevel van de officier van justitie voor in het bevel vermeld(e) onderzoeksdoel(en).

- Het wetsvoorstel vereist dat in het bevel van de officier van justitie een aanduiding van de aard en functionaliteit van het technische hulpmiddel wordt opgenomen.

Betrouwbaarheid en integriteit gegevens

- De gegevens die door een technisch hulpmiddel worden geregistreerd kunnen worden gebruikt als bewijs in een strafzaak.

- Het vergaarde bewijs moet betrouwbaar en integer zijn.

- Er gelden technische en procedurele eisen voor de inzet van technische hulpmiddelen en opleidingseisen voor de met de inzet belaste medewerkers.

Inzet van een technisch hulpmiddel

- De plaatsing, inzet en verwijdering van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar die lid is van een technisch team.

- Van de handelingen die door het technische team in het kader van het onderzoek in het geautomatiseerde werk worden verricht wordt proces-verbaal opgemaakt.

- Nadat het technische hulpmiddel is verwijderd zal de server aan de zijde van de politie geen gegevens meer kunnen ontvangen.

- In alle gevallen zal zoveel mogelijk worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten.

Geen verwijdering mogelijk

- In uitzonderingsgevallen kan worden afgezien van de (volledige) verwijdering van het technische hulpmiddel, namelijk als het verwijderen aanzienlijke risico's met zich brengt voor het systeem waarin het technische hulpmiddel is geïnstalleerd.

- Dan stelt de opsporingsambtenaar de officier van justitie van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering.

- De officier van justitie stelt de beheerder van het geautomatiseerde werk daarvan in kennis.

Controle op de inzet

- Alle in het kader van het onderzoek verrichte handelingen worden automatisch worden vastgelegd (gelogd) op de politieserver.

- Daardoor kan later worden nagegaan wat er in dat kader precies is gedaan en kan de integriteit van de bewijsverkrijging worden verzekerd.

- De Inspectie VenJ kan in het kader van haar toezichtstaak onderzoek naar de uitvoering van het onderzoek in een geautomatiseerd werk.

Bewijs

- In het pv van de inzet wordt verwezen naar het keuringsnummer van het technische hulpmiddel, waardoor de samenstelling hiervan, ter bescherming van de tactische belangen, kan worden afgeschermd.

- Bij twijfel kan de zittingsrechter de volledige gegevens opvragen of kan een rechter-commissaris getuigen achter gesloten deuren horen (procedure 187d Sv).

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.7 Verschoningsrecht

Wettelijke regeling

- Voor de bescherming van het verschoningsrecht bij de toepassing van de bevoegdheid tot het op afstand binnendringen in een geautomatiseerd werk aangesloten bij de bestaande regeling van artikel 126aa, tweede lid, Sv. Het EHRM heeft het Nederlandse systeem van artikel 126aa Sv voldoende precies en begrijpelijk geacht en geoordeeld dat dit systeem voldoende waarborgen biedt om te kunnen worden aangemerkt als «recht» in de zin van artikel 8, tweede lid, EVRM (EHRM 25 november 2004, appl. no. 16269/92 Aalmoes vs. Nederland).

- Deze regeling heeft betrekking op gegevens die ter kennis van de opsporingsambtenaren komen in het kader van de uitoefening van bijzondere opsporingsbevoegdheden jegens anderen dan de verschoningsgerechtigden (de zogenaamde «bijvangst»), en is ook van toepassing op het onderzoek in een geautomatiseerd werk.

- Als een proces-verbaal of een ander voorwerp, zoals de opname van een afgeluisterd telefoongesprek, mededelingen bevat door of aan een verschoningsgerechtigde dan worden het betreffende proces-verbaal of voorwerp voorgelegd aan de officier van justitie. Als de officier van justitie vaststelt dat de mededelingen onder de bescherming van het verschoningsrecht vallen, dan beveelt hij terstond de vernietiging van de processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen.

- De procedure is uitgewerkt in de OM-Instructie Vernietiging geïntercepteerde gesprekken met geheimhouders.

- Het verschoningsrecht kan in zeer uitzonderlijke omstandigheden worden doorbroken, waardoor de verzamelde gegevens alsnog gebruikt kunnen worden. Van zeer uitzonderlijke omstandigheden kan onder meer sprake zijn als de verschoningsgerechtigde zelf verdacht wordt van ernstige strafbare feiten. In de gevallen waarin de geheimhouder verdachte is, wordt het oordeel van een gezaghebbend lid van de betreffende beroepsgroep ingewonnen over de vraag welke gegevens dergelijke mededelingen behelzen. De officier van justitie kan de gegevens dan voorleggen aan de rechter-commissaris. Wanneer die oordeelt dat een doorbrekingsgrond van toepassing is dan kunnen de gegevens in het opsporingsonderzoek worden gebruikt.

Reikwijdte

- Op grond van de wetsgeschiedenis en de jurisprudentie van de Hoge Raad komt het verschoningsrecht toe aan de arts, de geestelijke, de notaris en de raadsman. Ook andere geneeskundige beroepsbeoefenaren dan de arts kunnen verschoningsgerechtigd zijn, zoals de apotheker of de verpleegkundige.

- Journalisten hebben op dit moment geen wettelijk verschoningsrecht vanwege hun stand, beroep of ambt, als bedoeld in artikel 218 Sv. In het arrest Goodwin heeft het EHRM geoordeeld dat aan journalisten geen volledig verschoningsrecht toekomt, maar dat zij vanwege het belang van de vrijheid van meningsuiting en de persvrijheid in een democratische samenleving onder omstandigheden wel aanspraak kunnen maken een recht op bronbescherming. Dit recht is niet absoluut maar kan door een zwaarderwegend belang opzij worden gezet.

- Inmiddels is het wetsvoorstel bronbescherming in strafzaken bij de Tweede Kamer ingediend (Kamerstukken II 2014/15, 34 032, nr.1) dat voorziet in wettelijke verankering van een recht op bronbescherming voor journalisten.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.8 De wettelijke regelingen in buurlanden

Nederland in internationale context

- De dilemma's die het karakter van cyberspace meebrengt voor de taak van de overheid om de rechtsstaat te handhaven spelen niet alleen in Nederland maar evenzeer in andere landen.

- De benadering die in andere Europese landen gekozen wordt is verschillend.

- Grofweg kunnen twee verschillende benaderingen worden onderscheiden. Ten eerste landen die actief inspelen op de huidige ontwikkelingen en met nieuwe wetgevende voorstellen komen om de praktijk duidelijke kaders te bieden. Ten tweede landen die vooralsnog geen additionele handvaten voor de opsporing in het digitale domein bieden of waar de praktijk opereert op basis van een ruime interpretatie van traditionele bevoegdheden.

- De Nederlandse regering geeft de voorkeur aan heldere kaders voor de opsporing en transparantie over hoe met de huidige technologische ontwikkelingen wordt omgegaan.

Landen met vergelijkbare bevoegdheden

- Frankrijk. In juni van dit jaar is een wettelijke regeling aangenomen die toestaat dat, wanneer de behoefte aan informatie met betrekking tot een ernstig misdrijf dit vereist, heimelijk een technisch hulpmiddel wordt geïnstalleerd met het doel toegang te verkrijgen tot elektronische gegevens, deze op

te slaan, te bewaren en over te dragen. Waarborgen zijn onder andere:

o gemotiveerde beslissing van de rechter-commissaris

o een nauwkeurige omschrijving van het strafbare feit, de exacte locatie of gedetailleerde omschrijving van de geautomatiseerde systemen voor het verwerken van gegevens, en de duur van de maatregel.

o Het op elektronische wijze aanbrengen en verwijderen van het technische middel gebeurt op gezag en onder toezicht van de rechter-commissaris.

- Verenigd Koninkrijk

Op 2 november 2016 is de Investigatory Powers Bill aangenomen. De wet is een revisie van de bevoegdheden van de inlichtingendiensten en de opsporingsdiensten. Deze wet bevat de bevoegdheid tot binnendringen in geautomatiseerd werk voor de opsporingsdiensten, in het VK equipment interference genoemd. De mogelijkheden zijn vergelijkbaar met het Nederlandse wetsvoorstel.

- Noorwegen

In juni van dit jaar is een wettelijke regeling aangenomen die het toestaat om met behulp van een technisch hulpmiddel niet-publiekelijke informatie uit een geautomatiseerd werk te lezen wanneer iemand wordt verdacht van een feit dat wordt bestraft met een gevangenisstraf van 10 jaar of meer, of voor een aantal aangewezen strafbare feiten, waaronder witwassen, terrorisme en mensenhandel.

Landen met minder (of minder geëxpliciteerde) bevoegdheden

- Duitsland

Duitsland kent een traditioneel bevel tot doorzoeking en inbeslagname van gegevensdragers. Daarnaast is er een mogelijkheid tot een “verlengd” onderzoek aan de gegevensdrager (StPO sectie 110(3)). Als er een risico is dat bewijs verloren gaat kunnen de Duitse opsporingsdiensten ook een gegevensdrager die fysiek niet verbonden is met de originele gegevensdrager, maar wel via deze gegevensdrager toegankelijk is, doorzoeken. Data die mogelijk belangrijk is voor het onderzoek mag dan worden veiliggesteld. Officieel mag geen onderzoek worden gedaan buiten Duits grondgebied. Voor de uitvoering van deze bevoegdheid wordt daarom steeds aangenomen dat de data waartoe toegang wordt verschaft zich (tevens) ook in Duitsland bevindt. De bewijslast voor het bewijzen dat dit niet het geval is ligt bij de verdachte.

- België

De Belgische wet kent geen bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Bepaalde bevoegdheden die in de Nederlandse wet onder deze bevoegdheid worden geplaatst, kunnen onder de Belgische wet worden geïnterpreteerd als netwerkzoeking. Opsporingsdiensten kunnen een primaire netwerkzoeking verder zetten op eigen informaticasystemen. Zo is het voor hen bijvoorbeeld mogelijk om onder bepaalde voorwaarden gebruik te maken van de gebruikersnaam en het wachtwoord van een Hotmailaccount. Of, wanneer een opsporingsambtenaar via technieken als social engineering een wachtwoord weet te bemachtigen, hiermee onder een valse hoedanigheid of met behulp van een valse sleutel toegang te verkrijgen tot een geautomatiseerd werk.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.9 Rechtsmacht

Internationale samenwerking

- De Nederlandse regering acht het van groot belang dat de landen internationaal met elkaar samenwerken om te komen tot een gemeenschappelijk optreden bij de aanpak van grensoverschrijdende computercriminaliteit. Als Voorzitter van de Raad van de Europese Unie heeft Nederland dit onderwerp geagendeerd. Daarnaast neemt Nederland actief deel aan het overleg in het kader van de Cybercrime Conventie van de Raad van Europa.

- De ontwikkeling van een dergelijk gemeenschappelijk internationaal optreden is echter pas op langere termijn te realiseren. In afwachting daarvan zal, als een verzoek om rechtshulp geen uitkomst biedt, moeten worden gekozen tussen twee minder ideale situaties, namelijk het afzien van het verrichten van opsporingshandelingen wanneer niet bekend is waar deze gegevens zich bevinden of in uitzonderlijke gevallen het onder voorwaarden zelfstandig uitoefenen van uitvoerende rechtsmacht.

Zelfstandig optreden onder voorwaarden

- Vanwege de dringende belangen die hierbij in het geding zijn kiest de regering voor de laatste optie, waarbij zo zorgvuldig mogelijk wordt gehandeld. Als bekend is dat de gegevens zich op het grondgebied van een andere staat bevinden, zal zo snel mogelijk een verzoek tot rechtshulp worden gedaan. Daarbij verantwoording kunnen worden

afgelegd over de reeds verrichte handelingen en de daarbij gemaakte afwegingen.

- Dit is een standaard procedure en er is geen reden om, als bekend is dat een geautomatiseerd werk of de gegevens zich op het grondgebied van een andere staat bevinden, een rechtshulpverzoek uit te stellen.

- Niet uitgesloten is dat, in afwachting van een reactie van de betreffende staat, bepaalde onderzoekshandelingen worden verricht. Dit is sterk afhankelijk van de aard en ernst van de strafbare feiten, de te verrichten onderzoekshandelingen en de aard van de rechtshulprelatie met het betreffende land. Als het gaat om een staat waarmee Nederland een intensieve relatie onderhoudt dan is de afweging anders dan wanneer het een staat betreft die bekend staat als een notoire «safe haven» voor criminaliteit.

- Een voorbeeld is een DDOS-aanval op kritische Nederlandse infrastructuur, waardoor de online afhandeling van het betalingsverkeer door banken onmogelijk is of de werking van militaire installaties wordt belemmerd. In een dergelijk geval kan het dringend noodzakelijk zijn om op te treden en een server binnen te dringen en bepaalde gegevens ontoegankelijk te maken zodat de DDOS-aanval kan worden beëindigd. Een ander voorbeeld is een situatie waarin sprake is van een terroristische dreiging, waarbij in een geautomatiseerd werk wordt binnengedrongen om telecommunicatie af te tappen of gegevens over te nemen om de daders zo snel mogelijk te kunnen achterhalen en een aanslag te voorkomen.

- Dit optreden kan niet bij voorbaat worden uitgesloten wanneer de aangezochte staat niet of niet tijdig op het rechtshulpverzoek reageert. In een dergelijk geval gaat de noodzaak van onverwijld ingrijpen voor op het afwachten van de reactie van de aangezochte staat. Dit neemt uiteraard niet weg dat, als de betrokken staat daarom vraagt, altijd

verantwoording zal worden afgelegd over het handelen de daarbij gemaakte afwegingen.

- De regering gaat ervan uit dat deze handelwijze niet op internationaalrechtelijke bezwaren stuit, juist omdat rechtshulp zal worden gevraagd zodra de locatie van het geautomatiseerde werk bekend is. Hiermee wordt tegemoet gekomen aan het soevereiniteitsbeginsel, dat met zich meebrengt dat een staat exclusief bevoegd is tot het handelen op het eigen grondgebied en jegens eigen onderdanen.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.10 Europese jurisprudentie

Algemeen

- Het recht op respect voor het privéleven, het familie- en gezinsleven, de woning en de correspondentie is vastgelegd in het Europees Verdrag ter bescherming van de Rechten van de Mens en de fundamentele vrijheden (art. 8, eerste lid, EVRM). Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht dan voor zover bij de wet voorzien en in een democratische samenleving noodzakelijk is in het belang van bepaald aangewezen maatschappelijke belangen, waaronder het voorkomen van wanordelijkheden en strafbare feiten (art. 8, tweede lid, EVRM).

- Het Handvest van de grondrechten van de Europese Unie voorziet eveneens in het recht van eenieder op bescherming van zowel het privéleven en van het familie- en gezinsleven (art. 7 Handvest) als de bescherming van persoonsgegevens (art. 8 Handvest).

- Het recht op de bescherming van de persoonlijke levenssfeer is geen absoluut recht maar dient te worden afgewogen tegen andere maatschappelijk zwaarwegende belangen, zoals bijvoorbeeld het belang van de voorkoming en opsporing van strafbare feiten.

- Het Europese Hof van Justitie heeft onlangs enkele arresten gewezen over de bescherming van persoonsgegevens die aanleiding hebben gegeven tot publiciteit.

De zaken van Digital Rights Ireland en Seitlinger

- In deze zaken heeft het Hof uitspraak gedaan over het bewaren van telecommunicatiegegevens van burgers ten behoeve van de opsporing en vervolging van ernstige misdrijven (zaken C-293/12 en C-294/12). Kernpunt van dit arrest betreft de vraag in hoeverre de overheid gegevens van burgers kan verzamelen en opslaan, zonder dat er op het moment van het verzamelen aanwijzingen bestaan dat er een verband bestaat tussen het gedrag van de personen van wie gegevens worden opgeslagen en hun betrokkenheid bij zware criminaliteit. In het onderhavige wetsvoorstel is echter geen sprake van het verzamelen en opslaan van gegevens van personen zonder dat er op het moment van het verzamelen sprake is van aanwijzingen van betrokkenheid van die personen bij strafbare feiten. De voorgestelde bevoegdheid van het binnendringen in een geautomatiseerd werk kan uitsluitend worden toegepast in geval van verdenking van betrokkenheid van een persoon bij ernstig misdrijf.

- Het arrest Seitlinger heeft dus betrekking op een andere situatie dan het onderhavige wetsvoorstel.

De zaak Maximilian Schrems/Data Protection Commissioner

- In deze zaak over de verstrekking van persoonsgegevens aan derde landen (C-362/15). In deze zaak heeft het Europese Hof van Justitie de doorgifte van persoonsgegevens door een dochterbedrijf van Facebook in Ierland aan het moederbedrijf in de Verenigde Staten getoetst aan de eisen die op grond van de privacyrichtlijn (richtlijn 95/46/EU) aan een dergelijke doorgifte moeten worden gesteld. De privacyrichtlijn biedt de mogelijkheid van doorgifte van persoonsgegevens aan een derde land als in dat land een passend beschermingsniveau wordt gewaarborgd. De Europese Commissie had in de zogenaamde Safe Harbour beschikking vastgesteld dat dit voor

de Verenigde Staten het geval is. Het Hof van Justitie oordeelde deze beschikking ongeldig. Dit oordeel hield nauw verband met de toegang tot de gegevens voor de Amerikaanse veiligheidsdiensten. Het onderhavige wetsvoorstel heeft echter geen betrekking op de verstrekking van persoonsgegevens van burgers door particuliere bedrijven aan de veiligheidsdiensten in derde landen.

- Ook het arrest Schrems heeft dus betrekking op een andere situatie dat het onderhavige wetsvoorstel.

De zaak Zakharov tegen Rusland

- In dit arrest heeft het EHRM de Russische wetgeving op het gebied van het afluisteren van telecommunicatie door de Russische veiligheidsdiensten getoetst aan het EVRM, in het bijzonder artikel 8 van het EVRM. Dit betrof afluistervoorzieningen die de Russische geheime dienst (FSB) in de gelegenheid stelde om zonder voorafgaande rechterlijke toetsing telecommunicatie af te tappen.

- Het Hof oordeelde dat het Russische wettelijke systeem geen adequate en effectieve garanties en waarborgen tegen misbruik bood, dit betrof in het bijzonder de omstandigheden waarin de autoriteiten bevoegd waren tot het heimelijk aftappen van telecommunicatie, de duur van het heimelijk aftappen, de procedures voor het vernietigen en opslaan van onderschepte data, de procedures voor het autoriseren van de autoriteiten om aftapmaatregelen te nemen, het toezicht op de interceptie en de notificatie van de interceptie en de effectiviteit van de beschikbare rechtsmiddelen.

- In het licht van deze tekortkomingen stelde het Hof vast dat de Russische wetgeving niet voldoet aan het vereiste van de «kwaliteit van de wet» en de «inbreuk» niet beperkt tot

hetgeen «in een democratische samenleving noodzakelijk is» en concludeerde dat artikel 8 EVRM is geschonden.

De zaak Szabó en Vissy tegen Hongarije

- Deze zaak betrof een klacht over schending van art. 8 EVRM vanwege de Hongaarse wetgeving, die voorzag in de bevoegdheid van een speciale antiterreureenheid van de politie om geheime onderzoeksmethoden toe te passen in het kader van het onderzoek naar verdachten van bepaalde misdaden.

- Het Hof herhaalde een aantal observaties van de zaak Zakharov, zoals dat de technische ontwikkeling de mogelijkheid biedt van grootschalig aftappen van communicatie van burgers. In het licht van de bescherming van het privéleven is het belangrijk dat de wet voorziet in goede waarborgen van voorzienbaarheid en procedure zodat de inbreuken alleen plaatsvinden wanneer dit in een democratische samenleving noodzakelijk is.

- Het Hof maakte zich er ernstig zorgen over dat in de Hongaarse regeling geen enkele verdenking nodig is en een volledige discretie voor de autoriteiten bestaat om te besluiten tot het toepassen van geheime onderzoeksmethoden. Het Hof achtte het buitengewoon problematisch dat er geen enkele onafhankelijke (rechterlijke) controle bestond en benadrukte het belang van toezicht achteraf, zowel in individuele gevallen als in zijn algemeenheid.

- Het Hof stelde unaniem een schending van art. 8 EVRM vast (punt 89).

- Het onderhavige wetsvoorstel computercriminaliteit wijkt op vrijwel al deze punten af van de wettelijke regelingen van de Russische Federatie en Hongarije. Het onderhavige wetsvoorstel is van toepassing op de opsporing en vervolging van strafbare feiten, en niet op de bescherming van de

staatsveiligheid. De gevallen waarin de bevoegdheid kan worden toegepast worden duidelijk in de wet vastgelegd.

- De bevoegde autoriteiten kunnen niet volledig naar eigen inzicht besluiten tot de toepassing van deze bevoegdheid. Er is altijd een voorafgaande rechterlijke machtiging vereist

- Verder wordt de betrokkene geïnformeerd over de toepassing van de bevoegdheid (notificatieplicht) en wordt systeemtoezicht uitgeoefend op de uitvoering van de wettelijke regels in praktijk.

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.11 Verhouding met de Wiv

Huidige bevoegdheden politie en justitie

- Aftappen: niet voor het publiek bestemde communicatie worden afgetapt en opgenomen die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst (art. 126m Sv). De voorwaarden voor toepassing zijn een misdrijf waarvoor voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op de rechtsorde oplevert, een dringend onderzoeksbelang en een voorafgaande machtiging van de rechter-commissaris.

- Direct afluisteren: vertrouwelijke communicatie (een gesprek tussen twee personen) kan worden opgenomen met een technisch hulpmiddel (art. 126l Sv). dit kan een kleine microfoon zijn die aan het zicht van buitenstaanders is onttrokken (een «bug») of een microfoon die een zeer groot bereik heeft (richtmicrofoon). De voorwaarden voor toepassing zijn gelijk aan het aftappen.

Toekomstige bevoegdheden politie en justitie

- Voorgesteld wordt de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk, met het oog op het verrichten van bepaalde onderzoekshandelingen.

- Deze bevoegdheid kan worden gebruikt voor het aftappen of het direct afluisteren.

- Voorwaarde is een feit waarvoor voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op de rechtsorde oplevert. Voor de onderzoekshandelingen moet het gaan om

een feit waarvoor voorlopige hechtenis mogelijk is, waarvoor vrijheidsstraf van tenminste acht jaar mogelijk is of dat bij AMvB is aangewezen. Voorts zijn vereist een dringend onderzoeksbelang en een voorafgaande machtiging van de rechter-commissaris.

Huidige bevoegdheden IenV-diensten o.g.v. Wiv 2002

- Aftappen: het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt (art. 25 Wiv 2002). Voor de uitoefening van deze bevoegdheid is de toestemming van de Minister vereist.

- Het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabel gebonden telecommunicatie voor een periode van drie maanden (art. 27 Wiv 2002). Dit betreft satellietcommunicatie. Voor de interceptie als zodanig is thans geen toestemming van de Minister vereist. Aan de hand van bepaalde criteria kan vervolgens nadere selectie van de verzamelde gegevens plaatsvinden, waarvoor wel ministeriële toestemming is vereist, omdat de selectie is gericht op het kennisnemen van de inhoud van de communicatie.

- Het binnendringen in een geautomatiseerd werk (artikel 24 Wiv 2002). Deze bevoegdheid kan uitsluitend worden ingezet voor de uitoefening van de wettelijke taken van de diensten in het belang van de nationale veiligheid. Voor de uitoefening van deze bevoegdheid is de toestemming van de Minister vereist.

Toekomstige bevoegdheden IenV-diensten

- In het conceptvoorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten wordt voorgesteld de bestaande bevoegdheid ex artikel 27 Wiv 2002 te vervangen door een nieuwe bevoegdheid, te weten het onderzoeksopdrachtgerichte onderzoek van communicatie. Deze bevoegdheid ziet zowel op de interceptie (in bulk) van niet-kabel gebonden als kabel gebonden telecommunicatie. Een vergelijkbare bevoegdheid ontbreekt in de sfeer van de strafvordering.

Concluderend

- De bevoegdheden van de politie tot het aftappen van telecommunicatie en het direct afluisteren van vertrouwelijke communicatie zijn beperkt tot de gerichte interceptie, dat wil zeggen dat de interceptie is beperkt tot de communicatie van een specifieke persoon of van een bepaald nummer. De politie is thans niet bevoegd tot de ongerichte interceptie van communicatie, ongeacht of die communicatie al dan niet via de kabel verloopt.

- De politie is thans niet bevoegd tot het binnendringen in een geautomatiseerd werk.

- In de regeling van het Wetboek van Strafvordering vormt het vereiste van een voorafgaande rechterlijke machtiging een belangrijke voorwaarde, in de regeling van de Wiv 2002 alsmede in het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten betreft dit de voorafgaande instemming van de verantwoordelijke Minister.

Factsheet 2 Ontoegankelijk maken gegevens (125p Sv)

Gegevens op internet ontoegankelijk maken

- Gegevens op internet kunnen ontoegankelijk gemaakt worden, dan wel door een tussenpersoon zelf dan wel op bevel van de OvJ, als er sprake is van strafbare inhoud.

- Het verwijderen van strafbare informatie op het internet door een tussenpersoon kan op grond van de Notice & Take Downprocedure (NTD) plaatsvinden als er sprake is van onmiskenbare onrechtmatige of strafbare content. Een ieder kan melding doen van onrechtmatige of strafbare inhoud op internet bij een tussenpersoon. Als er naar het oordeel van de tussenpersoon sprake is van onmiskenbaar onrechtmatige of strafbare inhoud dan wordt die inhoud verwijderd.

Bevoegdheid OvJ

- Als de gegevens niet worden verwijderd en er sprake is van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan dan kan de OvJ na gebruik maken van zijn strafvorderlijke bevoegdheid om gegevens ontoegankelijk te laten maken.

- De bevoegdheid van de OvJ wordt in het onderhavige wetsvoorstel overgeheveld van artikel 54a van het Wetboek van Strafrecht naar artikel 125p Sv en tegelijkertijd verduidelijkt en versterkt.

- Artikel 125p Sv introduceert een afzonderlijke en zelfstandige bevoegdheid voor de OvJ om bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan tussenpersonen te bevelen terstond alle maatregelen nemen die redelijkerwijs gevergd kunnen worden om gegevens on toegankelijk te maken.

Noodzaak bevoegdheid

- De bevoegdheid is van belang in gevallen waarin de tussenpersoon niet bereid is op basis van de gedragscode de gegevens ontoegankelijk te maken, bijvoorbeeld als de OvJ en tussenpersoon van mening verschillen of de vrijheid van meningsuiting in het geding is.

- Daarnaast kan het bevel ook worden gericht aan tussenpersonen die de NTD-code niet hebben ondertekend, waarbij te denken valt aan hosting providers en beheerders van een website.

- Zo nodig kan de OvJ vervolgen wegens het niet voldoen aan een bevoegd gegeven ambtelijk bevel (184 Sr) dan wel voor het plegen of medeplegen van het strafbare feit.

Actieplan jihadisme

- De maatregel kan worden ingezet bij de bestrijding van radicaliserende, haatzaaiende jihadistische content op internet en sociale media en maakt onderdeel uit van het Actieplan jihadisme.

Inzet bevoegdheid

- Een bevel tot ontoegankelijkmaking kan uitsluitend worden gegeven voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

- Bij de inzet van de bevoegdheid dienen de eisen van proportionaliteit en subsidiariteit in acht te worden genomen.

Rechterlijke toetsing

- De OvJ heeft een machtiging nodig van de rechter-commissaris.

- Voorafgaande rechterlijke toetsing wordt vereist gelet op de vrijheid van meningsuiting die bij een bevel tot ontoegankelijkmaking in het geding kan zijn.

- Een eerder wetsvoorstel waarin een geheel zelfstandige bevelsbevoegdheid voor de OvJ (zonder machtiging rc) in combinatie met een dwangsom was opgenomen kreeg veel kritiek in de consultatiefase: de vrees bestond onder meer dat het OM zou (moeten) gaan optreden als censuurpolitie.

- Het verdenkingscriterium is aangescherpt om te voorkomen dat de bevoegdheid wordt ingezet in bagatelzaken.

- De ontoegankelijkmaking betreft een voorlopige maatregel, de definitieve beslissing over de vernietiging van gegevens is voorbehouden aan de rechter die oordeelt over de strafzaak.

Uitsluiting vervolging tussenpersonen

- De vervolgingsuitsluitingsgrond voor de tussenpersoon in artikel 54a bij voldoen aan het bevel van de OvJ blijft in tact.

Factsheet 3 Overnemen en helen gegevens (138c en 139c Sr)

Noodzaak strafbaarstelling

- Het wetsvoorstel stelt het overnemen en helen van vertrouwelijke gegevens strafbaar.

- Dit is nodig omdat met het wederrechtelijk verkrijgen en via internet breed verspreiden van vertrouwelijke gegevens ernstig inbreuk kan worden gemaakt op de belangen van slachtoffers.

- Op grond van de jurisprudentie kunnen gegevens worden aangemerkt als een goed in de zin van artikel 310 Sr. Voor diefstal is echter vereist dat de gegevens buiten de beschikkingsmacht van de betrokkene worden gebracht, dit is bij overnemen (kopiëren) niet het geval.

- Niet nodig is dat computervredebreuk (art. 138ab Sr) is gepleegd, dus dat wederrechtelijke in een computer is binnengedrongen.

- Voorbeelden van strafwaardige gedragingen zijn: het kopiëren van gegevens door een werknemer waartoe hij in zijn functie toegang tot heeft, misbruik van creditcardgegevens en vormen van “wraakporno” waarbij seksueel beeldmateriaal op internet wordt gepubliceerd.

- De strafbepalingen hebben een brede reikwijdte: alle gegevens vallen eronder. Omdat in zijn algemeenheid grote risico’s voor slachtoffers verbonden zijn aan het overnemen en helen van gegevens, wordt geen onderscheid gemaakt in soort/aard van de gegevens.

- De strafbedreiging is gevangenisstraf van ten hoogste een jaar/geldboete van de vierde categorie (€20.500).

Overnemen van gegevens (138c Sr)

- De strafbepaling is van belang voor gevallen waarin iemand rechtmatige toegang heeft tot niet openbare gegevens op een computer.

- Voor strafbaarheid is niet nodig dat de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht.

- Het overnemen van gegevens is alleen strafbaar voor zover dit wederrechtelijk plaatsvindt. Van wederrechtelijkheid is geen sprake als het algemeen belang het handelen vereiste.

- Het recht op een vrije nieuwsgaring kan worden aangemerkt als een algemeen belang. Gerechtvaardigde activiteiten van journalisten/klokkenluiders zijn niet strafbaar. Het oordeel hierover in een concreet geval is aan de rechter.

- Gegevens zijn niet openbaar als ze op zodanige wijze zijn opgeslagen dat daaruit kan blijken dat de rechthebbende niet de intentie had de gegevens voor het publiek beschikbaar te stellen.

Helen van gegevens (139g Sr)

- De strafbepaling is vooral van belang voor gevallen waarin iemand gegevens voorhanden heeft die zijn verkregen uit een misdrijf dat door een ander is begaan of waarin niet kan worden bewezen dat degene die de gegevens voorhanden heeft deze zelf door misdrijf heeft verkregen.

- Een voorbeeld is het bij een persoon aantreffen van een grote hoeveelheid gegevens van creditcardhouders. Een ander voorbeeld betreft een persoon die met instemming van de

bezitter toegang heeft tot een computer, maar stiekem gegevens kopieert en op internet zet.

Aanpak van "wraakporno"

- De strafbaarstellingen van het overnemen en helen van gegevens draagt bij aan de aanpak van "wraakporno", de Tweede Kamer vraagt regelmatig aandacht voor bestrijding van dit fenomeen.

- Het gaat hier om gedrag waarbij seksueel beeldmateriaal wordt vergaard waarmee de afgebeelde vervolgens wordt afgeperst of zwartgemaakt, waarbij het motief is het uiten van frustratie, bijvoorbeeld na een verbroken relatie.

- Hoewel er op dit moment al voldoende (al dan niet strafrechtelijke) mogelijkheden zijn (onder andere op grond van de zedenwetgeving, smaad/belediging, Auteurswet) om op te treden tegen het ongewenst verspreiden van seksueel beeldmateriaal, kan het wetsvoorstel de aanpak hiervan nog wel verbeteren.

- Degene die rechtmatige toegang heeft tot vertrouwelijke gegevens, zoals seksueel beeldmateriaal op een computer en deze gegevens voor zichzelf of een ander kopieert, is nu niet strafbaar. Een rechthebbende heeft dan echter geen invloed op het gebruik dat van het seksueel beeldmateriaal wordt gemaakt, waardoor hij benadeeld kan worden.

- Strafrechtelijke vervolging wegens heling van seksueel beeldmateriaal dat door een misdrijf is verkregen is evenmin mogelijk.

- Na inwerkingtreding van het wetsvoorstel zijn dit wel strafbare gedragingen.

- Een specifieke strafbaarstelling van "wraakporno" is niet nodig en wordt niet voorzien.

- In de “zedenbrief” (29 februari 2016) aan de Tweede Kamer is aangekondigd dat in het kader van de modernisering van de zedentitel de mogelijkheid wordt onderzocht of seksuele afpersing met een seksueel motief strafbaar gesteld kan worden als zedendelict.

- Wanneer het motief van de afpersing echter gelegen is in het uiten van frustratie dan wel het schaden in de eer en goede naam, zoals bij wraakporno, biedt de bestaande wetgeving voldoende (strafrechtelijke) bescherming.

4. Grooming (248a en 248e Sr)

Factsheet 4.1 Strafbaarstelling grooming en verleiding

Grooming

- Grooming is het online vatbaar maken van een 16minner, voor een ontmoeting in de fysieke wereld met seksueel misbruik als doel. Grooming is strafbaar gesteld in artikel 248e van het Wetboek van Strafrecht.

Lokpuber

- De 'lokpuber' is een (meerderjarige) opsporingsambtenaar die zich op het internet uitgeeft als een minderjarige en op die manier, daarbij niet op eigen initiatief, in chatcontact kan komen met potentiele verdachten van grooming.

- In de jurisprudentie is bepaald dat het voor strafbaarheid in het kader van grooming noodzakelijk is dat de verdachte contact heeft gehad met een persoon die daadwerkelijk de leeftijd van 16 jaar nog niet heeft bereikt, hetgeen bij de inzet van de 'lokpuber', een volwassen opsporingsambtenaar, niet het geval is.

- Het wetsvoorstel wijzigt de delictsomschrijving in de artikelen 248a Sr (verleiding van een minderjarige) en 248e Sr (grooming) op zodanige wijze dat de inzet van de 'lokpuber' voor de opsporing van deze delicten mogelijk wordt.

- Het groomingsartikel beslaat niet het bewegen van een kind om naakt voor de webcam te gaan zitten of daar

ontuchtige handelingen voor te verrichten. Vandaar dat ook het verleidingsartikel wordt gewijzigd.

- Door de wetswijzigingen worden de opsporingsmogelijkheden bij grooming en verleiding van een minderjarige verruimd.

Poging tot grooming

- De jurisprudentie levert geen eenduidig beeld op ten aanzien van de juridische mogelijkheid van poging tot grooming.

- Voor strafbaarheid van 'grooming' is onder meer vereist dat de verdachte 'een ontmoeting voorstelt', en dat hij 'enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting'.

- Op 11 november 2014 heeft de Hoge Raad een arrest gewezen waarin de reikwijdte wordt geschetst van uitvoeringshandelingen in het kader van grooming.

- Uit het arrest van de Hoge Raad valt af te leiden dat die uitvoeringshandelingen ruim geïnterpreteerd dienen te worden.

- Handelingen als herhaaldelijk aandringen bij een slachtoffer, het onder druk zetten van een slachtoffer, en het geven van een telefoonnummer zijn volgens de Hoge Raad op het verwezenlijken van de voorgestelde ontmoeting.

- Concreet betekent dit dat verdachten in groomingzaken onder deze omstandigheden vervolgd kunnen worden voor voltooide grooming.

Slachtofferzorg grooming

- Voor slachtoffers van onder andere grooming-zaken is er een goede samenwerking tussen politie en slachtofferhulp Nederland.

- Politie, OM en slachtofferzorg hebben goede afspraken gemaakt hoe ze met slachtoffers van grote zedenzaken omgaan.

- Daarnaast is er een blijvende aanspreekbaarheid van de politiefunctionaris voor het slachtoffer.

4. Grooming (248a en 248e Sr)

Factsheet 4.2 inzet (virtuele) lokmiddelen

Inzet lokmiddelen

- De inzet van "lokmiddelen" bij de opsporing van online zedendelicten is in beginsel mogelijk.

- Opsporingsambtenaren zijn volgens rechtspraak van de Hoge Raad op basis van algemene taakstellende bepalingen de artikelen 3 Politiewet 2012 en 141 van het Wetboek van Strafvordering onder voorwaarden bevoegd tot het inzetten van lokmiddelen.

- De grens wordt gevormd door artikel 6 EVRM, dat het recht op een eerlijk proces waarborgt.

- Als iemand door het gebruik van lokmiddelen is bewogen tot andere handelingen dan waarop zijn opzet reeds is gericht (Tallon-criterium Hoge Raad) is er sprake van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs.

Inzet virtuele kindcreaties (concept-amendement VVD)

- In de TK is momenteel veel aandacht voor het Sweetieproject van Terre des Hommes.

- Sweetie is een door softwareprogrammeurs gecreëerd virtueel personage (een "avatar") dat is gebruikt door Terre des Hommes om in contact te komen met mensen die via de webcam deze Sweetie seksuele handelingen wilden laten verrichten tegen vergoeding.

- Er ligt een concept-amendement van de VVD om de inzet van een virtuele kindcreatie mogelijk te maken bij de opsporing

van online kindermisbruik via een wijziging van het Wetboek van Strafrecht (248e Sr, strafbaarstelling grooming).

- Het Wetboek van Strafrecht staat op zichzelf niet in de weg aan de inzet van virtuele kindcreaties bij de opsporing van grooming.

- Het voorgestelde amendement heeft gelet hierop geen toevoegde waarde.

- De inzet van virtuele kindcreaties is niet zozeer een materieelrechtelijke als wel een strafvorderlijke kwestie.

- Het OM kiest er zelf voor om bij de opsporing van online zedendelicten geen chatprogramma's/virtuele kindcreaties in te zetten, omdat hiermee al snel over de grens van geoorloofde uitlokking heen wordt gegaan.

- Het OM heeft hiertoe besloten na ervaringen met het Sweetieproject van Terre des Hommes.

- Het OM heeft zo'n 20 zaken aangeleverd gekregen van Terre des Hommes en heeft deze allemaal onderzocht.

- In geen van de zaken kon vervolging worden ingesteld, omdat telkens sprake was van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs.

- Concrete voorbeelden van uitlokgedrag van Sweetie zijn: communiceren over zaken waar betrokkenen het nog eerder niet over gehad hebben, suggestieve bewegingen maken, suggestieve voorstellen doen.

- Voor zover in de toekomst in de opsporingspraktijk gebruik gemaakt gaat worden van bewegende animaties zal de grens van geoorloofde uitlokking in acht moeten worden genomen.

- Er zijn onlangs schriftelijke Kamervragen gesteld over (de ervaringen van politie/OM met) het Sweetieproject (twee sets,

een kamerbreed, een D66), beantwoording vindt plaats langs de hiervoor vermelde lijn.

Sweetie 2.0

- Politie en OM werken samen met partners als Terre des Hommes om seksueel misbruik van kinderen aan te pakken.
- Het OM heeft uitgebreid gesproken met Terre des Hommes over de, vanuit strafvorderlijk perspectief, mislukte inzet van Sweetie.
- Afgesproken is dat een nieuw chatprogramma Sweetie 2.0 ontwikkeld zou worden door Terre des Hommes voor preventieve in doeleinden (waarschuwen, afschrikken).
- Sweetie 2.0 is nog ontwikkeling, het OM onderhoudt hierover contact met Terre des Hommes.

Inzet lokpuber

- De inzet van een virtuele kindcreatie voor de opsporing van online zedendelicten moet onderscheiden worden van de inzet van een zogenaamde “lokpuber“.
- Een lokpuber is een rechercheur die zich online voordoet als kind onder de zestien jaar en daarbij een afwachtende houding aanneemt.
- Op grond van huidige delictsomschrijvingen in de artikelen 248a Sr (verleiding van een minderjarige) en 248e Sr (grooming) is het materieelrechtelijk niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is.
- Het wetsvoorstel wijzigt deze artikelen op zodanige wijze dat het contact leggen met iemand die zich voordoet als een minderjarige alsnog strafbaar wordt.

- Hierdoor wordt de inzet van de lokpuber bij de opsporing van online grooming en verleiding van een minderjarige mogelijk.

Factsheet 5 Online handelsfraude (326d Sr)

Online handelsfraude

- Dit betreft het aanbieden van goederen of diensten op internet zonder dat er een intentie bestaat tot het leveren. Ook wel internetoplichting genoemd.

- Bij het landelijk meldpunt internetoplichting (LMIO) van de politie werd in 2014 ruim 7,9 miljoen euro aan internetfraude gemeld bij de politie. In totaal werd bijna 44.000 keer aangifte gedaan.

Belang preventie

- Voor de bestrijding van internetoplichting is een goede preventie essentieel. De bestrijding van online handelsfraude is een gedeelde verantwoordelijkheid van zowel private- als publieke partijen. Private partners hebben doorgaans beter zicht op waar en op welke wijze fraude het meest voorkomt. In overleg met de politie nemen de grotere marktpartijen zelf ook maatregelen die zijn gericht op het weren van malafide aanbieders.

- Dit blijkt echter niet voldoende om dit verschijnsel adequaat het hoofd te bieden. Er wordt namelijk gewerkt met tijdelijke websites, die voor een weekend online gaan en na het weekend offline. Zodra de kopers merken dat er niet wordt geleverd is de website al uit de lucht en de aanbieder van de goederen of diensten onvindbaar.

- Kenmerk van dergelijke vormen van handelsfraude is dat er een groot aantal slachtoffers is betrokken en dat een slachtoffer de verkoper of aanbieder niet kan aanspreken

omdat deze voor hem niet of nauwelijks is te achterhalen. De politie kan aan de hand van de aangiften of meldingen inzicht verkrijgen in de omvang van de handelsfraude en beschikt tevens over strafvorderlijke bevoegdheden om de daders op te sporen.

Noodzaak strafbaarstelling

- De vervolging van deze vorm van handelsfraude, op grond van het strafbare feit van oplichting (artikel 326 Sr) blijkt tot nu toe beperkt succesvol. Voor oplichting is vereist het aannemen van een valse naam of van een valse hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels. In de rechtspraak is geoordeeld dat het enkele aanbieden van goederen of diensten via het internet, zonder de intentie tot leveren, niet zonder meer oplichting oplevert.

- Bij de totstandkoming van het delict van oplichting kon niet worden voorzien dat het handelsverkeer in belangrijke mate via het internet zou verlopen en transacties in toenemende mate «op afstand» worden verricht. Er kan wel strafrechtelijk worden opgetreden tegen personen zich bij herhaling schuldig maken aan het kopen zonder te betalen (flessentrekkerij maar de mogelijkheden om strafrechtelijk op te treden tegen personen die zich bij herhaling schuldig maken aan het verkopen of aanbieden zonder te leveren zijn beperkt.

- Tegen deze achtergrond bestaat er aanleiding om het openbaar ministerie in staat te stellen vervolging in te stellen bij vormen van grootschalige handelsfraude, waarbij gebruik wordt gemaakt van het internet. De slachtoffers zijn daarbij gebaat, ook omdat zij zich dan ter zake van hun vordering tot schadevergoeding als benadeelde partij in het strafproces kunnen voegen (artikel 51f, eerste lid, Sv).

- Voorgesteld wordt een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vijfde categorie. Met de voorgestelde strafbedreiging wordt aangesloten bij de strafbedreiging voor oplichting (artikel 326 Sr) en flessentrekkerij (artikel 326a Sr).

Schaarse capaciteit

- De strafrechtelijke handhaving van online handelsfraude vindt plaats binnen de algemene handhavingskaders voor financieel-economische criminaliteit, waarbij een geïntegreerde aanpak wordt gehanteerd (preventie, toezicht, bestuursrechtelijke en strafrechtelijke aanpak). Vanwege de schaarse capaciteit voor opsporing en vervolging moeten het OM en de politie prioriteiten stellen en kan niet bij ieder geval van internetfraude worden overgaan tot opsporing en vervolging.

Factsheet 6 Decryptiebevel

Samenvatting

- Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is het voorstel voor het decryptiebevel aan de verdachte geschrapt.

- Met het voorstel voor het decryptiebevel aan de verdachte werd beoogd een extra mogelijkheid (naast de mogelijkheid tot binnendringen) op te nemen om versleutelde gegevens te laten ontsleutelen zodat kennis kan worden genomen van de inhoud van die gegevens met het oog op de waarheidsvinding.

- Het decryptiebevel aan de verdachte blijkt zowel juridisch als praktisch moeilijk haalbaar en komt daarnaast niet voldoende tegemoet aan de behoefte van de opsporingspraktijk.

Bezwaren

- Praktisch: Om het niet uitvoeren van een bevel tot decryptie als misdrijf aan te wijzen is opzet vereist. In de praktijk is dit bijzonder lastig te bewijzen als de verdachte een beroep doet op geheugenverlies of onjuiste gegevens verstrekt.

- Technisch: de technische ontwikkeling maakt het mogelijk bestanden op te slaan in het “hidden volume” waarvan de autoriteiten het bestaan moeilijk kunnen bewijzen. Hierdoor kan de verdachte voldoen aan het decryptiebevel zonder alle gegevens beschikbaar te stellen

- Juridisch/praktisch: Verhouding tot het nemo tenetur beginsel (beginsel dat een verdachte niet aan zijn eigen veroordeling hoeft mee te werken)

o Hier speelt de afweging tussen drie variabelen; (1) de hoogte van de strafbedreiging; (2) de verenigbaarheid met artikel 6 EVRM en (3) het risico van calculerend gedrag door de verdachte.

o De voorgestelde strafbedreiging van drie jaar gevangenisstraf (zoals in voorgesteld artikel 184b Sv) is aanzienlijk hoger dan de zes maanden gevangenisstraf waarover het EHRM zich in de zaak O'Heaney en Mc Guiness tegen Ierland heeft uitgesproken. Verlaging van die strafbedreiging kan bijdragen aan de kans dat het decryptiebevel door het EHRM verenigbaar wordt geacht met artikel 6 EVRM. Echter, een dergelijke verlaging zal het risico op calculerend gedrag door de verdachte navenant doen toenemen.

o In de afweging tussen deze drie variabelen is er geen uitkomst die zowel juridisch als praktisch een gunstige uitkomst heeft voor de in het wetsvoorstel beoogde doel.

Gemaakte afweging en conclusie

- Het decryptiebevel aan de verdachte leidt niet tot het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing, of is niet verenigbaar met art. 6 EVRM.

- De regering geeft daarom de voorkeur aan de bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk. Met behulp van deze bevoegdheid kunnen wachtwoorden en inlogcodes worden achterhaald en vastgelegd, zodat de versleutelde bestanden eenvoudig kunnen worden ontsleuteld en de versleutelde gegevens daadwerkelijk beschikbaar komen voor de opsporing. Bijkomend voordeel is dat deze bevoegdheid heimelijk wordt toegepast, zodat

gedurende het opsporingsonderzoek gegevens kunnen worden verzameld.

4. VRAGEN EN ANTWOORDEN (Q&A's)

Onderwerp : Financiën

Kamerlid :

Vraag: Waarom krijgt de politie geen extra middelen voor de uitvoering van het wetsvoorstel?

Antwoord:

- Politie ontvangt bijzondere bijdrage € 13,8 mln per jaar >> verdere professionalisering + bestrijding cybercrime.
- Aanschaf + implementatie van ICT-hulpmiddelen en voorbereiding implementatie van dit wetsvoorstel.
- Personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud ten laste algemene begroting politie.
- Nieuwe bevoegdheid leidt niet tot structurele toename van totale opsporingsinspanning.
- Overigens aan begroting politie extra bedrag toegevoegd voor aanpakken cybercrime. Voor 2017 > 1,4 miljoen euro, voor 2018 > 1,5 miljoen euro >> t.b.v. versterking personele en materiële capaciteit.

Onderwerp : Gegevens van niet verdachte personen (bijvangst)

Vraag: Hoe kan een privacy inbreuk van niet-verdachte personen worden voorkomen?

Antwoord:

- Inzage in communicatie van andere, niet-verdachte personen kan niet worden uitgesloten. Als verdachte via zijn geautomatiseerde werk communiceert over strafbare handelingen is er altijd wederpartij die informatie ontvangt en die niet perse verdachte is.
- Thans niet anders bij bevoegdheden als aftappen telecommunicatie of direct afluisteren.
- Wettelijke voorwaarden zodanig dat zoveel mogelijk wordt voorkomen dat de opsporing gegevens krijgt van derden.
- (1) Vereiste dat GW bij verdachte in gebruik is.
- (2) OvJ moet in bevel vermelden welk deel van GW het betreft en welke categorie van gegevens.
- (3) Alleen gegevens binnen reikwijdte bevel komen bij tactisch team >> gegevens van derden zoveel mogelijk beschermd.

Onderwerp : Definitie geautomatiseerd werk

Kamerlid :

Vraag: Waarom is de definitie van geautomatiseerd werk zo ruim? Gaat de politie pacemakers hacken en auto's tot stoppen dwingen?

Antwoord:

- Definitie GW sluit aan bij de definitie Cybercrimeverdrag Raad van Europa. >> Iets minder ruim dan die van de Europese Unie.
- Pacemakers en delen van auto's, zoals navigatiesystemen, vallen onder definitie.
- In WV wordt geen enkel soort geautomatiseerd werk bij voorbaat uitgesloten >> Ontwikkelingen binnen criminaliteit lastig te voorzien + risico misbruik uitgezonderde systemen door criminelen.
- Inperking evenmin niet toekomstbestendig.
- Binnendringen gebeurt zorgvuldig >> machtiging RC + beperking door proportionaliteit- en subsidiariteitstoets.
- In praktijk geen situatie voorstelbaar waarin binnendringen pacemaker proportioneel is.

Onderwerp : Aangiftebereidheid

Kamerlid :

Vraag: De aangiftebereidheid voor cybercrime en gedigitaliseerde criminaliteit moet worden verbeterd. Ik denk dat een publiekscampagne om de awareness bij burgers en bedrijven te vergroten een dringend nodig is. Hoe kijkt de minister hier tegenaan?

Antwoord:

- Zo hoog mogelijke aangiftebereidheid van groot belang voor effectievere aanpak criminaliteit >> geldt ook voor cybercrime en gedigitaliseerde criminaliteit.
- In brief 15 september jl. over de aangiftebereidheid aantal maatregelen aangekondigd om aangifte aan te moedigen.
- (1) Verbetering dienstverlening van de politie + aangifteproces optimaal inrichten >> laagdrempelige aangiftemogelijkheden.
- (2) Voor cybercrime en gedigitaliseerde criminaliteit meldpunten opgericht t.b.v. samenwerking met partners. Voorbeelden zijn landelijk meldpunt internetoplichting (LMIO), meldpunt kinderporno en centraal meld- en informatiepunt identiteitsfraude en –fouten.
- (3) Andere initiatieven zoals NCSC Handreiking Cybercrime >> verbetering aangiftebereidheid + aangiftekwaliteit.

Onderwerp : Kopen software, markt kwetsbaarheden

Kamerlid :

Vraag: Gaat de politie software kopen van bedenkelijke bedrijven? Houden we met het kopen van dergelijke software de markt voor onbekende kwetsbaarheden in stand?

Antwoord:

- Voor selectie van bedrijven geldt bestaande regelgeving voor inkoop.
- Bedrijven vermelden niet van welke kwetsbaarheden software gebruik maakt of hoe het bedrijf kennis daarover heeft verkregen.
- Het beperken van onderzoek naar kwetsbaarheden niet wenselijk >> kennis maakt systemen veiliger.
- Risico inzet kwetsbaarheden voor verkeerde doelen >> verkoop aan bepaalde partijen onwenselijk.
- Anonimiteit op internet maakt het makkelijk om heimelijk kennis over kwetsbaarheden te verkopen of te kopen >> lastig deze markt te controleren.
- Verkoop intrusion software (maakt gebruik van kwetsbaarheden) onder omstandigheden onderhevig aan exportcontrole.

Onderwerp : noodzaak en privacy

Kamerlid :

Vraag: Hoe reageert u op de argumenten tegen dit wetsvoorstel zoals gepresenteerd door BOF: Politie laat achterdeuren open staan; Noodzaak is onduidelijk; Schade economische belangen?

Antwoord:

- BOF benoemt drie essentiële elementen in de discussie.
- (1) Politie laat achterdeuren open staan. Politie is niet de enige die via die deur binnen kan komen.
- WV maakt computergebruik onveilig. Maar die kwetsbaarheden zijn er al. Kwetsbaarheden zijn talloos en wijdverbreid. Reeds bekende kwetsbaarheden wijd verbreid en gemakkelijk op te zoeken en in te zetten. Onbekende kwetsbaarheden vormen groot risico.
- Veel kwetsbaarheden al lang bij fabrikant bekend >> die kwetsbaarheden bieden criminaliteit mogelijkheden maar ook bruikbaar om criminaliteit op te sporen. Voorstelling dat politie kwetsbaarheid van internet verhoogd is overdreven.
- Beperking kwetsbaarheden in hardware + software van groot belang >> bevorderen melding kwetsbaarheden. In uitzonderlijke situaties melding uitstellen.
- (2) BOF stelt dat noodzaak WV onduidelijk is. Tijd heeft niet stilgestaan. Snelle ontwikkeling ICT >> biedt ook mogelijkheden voor criminaliteit. Bestaande opsporingsbevoegdheden schieten tekort >> toenemende

versleuteling van elektronische gegevens + gebruik van draadloze netwerken en cloudcomputingdiensten (locatie gegevens niet altijd bekend).

- (3) BOF benadrukt schade voor bedrijven als door inzet voorgestelde bevoegdheid gegevens kwijtraken en systemen stuk gaan. Risico verlies vertrouwen consumenten + verhuizen bedrijven naar buitenland.

- Mogelijke schade kan niet geheel worden uitgesloten maar risico's zo klein mogelijk houden >> zorgvuldige voorbereiding + inzet van deskundige getrainde personen + gebruik beproefde werkmethoden.

- Inzet gebaseerd op stapsgewijze benadering. Bevel wordt zorgvuldig voorbereid, risico's besproken met OvJ. Op basis informatie verdere beslissingen, conform werkwijze direct afluisteren. Dagelijks veelvuldig contact met OvJ.

- BOF gerespecteerde belangenbehartiger privacy >> in de actie "stop het hack voorstel" erg kort door de bocht.

Onderwerp : verschoningsrecht

Kamerlid :

Vraag: Kan een haatprediker zich op het wettelijk verschoningsrecht beroepen?

Antwoord:

- Op grond wetsgeschiedenis + jurisprudentie Hoge Raad kan worden aangenomen dat ook geestelijke beroep kan doen op wettelijk verschoningsrecht.

- Aldus kan ook imam in beginsel beroep doen op wettelijk verschoningsrecht.

- Verschoningsrecht beperkt tot informatie die onder een geheimhoudingsplicht valt en aan verschoningsgerechtigde als zodanig is toevertrouwd. Informatie die niet in kader advies of bijstand aan vertrouwenspersoon bekend wordt, valt dus buiten wettelijk verschoningsrecht.

- Uitingen van een haatprediker die niet vertrouwelijk worden gedaan, zoals tijdens openbare gebedssamenkomst of preek in moskee, vallen niet onder wettelijk verschoningsrecht.

Mogelijke vragen:

Waarom is alleen voor het overnemen van gegevens en het ontoegankelijkmaken van gegevens gekozen voor een drempel van een misdrijf waarvoor een gevangenisstraf van acht jaar of meer kan worden opgelegd?

Waarom is voor de andere opsporingshandelingen (tappen, direct afluisteren en vaststellen identiteit geautomatiseerd werk of gebruiker) een voorlopige hechtenisfeit al voldoende?

Is de vaststelling van de identiteit van het werk of de gebruiker een eerste stap? Hoe zit dan de verhouding met de andere opsporingshandelingen in elkaar? Is het eerst het een en dan het ander? En moet de RC dan opnieuw toestemming geven?

Vraag: Waarom wordt de procedure voor het ontoegankelijk maken van gegevens aangepast?

Antwoord:

Procedure artikel 54a Sr functioneert in praktijk niet goed >> zowel vervolgingsuitsluitingsgrond voor aanbieder telecommunicatiedienst als bevoegdheid voor OvJ tot geven bevel tot ontoegankelijk maken van gegevens. Combinatie vervolgingsuitsluitingsgrond en bevelsbevoegdheid werkt niet.

Daarom voorstel afzonderlijke bevoegdheid OvJ vorderen ontoegankelijkmaking gegevens. Aanvulling op bestaande vrijwillige Notice and take down (NTD) gedragscode.

College van procureurs-generaal >> NTD-gedragscode functioneert goed maar sommige internetproviders ondersteunen gedragscode niet.

Vraag: Waarom is de vordering van de officier van justitie beperkt tot ernstige strafbare feiten?

Antwoord:

College PG's waarschuwt voor OM als censurerende internetpolitie >> beperk bevoegdheid tot verdenking ernstig strafbaar feit (VH mogelijk).

Ook NOvA waarschuwt voor toepassing in bagatelgevallen. Vrijheid van meningsuiting kan hierbij in geding zijn.

Daarom is bevoegdheid gekoppeld aan ernstig strafbaar feit, waarvoor voorlopige hechtenis mogelijk is.

Nadat gegevens ontoegankelijk zijn is een rechterlijke beslissing nodig over lot gegevens. Ofwel teruggave aan rechthebbende ofwel vernietiging gegevens.

Vraag: hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn?

Antwoord:

Strikte wettelijke voorwaarden voor inzet bevoegdheid. (1) Criterium dringend opsporingsbelang. Eerst kiezen voor andere methoden, zoals vorderen van gegevens bij dienstverleners, plaatsen tap, doorzoeking of bevriezingsbevel.

(2) Voorafgaande machtiging RC. Toets dringend opsporingsbelang, op basis proportionaliteit en subsidiariteit.

(3) Toepassing voorbehouden aan speciale opsporingsambtenaren die over ICT-kennis beschikken en deel uitmaken van een speciaal team. Het technische team is organisatorisch gescheiden van het tactische team, dat het tactische opsporingsonderzoek vericht.

(4) Zorgvuldige voorbereiding inzet >> mogelijke beveiligingsmaatregelen + noodzaak heimelijk opereren. Methode binnendringen afstemmen op GW. Voorgenomen inzet voorgelegd aan Centrale Toetsingscommissie (CTC), die adviseert aan College PG’s over inzet bijzondere BOB-bevoegdheden.

Vanwege deze procedurele eisen geen gemakkelijke inzet.

Vraag: Waarom krijgen ook bijzondere opsporingsdiensten de mogelijkheid van de nieuwe bevoegdheid gebruik te maken? Zijn de vormen van criminaliteit waarmee deze diensten te maken krijgen ernstig genoeg zijn om de inzet van de nieuwe bevoegdheid te rechtvaardigen?

Antwoord:

BOD'en houden zich bezig met strafrechtelijke handhaving rechtsorde op beleidsterreinen ministers van EZ, FIN, LenI en SWZ.

Handhaving bijzondere wetten, zoals Wet op de Inkomstenbelasting en de Wet op de economische delicten + feiten strafbaar gesteld in commune strafrecht, zoals fraude + witwassen.

Opsporingsambtenaren BOD'en bevoegd tot inzet BOB-bevoegdheden, zoals de observatie of het aftappen van telecommunicatie. Alles onder gezag OvJ.

Vanwege de ontwikkelingen cybercrime ook BOD'en geconfronteerd met soortgelijke belemmeringen voor opsporing als de politie.

BOD-ambtenaren moeten voldoen aan eisen deskundigheid en samenwerking>> uitgewerkt bij AMvB.

Waarschijnlijk maakt alleen FIOD gebruik van bevoegdheid >> grootschalige financiële fraude gepleegd door technisch zeer capabele criminelen. Gebruik innovatieve hackmethoden, online handelsplaatsen op Darknet + alternatieve betalingsvormen zoals Bitcoin.

Vraag: Welke geautomatiseerde werken vallen op dit moment onder de definitie van geautomatiseerd werk vallen en waarom?

Antwoord: Begrip GW ingekaderd in Cybercrimeverdrag Raad van Europa. Is een apparaat of groep van onderling verbonden apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken.

Ieder apparaat dat op basis van een programma automatisch gegevens verwerkt valt onder reikwijdte GW. NL gehouden tot implementatie van dit verdrag.

Begripsomschrijving is ruim. Ook groep van onderling verbonden apparaten valt onder de definitie GW, mits een of meer van die apparaten op basis van een programma gegevens verwerkt.

Grens ligt niet zozeer in definitie GW als wel in beperking in toepassing bevoegdheid tot binnendringen. Als verschillende apparaten met elkaar zijn verbonden, bijvoorbeeld in een thuisnetwerk, dan zal bevel meerdere GW’s kunnen omvatten.

Vereist is dat de geautomatiseerde werken bij de verdachte in gebruik zijn + dat binnendringen noodzakelijk is voor opsporing ernstige strafbare feiten.

OvJ moet in bevel opnemen om welke GW’s het precies gaat zodat RC rechtmatigheid binnendringen kan toetsen. Inzet beperkt tot GW zoals in bevel omschreven.

Als blijkt dat ander GW moet worden binnengedrongen >> aanvullend bevel + aanvullende machtiging RC vereist. Bevel + machtiging mondeling mogelijk >> stapsgewijze aanpak met betrokkenheid RC

Vraag: Hoe weet de politie waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig zijn en hoe groot het risico is dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing? Hoe wordt voorkomen dat ongericht gegevens worden verzameld?

Antwoord: Zorgvuldige voorbereiding >> in verkennende fase informatie over strafbare feiten en personen in kaart gebracht. Beeld vormen van gegevens die nodig zijn voor het onderzoek naar de specifieke strafbare feiten.

Verkennende fase is basis bevel OvJ. Onderzoekshandelingen vermelden in bevel. Ook in bevel vermelden deel van GW + categorie van gegevens waarnaar wordt gezocht + aard en functionaliteit gebruikte software.

Onderzoek verricht door speciaal technisch team + alleen gegevens binnen reikwijdte bevel OvJ in beeld.

Bij aftappen telecommunicatie, vastlegging van in GW opgeslagen gegevens of vorderen gegevens bij derden is mogelijk dat ook gegevens van anderen in beeld komen. Dit is thans ook zo bij toepassing van die bevoegdheden in analoge wereld.

Vraag: Waarom is het op dit moment niet mogelijk om met bestaande bevoegdheden om gegevens te achterhalen die zijn opgeslagen in de Cloud? Kunnen praktijkvoorbeelden worden gegeven van opsporingsonderzoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen?

Antwoord:

Thans problemen als cloudaanbieder niet gevestigd in land waar de server staat met informatie. Dan RH-verzoek doen en dat kost veel tijd >> tot wel negen maanden + risico verlies bewijsmateriaal.

Diverse onderzoeken gestaakt vanwege niet of niet tijdig reageren op rechtshulpverzoeken. Bijvoorbeeld zaak waarbij klanten Nederlandse bank slachtoffer van computervredebreuk en vervolgens oplichting en diefstal. Ook een aanval op honderden emailadressen van MKB-bedrijven met daarin malware verwerkt die een Remote Acces Tool installeerde op GW's van die MKB-bedrijven (bewijs uit cloud was al weg).

Daarnaast probleem vaststelling locatie gegevens in de cloud. Als locatie niet te bepalen is >> RH-verzoek aan bepaald land niet mogelijk.

De voorgestelde bevoegdheid tot het op afstand binnendringen in geautomatiseerd werk brengt uitkomst omdat gegevens worden overgenomen van het GW zelf >> opsporing minder afhankelijk van informatie uit de cloud.

Vraag: Is het waar dat de politie op dit moment al computers hackt? Wat is daarvan de wettelijke grondslag?

Antwoord: Nee, dat is niet waar. Wel onder omstandigheden netwerkzoeking mogelijk, met machtiging RC. Dan betreden besloten plaats met als doel een GW te doorzoeken op vooraf bepaalde gegevensbestanden en deze gegevens zo nodig vast te leggen (art. 125i Sv).

In aantal strafzaken toegepast. Politie experimenteert niet met het overnemen van computers van verdachten.

Bij voorbereidingen op invoering WV hebben opsporingsambtenaren kennis opgedaan van technieken die hiervoor nodig zijn. Daarbij geen sprake van binnendringen in GW.

Vraag: hoe wordt omgegaan met het wettelijke verschoningsrecht, bijvoorbeeld van een advocaat?

Antwoord: Bestaande regeling bescherming verschoningsrecht bij toepassing BOB-bevoegdheden is van toepassing. Regeling verplicht tot vernietiging processen-verbaal en andere voorwerpen, voor zover die mededelingen behelzen gedaan door of aan een persoon die zich kan verschonen als hem als getuige naar de inhoud van die mededelingen zou worden gevraagd (art. 126aa Sv).

EHRM heeft het Nederlandse systeem voldoende precies en begrijpelijk geacht >> biedt voldoende waarborgen om te kunnen worden aangemerkt als «recht» in de zin van artikel 8 EVRM (Aalmoes vs. Nederland).

Als OvJ vaststelt dat mededelingen onder deze verplichting vallen >> terstond bevelen vernietiging processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen. Gegevens mogen niet in het opsporingsonderzoek worden gebruikt.

Als de geheimhouder zelf verdachte is, wordt oordeel van de deken ingewonnen over de vraag welke gegevens dergelijke mededelingen behelzen.

Procedure voor vernietiging gegevens uitgewerkt in Besluit bewaren en vernietigen niet-gevoegde stukken.

Vraag: Is de internettap niet voldoende om gegevens af te tappen die met een geautomatiseerd werk worden verzonden?

Antwoord: Nee. IP-tap wordt geplaatst op IP-adres. Bij IP-tap wordt alle dataverkeer afgetapt dat van en naar een huisadres of IP-adres gaat, dus ook het dataverkeer van huisgenoten of anderen die de betreffende aansluiting gebruiken.

In sommige gevallen biedt IP-tap geen soelaas. Bijvoorbeeld bij gebruik hotspots >> dan bij een groot aantal aanbieders IP-tap om internetverkeer via hotspots te onderscheppen.

Voor aftappen communicatie heeft aanbieder MAC-adres nodig >> bij hotspot komt niet MAC-adres laptop maar MAC-adres hotspot bij aanbieder binnen.

Verder is IP-tap beperkt tot de communicatie die via een aanbieder wordt afgehandeld; geen inzicht in gegevens die (reeds) op het geautomatiseerde werk zijn opgeslagen en die tijdens de periode van het tappen niet met anderen worden uitgewisseld.

Tenslotte biedt IP-tap geen soelaas bij versleuteling (encryptie). Dan wordt digitale informatie afgetapt die gecodeerd is. Criminelen maken steeds vaker gebruik van versleuteling van communicatie, zoals TOR, VPN en andere vergelijkbare mogelijkheden.

Vraag: Hoe rekening wordt gehouden met de wettelijke bronbescherming van journalisten?

Antwoord: Wettelijk verschoningsrecht beperkt tot de advocaat, de arts en de geestelijke. Journalisten geen wettelijk verschoningsrecht vanwege hun stand, beroep of ambt.

Arrest Goodwin >> EHRM heeft geoordeeld dat aan journalisten geen volledig verschoningsrecht toekomt, vanwege belang vrijheid meningsuiting en persvrijheid onder omstandigheden aanspraak op recht op bronbescherming. Dit recht is niet absoluut maar kan door zwaarderwegend belang opzij worden gezet. Op basis van dit arrest heeft Hoge Raad recht op bronbescherming voor journalist nader ingekaderd.

Arrest Sanoma >> wetsvoorstel bronbescherming in strafzaken >> wettelijke verankering recht op bronbescherming. In afwachting inwerkingtreding wetsvoorstel is geldend recht vastgelegd in Aanwijzing College van PG’s. Thans gevolgde beleid >> grote terughoudendheid bij toepassing van dwangmiddelen tegen journalisten.

Vraag: Kunt u nog even kort aangeven waarom dit eigenlijk nodig is?

Antwoord: In MvT uitgebreid ingegaan op ontwikkelingen die voorgestelde bevoegdheden noodzakelijk maken. Opkomst internet + wijdverbreid gebruik biedt samenleving voordelen maar ook risico's .

Drie wezenlijke problemen

(1) Toenemende versleuteling van elektronische gegevens. IP-tap biedt dan alleen nullen en enen maar geen leesbare gegevens. Verbod op decryptie of een verplichting tot verzwakking van encryptie niet wenselijk >> in bepaalde uitzonderlijke gevallen gericht in GW binnendringen zodat gegevens worden verkregen voordat deze worden versleuteld.

(2) Toenemend gebruik draadloze netwerken, «hotspots» + dynamische IP-adressen. Bij IP-tap op router wordt alleen in- en uitgaande communicatie afgetapt, interne communicatie op netwerk niet onderschept. Bij gebruik hotspot is tappen vrijwel onmogelijk.

(3) Toenemende opslag informatie in de cloud. Bestaande bevoegdheden als een netwerkzoeking en doorzoeking ter vastlegging van gegevens gaan uit van gegevens op een bepaalde gegevensdrager op een vaste plaats bevindt. Dit strookt steeds minder met werkelijkheid.

Vraag: Brengt dat hacken door de politie geen enorme schade toe aan Nederland als vestigingsland voor bedrijven?

Antwoord:

Inzet bevoegdheid binnendringen in GW alleen in uitzonderlijke gevallen, als minder ingrijpende bevoegdheid niet helpt. Bij cloudcomputingdiensten minder ingrijpende bevoegdheid voorhanden, zoals vorderen van gegevens bij dienstverlener of doorzoeking ter vastlegging van gegevens.

Meeste clouddienstverleners werken goed samen met opsporing (op basis vordering verstrekking gegevens). Sommige clouddienstverleners werken slecht mee of nemen technische maatregelen om opsporing te hinderen (bullet proof hosting providers).

Binnendringen bij cloudcomputingdiensten niet bij voorbaat geheel uitgesloten >> beperkt tot uitzonderlijke gevallen.

Bevoegdheid kan bijdragen aan veiligheid van in Nederland gevestigde bedrijven omdat opsporing kan optreden tegen strafbare feiten jegens cloudproviders.

Vraag: De Minister van Veiligheid en Justitie heeft in antwoord op Kamervragen laten weten dat de politie over software beschikt die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. Hoe zit dat?

Antwoord: Inzet software gericht op direct afluisteren van gesprekken (126l Sv). Binnendringen in een ruimte en installeren keylogger op toetsenbord >> keylogger registreert toetsaanslagen op het toetsenbord. Er wordt dan dus niet gehackt.

Daarnaast onder omstandigheden, op basis machtiging RC, betreden van besloten plaats en vanaf die plaats onderzoek doen in een elders aanwezig GW (art. 125i Sv). Deze bevoegdheid is ook bekend als de netwerkzoeking.

Vraag: Is dit niet een hele ingrijpende bevoegdheid die de positie van de verdachte wijzigt omdat dit heimelijk wordt toegepast en die dermate ingrijpend is dat dit meegenomen moet worden bij de vaststelling van de contouren van het modernisering van het Wetboek van Strafvordering.

Antwoord: Voorwaarden voor inzet voorgestelde bevoegdheid komen overeen met de voorwaarden voor bestaande opsporingsbevoegdheden met een vergelijkbaar indringend karakter. Geen sprake van ingrijpende wijziging positie verdachte.

Inzet bevoegdheid bij verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven ernstige inbreuk op rechtsorde oplevert.

Dit vereiste ook bij andere heimelijke Bob-bevoegdheden als infiltratie, het direct afluisteren of het vorderen van bijzondere persoonsgegevens, zoals gegevens over iemand godsdienst of levensovertuiging, ras of politieke gezindheid.

Bij binnendringen voor veiligstellen of ontoegankelijk maken van gegevens geldt zwaarder verdenkingscriterium >> verdenking van misdrijf waarop gevangenisstraf van acht jaar of meer is gesteld dan wel misdrijf dat bij algemene maatregel van bestuur is aangewezen.

Vraag: Kan ook zomaar een pacemaker door de politie worden gehackt? Waar zijn we dan mee bezig? Wilt u de apparaten waarin kan worden binnengedrongen niet bij voorbaat beperken, bijvoorbeeld bij algemene maatregel van bestuur?

Antwoord: Doel van bevoegdheid is toegang tot gegevens die in GW zijn of worden verwerkt t.b.v. opsporing ernstige vormen van computercriminaliteit of andere ernstige misdrijven.

Pacemaker valt onder definitie GW >> in pacemaker naar verwachting geen gegevens die bijdragen aan opsporing ernstige vormen van computercriminaliteit of andere ernstige strafbare feiten.

Als dit al zo zou zijn dan is het in praktijk moeilijk denkbaar dat RC het binnendringen in pacemaker proportioneel acht.

Vraag: Kan de politie ook informatiesystemen in auto's, zoals de TomTom, gaan hacken?

Antwoord: Als apparaten in auto voldoen aan definitie GW >> dan op afstand binnendringen mogelijk als daarin gegevens zijn of worden verwerkt die van belang zijn voor de opsporing van ernstige strafbare feiten.

Bijvoorbeeld navigatiesysteem dat informatie bevat over route of verblijfplaats voertuig >> kan zeer interessant zijn voor opsporing liquidatie. Dus bij voorbaat niet eenvoudig te beperken tot bepaalde GW's.

In algemeen niet wenselijk specifieke apparaten van bevoegdheid uit te sluiten. Aanwijzen van specifieke categorie apparaten waar de bevoegdheid niet voor kan worden toegepast, kan betekenen dat cybercriminelen die deze apparaten voor criminele doeleinden gebruiken niet effectief kunnen worden aangepakt.

Wel kan aard van GW reden zijn voor grote terughoudendheid bij inzet, of bepalend zijn voor het besluit tot de inzet of juist het afzien daarvan.

Vraag: kan de politie deze bevoegdheid gebruiken om een voertuig op afstand tot stilstand te brengen?

Antwoord: Bevoegdheid tot binnendringen van GW is gekoppeld aan bepaalde onderzoekshandelingen >> aftappen telecommunicatie, direct afluisteren, observatie, vastleggen van gegevens en ontoegankelijk maken gegevens.

Op afstand laten stoppen voertuig mogelijk als een vorm van het ontoegankelijk maken van gegevens >> gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten.

Toepassing voor stoppen voertuig niet voor de hand vanwege beperkt verband tussen gegevens boordcomputer en het plegen van een strafbaar feit. Bovendien vormen gegevens boordcomputer geen gegevens waarvan het bezit of de verspreiding minder wenselijk is vanuit het oogpunt van het belang van de bescherming van slachtoffers of van kwetsbare groepen in de samenleving.

Niet waarschijnlijk dat OvJ of RC hiervoor bevel of machtiging afgeven.

Vraag: Kan iemand het verschoningsrecht misbruiken door een map op de harde schijf «medisch dossier» of «gesprekken met mijn advocaat» te noemen? Mogen politie en justitie dan verder mogen zoeken naar de informatie die hierachter ligt?

Antwoord: Naamgeving «medisch dossier» of «gesprekken met mijn advocaat» van een map op een computer kan aanleiding geven voor vermoeden dat gegevens in die map onder verschoningsrecht vallen.

Bij twijfel over verschoningsrecht of vermoede van doorbrekingsgrond >> OvJ kan de gegevens voorleggen aan RC. Als RC oordeelt dat gegevens niet onder verschoningsrecht vallen kunnen gegevens worden gebruikt.

Dit kan geval zijn als ondanks de naam «medisch dossier» een map helemaal geen gegevens bevat die onder het medisch beroepsgeheim vallen of een doorbrekingsgrond van toepassing is, bijvoorbeeld omdat de verschoningsgerechtigde zelf ook verdachte is.

Vraag: De regering wil een lijst van delicten opstellen, waarvoor geen gevangenisstraf van tenminste acht jaar kan worden opgelegd maar waarbij een computer toch kan worden doorzocht om gegevens over te nemen of gegevens ontoegankelijk te maken. Wordt daarmee niet terug genomen wat met de grens van acht jaar is gegeven?

Antwoord:

Bij AMvB aanwijzen misdrijven die worden gepleegd m.b.v. GW + duidelijk maatschappelijk belang bij beëindiging strafbare situatie en vervolging daders.

Misdrijven als gebruik van een botnet, aanbieden, verspreiden of bezitten kinderpornografie, verleiding minderjarige tot ontucht en «grooming». Dan vaak geen ander aangrijpingspunt voor opsporing.

Aanwijzing delicten biedt mogelijkheid flexibel in te spelen op snelle ontwikkelingen cybercrime.

Vraag: Wat wordt precies bedoeld met het vereiste dat het geautomatiseerde werk bij de verdachte in gebruik is?

Antwoord: Op grond van feiten + omstandigheden aannemelijk dat verdachte gebruik maakt van het GW. Niet vereist dat verdachte enige gebruiker is.

Niet vereist dat verdachte feitelijk van het geautomatiseerde werk gebruik maakt tijdens het binnendringen. Met de aanduiding «een GW dat bij de verdachte in gebruik is» is tevens bedoeld het GW waarvan verdachte gebruik heeft gemaakt

Niet vereist dat verdachte eigenaar is van het geautomatiseerde werk. Evenmin vereist aantonen dat gegevens aan verdachte toebehoren. Als verdachte verweer voert dat hij niets te maken heeft met de vastgelegde gegevens dan is het aan OvJ om met feiten en omstandigheden dit verweer te weerleggen

Met vereiste dat GW bij verdachte in gebruik is wordt voorkomen dat bevoegdheid wordt ingezet jegens anderen dan verdachte.

Vraag: Hoe verhoudt het ontoegankelijk maken van gegevens zich tot het doel juist heimelijk een geautomatiseerd werk binnen te dringen zonder dat de desbetreffende persoon daar weet van heeft?

Antwoord: Bevoegdheid ontoegankelijkmaken gegevens vergelijkbaar met bevoegdheid tot inbeslagneming voorwerpen met het oog op onttrekking aan verkeer.

Voor beide bevoegdheden >> maatregel ter bescherming van maatschappij. Bij voorwerpen drugs of vuurwapens, bij gegevens kinderpornografie of een botnet dat essentiele maatschappelijke diensten belemmert.

Door ontoegankelijkmaken kan betrokkene op de hoogte raken van opsporingsonderzoek. Beperking van beschikbaarheid van gegevens in maatschappelijk verkeer prevaleert boven het belang van de afscherming van opsporingsonderzoek jegens betrokkene.

Situatie vergelijkbaar met verbod op doorlaten >> ook betrekking op het voorkomen dat schadelijke voorwerpen, zoals drugs of vuurwapens, op de makt komen. De politie moet die voorwerpen dan inbeslag nemen. Belang van het voorkomen dat illegale goederen op de markt komen weegt zwaarder dan het belang van afscherming van het opsporingsonderzoek.

Vraag: Hoe lang duurt het ontoegankelijk maken van gegevens?

Antwoord: OvJ bepaalt specifieke maatregelen om gegevens ontoegankelijk te maken. Als gegevens worden verwijderd dan dienen zij te worden behouden t.b.v. de strafvordering. In het kader van de ontoegankelijkmaking kunnen de gegevens dan ook niet worden gewist.

Ontoegankelijkmaking betreft voorlopige maatregel, in afwachting van beslissing rechter. Ontoegankelijkmaking van de gegevens duurt in beginsel tot het moment van de rechterlijke beslissing (o.g.v. art. 354 of 552fa Sv).

Zodra belang strafvordering zich niet meer verzet tegen opheffing maatregel >> OvJ bepaalt dat gegevens weer ter beschikking worden gesteld van beheerder GW.

Vraag: Is het heimelijk binnendringen van computers wel verenigbaar met het Cybercrimeverdrag?

Antwoord: Cybercrimeverdrag >> iedere partij neemt wetgevende en andere maatregelen om aan eigen autoriteiten bevoegdheid te verlenen tot het op haar grondgebied doorzoeken van of zich op vergelijkbare wijze toegang verschaffen tot computersysteem en de daarin opgeslagen computergegevens (art. 19 Cybercrimeverdrag).

Toelichtend rapport («Explanatory report») >> bepaling heeft betrekking op doorzoeking van plaatsen ter vastlegging van gegevens die op een geautomatiseerd werk of een gegevensdrager zijn opgeslagen. Dit is in NL geregeld (art 125i Sv).

Cybercrimeverdrag regelt niets over het zonder toestemming van de gebruiker heimelijk binnendringen van GW, maar staat daar anderzijds ook niet aan in de weg.

Aldus laat dit verdrag ruimte om zonder toestemming van de gebruiker zijn GW heimelijk binnen te dringen.

Vraag: Kan op basis van het wetsvoorstel een peilzender worden aangebracht om een persoon te volgen?

Antwoord: Ja, met stelselmatige observatie kunnen gangen van persoon worden nagegaan. Kan ook m.b.v. peilzender. Binnendringen van GW biedt mogelijkheid via plaatsing van software inschakelen GPS-functie van GW >> locatie aparaat kan zeer nauwkeurig worden bepaald.

Als het om smartphone gaat dan kan via locatie smartphone de locatie van gebruiker worden vastgesteld en diens bewegingen gevolgd >> smartphone is peilzender.

Plaatsbepaling op basis GPS-gegevens nuttig als andere observatiemethoden niet of onvoldoende opleveren of als verblijfplaats verdachte onbekend is.

Vraag: Is het via software volgen van gegevensstromen niet even ingrijpend voor de privacy als het permanent waarnemen wat zich in een woning afspeelt? Er kunnen toch geen camera's in een woning worden gehangen?

Antwoord: Raad van State >> differentiatie in opsporingshandelingen, afhankelijk van ingrijpendheid inbreuk op de persoonlijke levenssfeer.

Eens met Raad van State dat op afstand binnendringen gevolgd door doorzoeken van alle gegevens die GW zijn opgeslagen, verdergaande inbreuk op de privacy oplevert dan binnendringen gevolgd door het aftappen van communicatie of de stelselmatige observatie.

Raad van State vergelijkt bevoegdheid tot het doorzoeken van gegevens met bestaande bevoegdheid van heimelijk binnentreden in woning t.b.v. opnemen vertrouwelijke communicatie (art. 126l Sv) >> beperkt tot verdenking misdrijf met gevangenisstraf acht jaar of meer.

N.a.v. advies Raad van State wetsvoorstel aangescherpt >> voor onderzoekshandelingen t.b.v. vastleggen of ontoegankelijk maken van gegevens beperkt tot verdenking misdrijf met gevangenisstraf acht jaar of meer **of** een **misdrijf dat bij algemene maatregel van bestuur is aangewezen**.

Vraag: Kan in dit verband ook de webcam door de politie worden aangezet?

Antwoord: Dit is **niet** mogelijk. Bij stelselmatige observatie verbod op betreden woning om technisch hulpmiddel, zoals camera, te installeren. De politie mag een woning dus niet betreden om een webcam op te hangen. Uit dit verbod vloeit voort dat webcam niet kan worden aangezet

Heimelijk aanzetten van webcam in woning is, evenals heimelijke betreding van woning, bij toepassing van bevoegdheid niet toegestaan.

Vraag: Wat wordt er precies in het Besluit technische hulpmiddelen geregeld?

Antwoord: Besluit technische hulpmiddelen strafvordering wordt niet aangepast >> nieuwe AMvB voor digitale opsporing.

(1) eisen inrichting en werking technisch hulpmiddel dat wordt gebruikt voor onderzoek in GW >> de vastgelegde gegevens betrouwbaar, voor derden toetsbaar en niet manipuleerbaar.

(2) instelling van software kan worden gedifferentieerd naar gebruik verschillende functionaliteiten.

(3) inhoud geregistreerde gegevens identiek aan inhoud gedetecteerde gegevens.

(4) transport signalen van GW naar server via versleuteld bestand.

(5) Bij keuring wordt getoetst of software aan eisen voldoet. Alleen na goedkeuring mag software worden ingezet.

(6) Logging technische handelingen >> controle op uitvoering bevel OvJ.

Vraag: Waarom er niet voor gekozen is de rechter-commissaris aanwezig te laten zijn tijdens het hacken, aangezien bij een huiszoeking de rechter-commissaris wel aanwezig is?

Antwoord: Bevel binnendringen GW geldt voor periode van vier weken >> tijdstip uitvoering ligt tevoren niet vast + duur inzet kan verschillen.

Aanwezigheid RC tijdens binnendringen >> praktische uitvoeringsproblemen. RC kan niet vier weken 'standby' zijn.

RC kan wel bepalen dat binnendringen in GW en/of verrichten bepaalde onderzoekshandelingen in zijn aanwezigheid worden verricht.

RC niet altijd aanwezig bij doorzoeking woning. In geval dringende noodzaak kan OvJ of hulpOvJ optreden. Verder RC tijdens doorzoeking niet altijd permanent aanwezig, bijvoorbeeld bij gelijktijdig doorzoeken verschillende plaatsen.

Vraag: Kan het bewijsmateriaal worden gemanipuleerd dor de logging uit te schakelen?

Antwoord: Software laat niet toe manipuleren, wijzigen of verwijderen gegevens. Controle software voor inzet.

Logging kan worden uitgeschakeld >> altijd zichtbaar in loggingsgegevens.

Alleen speciale ambtenaren toegang tot systeem van waaruit op afstand binnendringen GW wordt uitgevoerd. Tactische opsporingsambtenaren die opsporingsonderzoek doen geen toegang.

In theorie kan opsporingsambtenaar gegevens op apparaat zetten >> situatie wijkt niet af van analoge wereld. Tijdens huiszoeking verdovende middelen in kast leggen of tijdens doorzoeking auto wapens in kofferbak leggen.

Digitale omgeving maakt juist controle mogelijk d.m.v. logging. Logging zal manipulatie aan het licht brengen.

Vraag: Bent u bereid geautomatiseerde werken die zich op (of in) een persoon bevinden, zoals een telefoon of pacemaker, uit te sluiten?

Antwoord: Huidige techniek maakt locatiebepaling GW mogelijk. GW wordt peilzender. Bij smartphone kan locatie bezitter worden bepaald.

Plaatsbepaling op basis GPS-gegevens nuttig als andere observatiemogelijkheden niet tot resultaat leiden of als verblijfplaats verdachte onbekend is >> de peilzender in mobiele telefoon bevindt zich op of aan het lichaam of de kleding van de verdachte.

OvJ moet voorgenomen inzet technisch middel in bevel melden >> voorafgaande rechterlijke toetsing verzekerd.

Vraag: Is er een verschil is tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem en zo ja, zijn daar dan verschillende bevoegdheden voor nodig?

Antwoord: MvT >> term onderzoek in GW omvat (1) het op afstand heimelijk binnendringen in GW en (2) verrichten van bepaalde onderzoekshandelingen.

Binnendringen omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel t.b.v. vastleggen gegevens.

Verrichten van onderzoekshandelingen omvat bevoegdheden die in WV zijn omschreven. Dit betreft (1) vaststelling bepaalde kenmerken van GW of gebruiker (2) vastlegging gegevens die in GW zijn of worden opgeslagen (3) ontoegankelijkmaking gegevens (4) aftappen telecommunicatie en direct afluisteren en (5) bevel stelselmatige observatie.

Voor binnendringen bevel OvJ + machtiging RC + VH-feit.

Voor onderzoekshandelingen bevel OvJ + machtiging RC + VH-feit voor (1), (4) en (5). VH-feit + acht jaar **of** VH-feit op lijst AMvB voor (2) en (3).

Bevel of machtiging binnendringen kan worden gecombineerd met bevel of machtiging voor onderzoekshandeling(en), zodat één bevel wordt gegeven. Dit is aan RC ter beoordeling.

Vraag: Heeft de betrokkene recht op schadevergoeding als door het binnendringen schade is ontstaan?

Antwoord: O.g.v. WSv vergoeding specifieke vormen van schade >> zoals na onterecht voorarrest.

WSv kent geen regeling voor andere vormen van strafvorderlijke schade, zoals na inbeslagneming of huiszoeking.

Betrokkene kan schade claimen bij burgerlijke rechter >> beroep op onrechtmatige (overheids)daad.

Degene die claimt moet bewijzen dat schade is veroorzaakt door degene die daarop wordt aangesproken («wie eist bewijst»).

Op basis van inbreng betrokkene kan rechter aan politie opdragen aantonen dat schade niet door politie is veroorzaakt. Logging kan helderheid bieden over technische handelingen die hebben plaatsgevonden >> aan rechter te beslissen over schadevergoeding.

In beginsel geen grondslag vergoeding strafvorderlijke schade na onherroepelijke veroordeling. Alleen anders als vanaf aanvang geen rechtvaardiging strafvorderlijk optreden vanwege strijd met het recht. Bijvoorbeeld bij optreden zonder redelijk vermoeden van schuld of bij toepassen bevoegdheden zonder machtiging RC.

Vraag: Wordt voor het overnemen van gegevens altijd een technisch hulpmiddel gebruikt?

Antwoord: In bepaalde gevallen blijft plaatsen technisch hulpmiddel (software) achterwege. Bijvoorbeeld als benodigde gegevens direct na binnendringen kunnen worden ingezien of overgenomen t.b.v. vaststellen identiteit GW.

Noodzaak inzet technisch hulpmiddel afhankelijk van aard inzet, aard GW, en of gegevens zonder technisch hulpmiddel kunnen worden vergaard.

Vraag: Worden bedrijven gedwongen om kwetsbaarheden in software in te bouwen? Wordt antivirusbedrijven gevraagd bepaalde aanvallen door te laten

Antwoord: Bedrijven niet gedwongen tot inbouwen kwetsbaarheden in software >> evenmin worden antivirusbedrijven gevraagd bepaalde aanvallen door te laten.

Niet bij voorbaat uitsluiten dergelijke keuze in uitzonderlijk geval in opsporingsonderzoek. Directe en maatschappelijke gevolgen van aanval, kans op succes in het opsporingsonderzoek en mogelijkheid schade te herstellen bij afweging van belang.

Vraag: Hoe wordt voorkomen dat derden ook gebruik maken van wetsbaarheden die de politie gebruikt?

Antwoord: Bij gebruik bepaalde kwetsbaarheid door politie >> maatregelen om te voorkómen dat anderen daar tegelijk gebruik van maken. Bijvoorbeeld vooraf analyseren GW, na binnendringen nader analyseren t.b.v. inschatting risico, in tijd beperken contact tussen systeem en systeem politie en het monitoren van activiteiten in het systeem.

Maatregelen niet alleen t.b.v. beperken mogelijkheid medegebruik kwetsbaarheid door derden >> ook t.b.v. beperken risico van ontdekking opsporingsonderzoek en t.b.v. bewaking integriteit bewijsmateriaal.

Voor geen enkel systeem dat met internet is verbonden bij voorbaat volledig uit te sluiten dat op een bepaald moment wordt binnengedrongen door criminelen of buitenlandse mogendheden.

Vraag: Waarom wordt de software niet altijd verwijderd na afloop van het onderzoek?

Antwoord: Nadat afronding onderzoek in GW volgt verwijdering TH >> soms biedt software mogelijkheid zelfstandige verwijdering na vooraf ingestelde periode.

Na verwijdering software ontvangt politieserver geen gegevens meer.

In uitzonderlijke gevallen afzien van (volledige) verwijdering TH >> zwaarwegende belangen tegen verwijdering, zoals als verwijderen aanzienlijke risico's oplevert voor systeem.

Achtergebleven sporen hebben als zodanig niet of nauwelijks invloed op functioneren GW. Bij risico's opleveren functioneren GW >> OvJ moet beheerder systeem informeren en informatie verstrekken t.b.v. verwijdering sporen.

Als software in GW blijft wordt vanuit server politie dataverkeer stopgezet zodat de politie geen gegevens meer ontvangt.

Opsporingsinstanties hebben zelf geen belang bij aanwezig blijven software vanwege risico ontdekking + afbreukrisico opsporingsonderzoek en vernrietiging bewijsmateriaal door verdachte.

Vraag: Waarom wilt u geen onafhankelijk toezicht op de uitvoering van de hackbevoegdheid?

Antwoord: Dergelijk toezicht reeds in wet voorzien. Inspectie Veiligheid en Justitie (VenJ) is als rijksinspectie belast met toezicht op kwaliteit taakuitvoering door de politie.

De Inspectie VenJ is rijksinspectie >> ruimte om zelf informatie te verzamelen, oordeel te vormen en te adviseren. Onafhankelijke oordeelsvorming.

Inspecteurs beschikken over de wettelijke bevoegdheden toezicht o.g.v. de Awb.

Toezicht Inspectie gericht op functioneren van wettelijke systeem rond onderzoek in GW >> systeemtoezicht. Kader gevormd door grenzen bevel OvJ en de machtiging RC. Oordeelsvorming OvJ en RC valt hierbuiten.

Toezicht op aspecten als autorisaties bevoegde opsporingsambtenaren voor uitvoering bevel OvJ, expertise en kennis opsporingsambtenaren, inzet van TH (kwaliteit en betrouwbaarheid), kwaliteit logging, beveiliging vastgelegde gegevens en verder gebruik verzamelde gegevens, inclusief de bewaring en vernietiging.

Inspectie stelt jaarlijks rapport op waarin verslag van toezicht op de uitvoering bevoegdheid. Verslag wordt openbaar gemaakt.

Vraag: Voldoet dit wetsvoorstel wel aan de eisen van het EVRM?

Antwoord: EVRM >> recht eerbiediging persoonlijke levenssfeer (artikel 8 EVRM).

Geen absoluut recht maar afgewogen tegen andere maatschappelijk zwaarwegende belangen. Geen inmenging toegestaan dan voor zover bij wet voorzien en in democratische samenleving noodzakelijk in belang van o.a. nationale veiligheid of voorkomen strafbare feiten.

Inmenging bij wet voorzien >> wettelijke regeling voor burger voldoende kenbaar + voorzienbaar.

Jurisprudentie EHRM >> wettelijke regeling voldoende toegankelijk moet zijn + voldoende precies zodat voldoende indicatie omstandigheden waarin en voorwaarden waaronder overheid tot inmenging mag overgaan.

Jurisprudentie EHRM >> inmenging door openbaar gezag voldoet aan noodzakelijkheid en evenredigheid, dient specifieke, expliciete en legitieme doeleinden, vindt op adequate en relevante wijze plaats, en niet buitensporig in verhouding tot doel inmenging.

Voorgestelde bevoegdheid wordt bij wet vastgelegd >> daarbij vastgelegd omstandigheden waarin + voorwaarden waaronder. Gaat om opsporing ernstige strafbare feiten >> erkend als belang dat inmenging openbaar gezag in recht op bescherming persoonlijke levenssfeer kan rechtvaardigen.

Regeling in WSv voor burger voldoende toegankelijk. Regeling beschrijft nauwkeurig in welke omstandigheden + onder welke voorwaarden toegepast. Onderzoekshandelingen nauwkeurig omschreven + sluiten merendeels aan bij bestaande

bevoegdheden in WSv. Vereiste van voorafgaande rechterlijke toetsing >> geen risico willekeurige toepassing door overheidsorgaan.

Aan noodzakelijkheidscriterium voldaan >> bevoegdheid onvermijdelijk is om ontwikkeling cybercrime het hoofd te bieden >> versleuteling van gegevens en opslag van gegevens in de cloud. Inzet traditionele opsporingsbevoegdheden is dan zinloos.

Aan evenredigheidsbeginsel invulling gegeven door beperking tot in de wet vastgelegde onderzoekshandelingen >> sluiten merendeels aan bij bestaande bevoegdheden in WSV. Uitsluitend gegevens vastleggen die nodig zijn voor opsporing betreffende ernstige strafbare feit. Verplichting tot logging t.b.v. controle achteraf.

V.w.b. proportionaliteit en subsidiariteit >> alleen toepassen als met bestaande bevoegdheden doel niet kan worden bereikt >> vereiste van het dringende onderzoeksbelang.

Regering ziet geen reden waarom voorgestelde regeling niet voldoet aan de vereisten op het gebied van de bescherming van de persoonlijke levenssfeer, zoals die voortvloeien uit artikel 8 EVRM.

Vraag: Wat vindt u er van dat de FBI wil dat Apple een achterdeur inbouwt wil in de iPhone waardoor de FBI zich toegang kan verschaffen tot de iPhone van een vereende terrorist. Gaat de Nederlandse regering dat ook doen?

Antwoord: Nederlandse wetgeving voorziet in verplichting voor anderen dan verdachte tot beschikbaar stellen van kennis omtrent beveiliging GW of versleuteling gegevens (art. 125k, 126m, zesde lid, en 126nh Sv).

Verplichting strekt niet zover dat aanbieder van product of dienst kwetsbaarheden moet inbouwen t.b.v. mogelijk gebruik door politie en justitie.

Kabinetsstandpunt over encryptie >> onderstreept noodzaak rechtmatige toegang tot gegevens en communicatie in het licht van waarborgen veiligheid en opsporing strafbare feiten.

Tegelijkertijd onderschrijven belang sterke encryptie voor veilig internet + bescherming privacy burgers + belang Nederlandse economie.

Op dit moment geen aanvullende beperkende t.a.v. ontwikkeling, beschikbaarheid en gebruik encryptie in Nederland.

Vraag: Klopt het nu dat als bekend is dat een geautomatiseerd systeem in het buitenland staat, dat dan een rechtshulpverzoek zal worden gedaan om de gegevens te verkrijgen?

Antwoord: Ja, als bekend GW of gegevens op grondgebied een andere staat >> zo snel mogelijk rechtshulpverzoek.

In afwachting reactie niet uitgesloten verrichten bepaalde onderzoekshandelingen >> afhankelijk aard en ernst strafbare feiten, te verrichten onderzoekshandelingen en aard rechtshulprelatie. Intensiteit rechtshulprelatie weegt ook mee >>bij staat waarmee NL intensieve relatie onderhoudt andere afweging dan bij staat die bekend staat als notoire «safe haven» voor criminaliteit.

Voorbeeld DDOS-aanval op kritische Nederlandse infrastructuur >> online afhandeling betalingsverkeer onmogelijk of militaire installaties belemmerd >> mogelijk dringende noodzaak binnendringen server en ontoegankelijkmaken bepaalde gegevens ter beeindiging DDOS-aanval.

Voorbeeld terroristische dreiging >> binnendringen in GW t.b.v. aftappen telecommunicatie of overnemen gegevens om aanslag te voorkomen en daders te achterhalen.

Als betrokken staat daarom vraagt wordt altijd verantwoording over het handelen + de daarbij gemaakte afwegingen.

Vraag: Staat eigenmachtig optreden niet haaks op de internationale oriëntatie van Nederland? Doen andere landen dit ook?

Antwoord: Rapport Transborder Group Raad van Europa >> opsporingsdiensten van veel staten verschaffen zich toegang tot gegevens op grondgebied andere staten t.b.v. veilig stellen elektronisch bewijs >> inbreuk op soevereiniteit van die staten.

Regering acht internationale samenwerking van belang om te komen tot gemeenschappelijk optreden bij aanpak grensoverschrijdende computercriminaliteit.

Als Voorzitter Europese Unie heeft NL dit onderwerp geagendeerd. Daarnaast actief deelnemen aan het overleg in het kader van de Cybercrime Conventie van de Raad van Europa.

Ontwikkeling gemeenschappelijk internationaal optreden pas op langere termijn te realiseren. In afwachting daarvan zal, als rechtshulpverzoek geen uitkomst biedt, keuze tussen twee minder ideale situaties >> afzien van verrichten opsporingshandelingen wanneer niet bekend waar gegevens zich bevinden of in uitzonderlijke gevallen het onder voorwaarden zelfstandig uitoefenen van uitvoerende rechtsmacht.

Vanwege dringende belangen die in geding zijn kiest regering voor laatste optie, waarbij zo zorgvuldig mogelijk wordt gehandeld en, zodra bekend is dat een geautomatiseerd werk zich in andere staat bevindt, zo snel mogelijk een verzoek tot rechtshulp volgt.

Vraag: Het toezicht door de Inspectie VenJ is niet onafhankelijk. Waarom wilt u geen onafhankelijk toezicht, zoals door de CTIVD?

Antwoord: Specifieke situatie in opsporing voor ogen houden. OvJ gezag over opsporing strafbare feiten. Die taak omvat toezicht op opereren van politie.

In een concrete strafzaak controle door de rechter. Zittingsrechter + de RC. Machtiging RC vereist voor binnendringen GW.

Inspectie VenJ systeemtoezicht op taakuitvoering politie.

Autoriteit Persoonsgegevens toezicht op naleving privacywetgeving + zorgvuldige verwerking persoonsgegevens.

Oprichting nieuw orgaan voor toezicht op onderzoek in GW >> enorme drukte op gebied toezicht politie.

Klemt temeer omdat toezicht door dergelijk orgaan snel raakt aan oordeelsvorming OvJ en rechter. OvJ is magistraat, wiens handelen wordt gecontroleerd door rechter. De rechter zelf is onafhankelijk. Toezicht op rechterlijke oordeelsvorming door andere onafhankelijke instantie niet wenselijk.

Bij IenV-diensten andere situatie >> in beginsel geen toesging door onafhankelijke rechter. M.u.v. enkele specifieke bevoegdheden is handelen van de diensten afhankelijk van instemming van Minister van BZK. In dat systeem past afzonderlijk toezichthoudend orgaan zoals CTIVD.

Vraag: Wat zijn de extra kosten voor de Inspectie en hoe wordt dit gedekt?

Antwoord:

Uit onderzoek van de Inspectie (overleg met CTIVD + landelijk project computercriminaliteit nationale politie) blijkt dat het toezicht arbeidsintensief is en veel kennis vergt. Dit betreft met name juridische kennis (bijv. kennis van de privacywetgeving), technische kennis (bijv. kennis van de benodigde werkmethodieken en informatiebeveiliging) en organisatorische kennis.

Om dit toezicht binnen de Inspectie Veiligheid en Justitie structureel vorm te geven zijn ten minste 4 fte'n noodzakelijk. De structurele kosten daarvan worden geraamd op €400.000 per jaar. Op termijn kan verhoging noodzakelijk zijn, als de bevoegdheid meer frequent wordt toegepast.

5. PARLEMENTAIRE STUKKEN 34 372 (+ 26 643)

Onderwerp : Overnemen en helen van gegevens (1)

Kamerlid :

Vraag: Is strafbaarstelling van het overnemen van niet-openbare gegevens wel proportioneel?

Antwoord:

- Met het overnemen van niet-openbare gegevens kan ernstig inbreuk worden gemaakt op de belangen van de slachtoffers.
- Het gaat hier om gedrag als het kopiëren van gegevens door een werknemer waartoe hij in zijn functie toegang heeft of misbruik van creditcardgegevens.
- Ook kan worden gedacht aan vormen van «wraakporno», waarbij seksueel beeldmateriaal wordt ontvreemd en op internet wordt gepubliceerd.
- Gelet op de risico’s voor de slachtoffers zie ik niet in waarom de voorgestelde strafbaarstelling niet proportioneel zou zijn.

Onderwerp : Overnemen en helen van gegevens (2)

Kamerlid :

Vraag: Hoe wordt getoetst of iemand te goeder trouw handelde bij het overnemen van gegevens?

Antwoord:

- Het overnemen van gegevens is alleen strafbaar voor zover dit wederrechtelijk plaatsvindt.
- Van wederrechtelijkheid is geen sprake als het algemeen belang het handelen vereiste.
- Met de term algemeen belang wordt volgens het spraakgebruik geduid op datgene dat voor de samen-leving als geheel van betekenis is en het belang van een individu of van een groep van personen overstijgt.
- Het is aan de rechter om te beoordelen in een concreet geval sprake is van een algemeen belang
- Of iemand te goeder trouw handelde wordt eveneens getoetst wanneer de rechter in een concreet geval oordeelt over de strafbaarheid van de gedraging van de vervolgde persoon.

Onderwerp : Overnemen en helen van gegevens (3)

Kamerlid :

Vraag: Hoe beoordeelt u de zorg dat de strafbaarstelling van het overnemen en helen van gegevens tot gevolg heeft dat klokkenluiders en journalisten bepaalde informatie niet zullen durven delen?

Antwoord:

- Gerechtvaardigde activiteiten van journalisten en klokkenluiders, of van degenen die hen daarbij faciliteren zijn niet strafbaar.
- Het wetsvoorstel bevat een strafuitsluitingsgrond: niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het verwerven, voorhanden hebben, ter beschikkingstellen, bekendmaken of gebruik van de gegevens vereiste.
- Het recht op een vrije nieuwsgaring kan worden aangemerkt als een algemeen belang.
- Ditzelfde geldt voor het recht op de vrijheid van meningsuiting, dat ook grondwettelijk verankerd is.
- Of journalisten en klokkenluiders in een concreet geval een beroep kunnen doen op omstandigheden als het algemeen belang of de goede trouw is aan de rechter om te beoordelen.

Eventueel(bij doorvragen over jurisprudentie):

- Bij de voorgestelde strafbaarstelling van de heling van gegevens zijn conflicterende belangen aan de orde.
- Enerzijds het belang van de rechthebbende op bescherming tegen onbevoegd gebruik van gegevens door derden die door misdrijf zijn verkregen; anderzijds het maatschappelijke belang dat misstanden vrijelijk kunnen worden geopenbaard door journalisten of klokkenluiders zonder dat het risico bestaat op strafvervolging.

- Als hoofdregels gelden in de jurisprudentie dat sprake moet zijn van een «serieuze» misstand en dat de wijze van melden in verhouding behoort te staan tot de ernst van de misstand.
- Het binnendringen in een geautomatiseerd werk, het raadplegen van medische dossiers, en het uitprinten van gegevens door een journalist zijn door de rechter niet wederrechtelijk geoordeeld in het licht van het hogere belang dat daarmee gediend was, namelijk het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens.
- De rechter oordeelde dat deze handelwijze een wezenlijk maatschappelijk belang kon dienen.

Onderwerp : Overnemen en helen gegevens (4)

Kamerlid :

Vraag: Wat gebeurt er als gegevens worden gebruikt die onvoldoende beveiligd zijn, waardoor als niet-openbaar bedoelde informatie feitelijk wel toegankelijk is?

Antwoord:

- Gegevens zijn niet openbaar als ze op zodanige wijze zijn opgeslagen dat daaruit kan blijken dat de rechthebbende niet de intentie had de gegevens voor het publiek beschikbaar te stellen.
- Dat de informatie niet of niet voldoende is beveiligd tegen de intenties van kwaadwillenden doet daaraan niet af.
- Een voorbeeld is een afbeelding die is opgeslagen op een mailserver in de cloud.
- Als een derde beschikking krijgt over die gegevens door zich toegang te verschaffen tot de mailbox, dan verandert daardoor niet het karakter van de betreffende afbeelding.
- Uit het feit dat die afbeelding is opgeslagen in een mailbox die niet voor anderen dan de rechthebbende(n) op de betreffende mailbox toegankelijk is, volgt dat het hier gaat om gegevens die niet voor het publiek beschikbaar en daarmee niet openbaar zijn.

Onderwerp : Overnemen en helen van gegevens (5)

Kamerlid :

Vraag:
Waarom wordt het soort gegevens dat uit een geautomatiseerd niet nader beperkt in de strafbaarstellingen?

Antwoord:

- Het wetsvoorstel maakt geen onderscheid in het soort gegevens dat uit een geautomatiseerd werk wordt ontvreemd.
- Ik ben geen voorstander van nadere beperking.
- In de eerste plaats omdat aan het wederrechtelijk verkrijgen en via het internet breed verspreiden van gegevens in zijn algemeenheid grote risico’s zijn verbonden voor slachtoffers.
- Ten tweede omdat het niet goed mogelijk is om een criterium vast te stellen dat voldoende onderscheidend is.

Onderwerp : Overnemen en helen (6)

Kamerlid :

Vraag:
Hoe kunnen de strafbaarstellingen van het overnemen en helen van gegevens bijdragen aan de aanpak van "wraakporno"?

Antwoord:

- Wraakporno is gedrag waarbij seksueel beeldmateriaal wordt vergaard waarmee de afgebeelde vervolgens wordt afgeperst of zwartgemaakt, waarbij het motief is het uiten van frustratie, bijvoorbeeld na een verbroken relatie.
- Hoewel er op dit moment al voldoende mogelijkheden zijn - onder andere op grond van de zedendelicten en de uitingsdelicten, zoals belediging en smaad, en de Auteurswet - om op te treden tegen het ongewenst verspreiden van seksueel beeldmateriaal, kan het wetsvoorstel de aanpak hiervan nog wel verbeteren.
- Degene die rechtmatige toegang heeft tot vertrouwelijke gegevens, zoals seksueel beeldmateriaal op een computer en deze gegevens voor zichzelf of een ander kopieert, is nu niet strafbaar. Een rechthebbende heeft dan echter geen invloed op het gebruik dat van het seksueel beeldmateriaal wordt gemaakt, waardoor hij benadeeld kan worden.
- Strafrechtelijke vervolging wegens heling van seksueel beeldmateriaal dat door een misdrijf is verkregen is evenmin mogelijk.
- Na inwerkingtreding van het wetsvoorstel zijn dit wel strafbare gedragingen.

(Eventueel, wanneer gevraagd wordt om specifieke strafbaarstelling):

- Een specifieke strafbaarstelling van “wraakporno” is niet nodig en wordt niet voorzien.
- In de “zedenbrief” van 29 februari 2016 aan de Tweede Kamer heeft de minister van Veiligheid en Justitie aangekondigd dat in het kader van de modernisering van de zedentitel de mogelijkheid wordt onderzocht of seksuele afpersing met een seksueel motief strafbaar gesteld kan worden als zedendelict.
- Wanneer het motief van de afpersing echter gelegen is in het uiten van frustratie dan wel het schaden in de eer en goede naam, zoals bij wraakporno, biedt de bestaande wetgeving voldoende - al dan niet strafrechtelijke - bescherming.

Onderwerp : Overnemen en helen gegevens (8)

Kamerlid :

Vraag:
Wordt met dit wetsvoorstel de toezegging gestand gedaan om sexting/wraakporno wettelijk te bestrijden (Kamerstukken II 2014/15, 28 684, nr. 443)?

Antwoord:

- In de brief van 12 juni 2015 aan Uw Kamer, is toegezegd dat in het wetsvoorstel Computercriminaliteit III nieuwe strafbaarstellingen geïntroduceerd zouden worden op grond waarvan het strafbaar wordt om vertrouwelijke gegevens van personen, zoals seksueel getint beeldmateriaal, te kopiëren of gegevens die door misdrijf zijn verkregen voorhanden te hebben of bekend te maken.
- Deze strafbaarstellingen zijn in het wetsvoorstel opgenomen, het betreft de voorgestelde de artikelen 138c en 139g van het Wetboek van Strafrecht.

Onderwerp : Grooming (1)

Kamerlid :

Vraag:
Hoe wordt voorkomen dat grooming niet bewezen kan worden omdat sprake is van uitlokking?

Antwoord:

- De inzet van "lokmiddelen" bij de opsporing van online seksueel misbruik is in beginsel mogelijk.
- Opsporingsambtenaren zijn volgens rechtspraak van de Hoge Raad op basis van algemene taakstellende bepalingen de artikelen 3 Politiewet 2012 en 141 van het Wetboek van Strafvordering onder voorwaarden bevoegd tot het inzetten van lokmiddelen.
- De grens wordt gevormd door artikel 6 EVRM, dat het recht op een eerlijk proces waarborgt.
- Als iemand door het gebruik van lokmiddelen is bewogen tot andere handelingen dan waarop zijn opzet reeds is gericht - dit wordt ook wel aangeduid als het Tallon-criterium van de Hoge Raad - is er sprake van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs.
- Om te voorkomen dat sprake is van uitlokking zal de opsporingsambtenaar die als lokpuber fungeert zich passief opstellen en wachten tot iemand contact legt.

Onderwerp : Grooming (2)

Kamerlid :

Vraag: Zijn er omstandigheden denkbaar waarin de opsporingsambtenaar wel zelf contact legt?

Antwoord:

- Het is niet bij voorbaat uitgesloten dat de opsporingsambtenaar de communicatie start; de opsporingsambtenaar zal een profiel moeten aanmaken zodat de groomer in staat is contact te leggen.
- De opsporingsambtenaar zal zich daarbij zodanig opstellen dat de verdachte niet wordt gebracht tot andere handelingen dan waarop zijn opzet van tevoren was gericht.

Onderwerp : Grooming (3)

Kamerlid :

Vraag:
Aan welke voorwaarden dienen profielfoto's die gebruikt worden door lokpubers te voldoen?

Antwoord:

- De opsporingsambtenaar die fungeert als lokpuber zal zich, om het verwijt van uitlokking te voorkomen, passief opstellen en afwachten totdat iemand contact met hem legt via internet.
- Het profiel dat door de opsporingsambtenaar wordt aangemaakt, zal een profiel zijn dat niet opvalt tussen andere profielen van deelnemers aan het sociale medium waarop de opsporingsambtenaar zich begeeft.
- Aangezien de deelnemers vaak jonge kinderen zijn, kan gedacht worden aan een foto van een dier of een plaatje van een stripfiguur.

Onderwerp : Grooming (4)

Kamerlid :

Vraag: Is het niet verstandig om alsnog in de wet vast te leggen wanneer een lokpuber mag worden ingezet?

Antwoord:

- Bij de huidige stand van de jurisprudentie wordt geen aanleiding gezien voor een nadere regeling over de inzet van de lokpuber.
- Die inzet vindt een toereikende grondslag in de algemene taakstellende bepalingen van opsporingsambtenaren - de artikelen 3 Politiewet en 141 van het Wetboek van Strafvordering - hetgeen bevestigd is in de rechtspraak.
- Wel zal, zoals ook in de contourennota modernisering Wetboek van Strafvordering tot uitdrukking is gebracht in het kader van de voorgenomen modernisering van het Wetboek van Strafvordering worden bezien of het Tallon-criterium als algemene bepaling voor het voorbereidend onderzoek in het wetboek kan worden gecodificeerd.

Onderwerp : Grooming (5)

Kamerlid :

Vraag:
Hoe staat u tegenover de inzet van virtuele kindcreaties - bijvoorbeeld het Sweetieproject van Terre des Hommes - bij de opsporing van online misbruik van kinderen?

Antwoord:

- Het Wetboek van Strafrecht staat op zichzelf niet in de weg aan de inzet van virtuele kindcreaties bij de opsporing van grooming.
- De inzet van virtuele kindcreaties is niet zozeer een materieelrechtelijke als wel een strafvorderlijke kwestie.
- Het OM kiest ervoor om bij de opsporing van online zedendelicten virtuele kindcreaties in te zetten, omdat hiermee al snel over de grens van geoorloofde uitlokking heen wordt gegaan.
- Het OM heeft hiertoe besloten na ervaringen met het Sweetieproject van Terre des Hommes.
- Het OM heeft zo'n 20 zaken aangeleverd gekregen van Terre des Hommes en heeft deze zaken allemaal onderzocht.
- In geen van de zaken kon vervolging worden ingesteld, omdat telkens sprake was van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs.
- Voor zover in de toekomst in de opsporingspraktijk gebruik gemaakt gaat worden van bewegende animaties zal de grens van geoorloofde uitlokking in acht moeten worden genomen.

Onderwerp : Grooming (6)

Kamerlid :

Vraag: Wat is het verschil tussen de inzet van een lokpuber en de inzet van een virtuele kindcreatie?

Antwoord:

- Een virtuele kindcreatie is een virtueel personage - een "avatar" - dat wordt gebruikt om in contact te komen met mensen die webcamseks willen met een minderjarig meisje.
- Een lokpuber is een rechercheur die zich online voordoet als kind onder de zestien jaar en daarbij een afwachtende houding aanneemt.
- Het Wetboek van Strafrecht staat - na inwerkingtreding van de in het wetsvoorstel voorgestelde wijzigingen - op zichzelf niet in de weg aan de inzet van lokmiddelen bij de opsporing van grooming.
- De inzet van lokmiddelen is vooral een strafvorderlijke kwestie.
- Het OM kiest ervoor om bij de opsporing van online zedendelicten virtuele kindcreaties in te zetten, omdat uit ervaringen met het Sweetieproject van Terre des Hommes is gebleken dat een geautomatiseerde gesprekspartner al snel over de grens van geoorloofde uitlokking heengaat.
- De inzet van een lokpuber is maatwerk: om te voorkomen dat sprake is van uitlokking zal de opsporingsambtenaar die als lokpuber fungeert zich passief opstellen, wachten tot iemand contact legt en tijdens die contacten behoedzaam te werk gaan.

Onderwerp : Grooming (7)

Kamerlid :

Vraag: Waarom is de inzet van de lokpuber nu niet mogelijk?

Antwoord:

- Op grond van huidige delictsomschrijvingen in de artikelen 248a van het Wetboek van Strafrecht dat verleiding van een minderjarige strafbaar stelt en 248e van het Wetboek van Strafrecht, dat grooming strafbaar stelt, is het materieelrechtelijk niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is.
- Het wetsvoorstel wijzigt deze artikelen op zodanige wijze dat het contact leggen met iemand die zich voordoet als een minderjarige alsnog strafbaar wordt.
- Hierdoor wordt de inzet van de lokpuber bij de opsporing van online grooming en verleiding van een minderjarige mogelijk.

Onderwerp : Grooming (8)

Kamerlid :

Vraag:
Waarom is de inzet van de lokpuber gerechtvaardigd? Zijn er geen alternatieven?

Antwoord:

- Door het stopzetten van de inzet van de lokpuber is de preventieve opsporing van grooming feitelijk onmogelijk geworden.
- Opsporing achteraf kan nog steeds plaatsvinden, op basis van meldingen of aangifte.
- Dit is echter geen aanvaardbaar alternatief voor de preventieve inzet van de lokpuber omdat het schadelijke contact met een minderjarige dan vaak al heeft plaatsgevonden, met alle gevolgen van dien.

Onderwerp : Grooming (9)

Kamerlid :

Vraag:
Werken politie en OM samen met organisaties als Terre des Hommes bij de bestrijding van seksueel misbruik van kinderen? Wat is de stand van zaken met betrekking tot het Sweetieproject?

Antwoord:

- Politie en OM werken samen met partners als Terre des Hommes om seksueel misbruik van kinderen aan te pakken.
- Het OM heeft uitgebreid gesproken met Terre des Hommes over de, vanuit strafvorderlijk perspectief, mislukte inzet van Sweetie.
- Afgesproken is dat een nieuw chatprogramma Sweetie 2.0 ontwikkeld zou worden door Terre des Hommes voor preventieve in doeleinden.
- Sweetie 2.0 is nog ontwikkeling, het OM onderhoudt hierover contact met Terre des Hommes.

Onderwerp : Grooming (10)

Kamerlid :

Vraag: Kan een minderjarige ook grooming plegen?

Antwoord:

- De strafbepaling stelt geen eisen aan de leeftijd van de dader. Ook minderjarige daders kunnen zich schuldig maken aan grooming.
- Voor een veroordeling voor grooming is nodig dat alle delictsbestanddelen bewezen kunnen worden.
- In artikel 248e van het Wetboek van Strafrecht, dat grooming strafbaar stelt, is een ontuchtbestanddeel opgenomen.
- Een dader moet het oogmerk hebben om ontuchtige handelingen te plegen.
- Dat betekent dat er sprake moet zijn van het oogmerk om gedragingen te plegen die in strijd zijn met de sociaal-ethische norm.
- Als een kind van zestien een kind van tien benadert, zal er doorgaans wel sprake zijn van een ontuchtig oogmerk.
- Bij vrijwillige contacten tussen leeftijdsgenoten, bijvoorbeeld twee vijftienjarigen, hoeft dit niet het geval te zijn.
- Indien er geen sprake is van handelingen met een strafbaar karakter blijft vervolging achterwege.

Onderwerp : Grooming (11)

Kamerlid :

Vraag: Is de strafbaarstelling van grooming geen intentiestrafrecht? Moet voor de strafbaarheid van grooming niet worden vereist dat de verdachte daadwerkelijk daad bij woord voegt?

Antwoord:

- Onder invloed van internationale regelgeving is de strafrechtelijke bescherming van kinderen uitgebreid tot de voorfase van fysiek misbruik.
- De strafbaarstelling van grooming, het benaderen van kinderen voor seksuele doeleinden, is een gevolg van het Verdrag van Lanzarote. Ook is dit gedrag strafbaar gesteld in de EU-richtlijn seksueel misbruik van kinderen uit 2011.
- Nederland is dus internationaal gezien verplicht om grooming strafbaar te stellen.
- Op grond van het Verdrag en de richtlijn dient de dader enige handeling te verrichten gericht op het verwezenlijken van een ontmoeting met een minderjarige.
- Niet wordt vereist dat daadwerkelijk een ontmoeting heeft plaatsgevonden.
- Als deze eis in de Nederlandse strafwet zou worden gesteld, zou Nederland in strijd handelen met de internationale verplichtingen.

Onderwerp : Grooming (12)

Kamerlid :

Vraag: Wat doet Nederland in internationaal verband om grooming/online misbruik van kinderen te bestrijden?

Antwoord:

Onderwerp : Grooming (13)

Kamerlid :

Vraag:
Wanneer kan het wetsvoorstel tot modernisering van de zedenwetgeving tegemoet worden gezien?

In hoeverre stelt het wetsvoorstel online misbruik van kinderen strafbaar?

Antwoord:

- Bij brief van 29 februari 2016 heeft de Minister van Veiligheid en Justitie het WODC-onderzoek «Herziening van de zedendelicten» voorzien van een beleidsreactie aan Uw Kamer toegezonden.
- Het WODC-onderzoek bevestigt dat de strafrechtelijke bescherming tegen zedenmisdrijven uit juridisch oogpunt in beginsel toereikend en in overeenstemming met de internationale wet- en regelgeving is.
- Tegelijkertijd toont het onderzoek aan dat de zedenwetgeving op onderdelen verduidelijkt en bij de tijd gebracht kan worden gebracht.
- Daarom is een wetgevingstraject gestart met als doel modernisering van de zedentitel.
- De strafrechtelijke bescherming tegen digitaal gepleegd misbruik krijgt een duidelijke plaats in de strafwet en wordt op onderdelen verruimd.
- Zo wordt het op verregaande en seksualiserende wijze met kinderen communiceren strafbaar gesteld.

- De Minister heeft eerder de verwachting uitgesproken in het najaar van 2016 een wetsvoorstel tot modernisering van de zedenwetgeving in consultatie te geven.
- De voorbereiding van het wetsvoorstel neemt iets meer tijd in beslag: waarschijnlijker is dat consultatie in het voorjaar 2017 kan plaatsvinden.

Van: 9
Verzonden: woensdag 7 december 2016 15:47
Aan: 9
Onderwerp: Fw: Dossier CC III
Bijlagen: CCIII.spreektekst.docx; CCIII.dossier02.02.16.docx; CCIII Q&A's overnemen+grooming.docx

Met vriendelijke groet,

9

Staf Korpsleiding Politie
Directie Operatien

Verzonden vanaf mijn Blackberry

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Van: 10.2.e
Verzonden: donderdag 8 december 2016 08:18
Aan: 10.2.e
Onderwerp: AFGEWEZEN CCIII - D66 verzoekt uitstel plenaire behandeling

Het verzoek is afgewezen, de plenaire behandeling van CCIII gaat komende week gewoon door

Van: 10.2.e
Verzonden: donderdag 8 december 2016 10:34
Aan: 10.2.e (Parket-Generaal) 10.2.e @om.nl); 10.2.e
Onderwerp: FW: Dossier CC III
Bijlagen: CCIII.spreektekst.docx; CCIII.dossier02.02.16.docx; CCIII Q&A's overnemen+grooming.docx

Graag even meelezen. Ze maken het vandaag af, dus kort deadline.

Groet.

10.2.e

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

Vanaf hier dubbel. Zie opm. inv.lst en docs 513, 514 en 515.

From: Plas, Theo van der (T.G.)
Sent: Friday, December 09, 2016 11:48 PM
To: 10.2.e
Subject: Antw: Interview KC Elsevier

Jaaaa. Ik schrijf net een mailtje aan 10.2.e over cc III, kijken of hij maandag wil of een ander opvatting heeft om toch in de media te willen gaan.

Groeten,theo

Van: 10.2.e BD/DRC/CV
Verzonden: vrijdag 9 december 2016 16:07
Aan: 10.2.e BD/DWJZ/SSR; 10.2.e - BD/DWJZ/SSR; 10.2.e BD/DRC/CV; 10.2.e (Parket-Generaal) 10.2.e @om.nl); 10.2.e (Landelijk Parket Rotterdam); 10.2.e @klpd.politie.nl)
Onderwerp: E-mail verzenden: Aanvullende spreektekst en QA kwetsbaarheden.docx

Beste collega's,

Ter commentaar bij deze enige aanvullende teksten over kwetsbaarheden.

Groet,

10.2.e

Aanvullend - spreektekst kwetsbaarheden

Samen met dit wetsvoorstel heeft de Kamer de brief over hoe we omgaan met kwetsbaarheden in hardware en software geagendeerd. Het gaat hierbij overigens om kwetsbaarheden waarmee het mogelijk is via het internet binnen te dringen in een geautomatiseerd werk. Het gaat niet om methoden die gebruikt worden om in beslag genomen telefoons of andere gegevensdragers uit te lezen. Dat valt in de wet onder het onderzoek aan in beslag genomen voorwerpen.

Laat ik voorop stellen dat ik het belangrijk vindt dat er zo min mogelijk kwetsbaarheden op het internet zijn. Kwetsbaarheden zijn niet goed voor de veiligheid van het internet, net zoals slechte sloten niet goed zijn voor de beveiliging tegen inbraak. Daarom heb ik de Kamer laten weten dat als we kwetsbaarheden aantreffen waarvan we denken dat ze nog niet bekend zijn, dat we die in beginsel altijd gaan melden aan de fabrikant van de hardware of software. Ook het binnendringen in een geautomatiseerd werk door de politie zal vrijwel altijd gebeuren met kwetsbaarheden die al bij fabrikanten bekend zijn.

Wel is het nodig dat we in bepaalde gevallen een uitzondering maken, en ik zal dat toelichten. Er zijn producten in omloop, zoals telefoons of softwarepakketten, die er speciaal op gericht zijn anoniem te communiceren. Soms zijn deze producten gemaakt met het oog op de privacy van de burger die niets

verkeerd doet. Maar we zien ook dat sommige van die producten vrijwel alleen gebruikt worden door criminelen. Ook zijn er producten die zelfs gemaakt worden door criminele organisaties. Het zou dan wat vreemd zijn dat we die criminelen gaan helpen om te zorgen dat wij ze niet kunnen opsporen.

Ook kan het vóórkomen dat een buitenlandse politiedienst een methode ontwikkelt om binnen te dringen, en die methode met ons deelt op voorwaarde dat we die niet bekend stellen. Dan moeten we daar in het belang van de opsporing aan kunnen voldoen.

Dan de afweging om een kwetsbaarheid niet te melden. In beginsel moet het gaan om uitstel van de melding, en niet om afstel. Vaak zal na afloop van een opsporingsonderzoek een onbekende kwetsbaarheid alsnog gemeld kunnen worden. Als een criminele organisatie de software heeft gemaakt, dan kan dat uitstel langer duren.

Dan moeten we vervolgens kijken wie de afweging kan maken om de melding van een onbekende kwetsbaarheid uit te stellen. Dat is wat mij betreft het College van Procureurs-Generaal. Zij kunnen inschatten of de kwetsbaarheid van belang is voor de opsporing. Als de software of hardware door veel mensen wordt gebruikt die niets hebben misdaan, dan wordt die gemeld.

Ik wil ver weg blijven van het beeld dat we onbekende kwetsbaarheden in gangbare producten niet zouden melden. Natuurlijk doen we dat wel. We gaan het niet geheim houden als er een veiligheidslek zit in Internet Explorer of in Firefox. We moeten juist de criminaliteit op internet tegengaan, dus die gaten willen we laten dichten.

Q: Geldt de regeling voor het melden van onbekende kwetsbaarheden ook voor onderzoek aan bijvoorbeeld in beslag genomen telefoons?

- Nee, het gaat alleen om kwetsbaarheden die kunnen worden gebruikt om via het internet een geautomatiseerd werk binnen te dringen, dus op afstand.
- Onderzoek aan in beslag genomen mobiele telefoons of andere apparaten valt onder het onderzoek aan in beslag genomen voorwerpen.
- Een kwetsbaarheid kan ook ontstaan door bijvoorbeeld een hardwarematige configuratie, en die kan dan gemeld worden.
- Het melden van kwetsbaarheden beoogt het internet veiliger te maken, niet de beveiliging van telefoons of andere gegevensdragers.

Q: Waarom wil de politie de mogelijkheid hebben om onbekende kwetsbaarheden niet te melden?
Q: Op basis van welke criteria wordt bepaald of de melding van een onbekende kwetsbaarheid wordt uitgesteld?

- Er kunnen diverse redenen zijn om een onbekende kwetsbaarheid nog niet te melden.
- Het belang van het onderzoek kan worden geschaad, omdat het onderzoek door de melding kan worden onderkend.
- De onbekende kwetsbaarheid is gevonden in een product dat voornamelijk door criminelen wordt gebruikt om onvindbaar te blijven. Een voorbeeld daarvan is een telefoon speciaal ontworpen om anoniem berichten te sturen voor hele hoge kosten.
- Ook kunnen er producten voor dat doel door criminelen of terroristen zijn gemaakt. Dan gaan we die criminelen of terroristen natuurlijk niet helpen de politie te ontlopen.
- Een ander voorbeeld is de situatie dat de kwetsbaarheid op voorwaarde van geheimhouding door een buitenlandse politiedienst aan de Nederlandse politie is gemeld in het kader van een opsporingsonderzoek. Als we een dergelijke kwetsbaarheid willen melden, dan zullen we eerst overleg plegen met die buitenlandse politiedienst.

Q: Kunt u voorbeelden noemen van producten waarvan u verwacht dat de melding van onbekende kwetsbaarheden in die producten wordt uitgesteld?

- Indien bijvoorbeeld een telefoon voor veel geld wordt verkocht, terwijl er alleen anoniem mee kan worden gebeld of berichten mee kunnen worden verzonden, dan is het mogelijk dat vooral criminelen dat geld er voor over hebben.
- Dat kan ook gelden voor dure softwareprogramma's of programma's die kunnen worden gebruikt voor criminele doeleinden.
- Een voorbeeld daarvan is het programma Blackshades, waarmee op afstand computers konden worden binnengedrongen. Dat programma werd via internet verkocht, door een anonieme verkoperm, en de kopers pleegden er strafbare feiten mee.

Q: Op welk moment wordt gekeken of een onbekende kwetsbaarheid aan de fabrikant kan worden gemeld?
Q: Hoe lang kan de melding worden uitgesteld? Zit hier een limiet aan?

- Op het moment dat deze wordt ontdekt, en dat de politie of de officier van justitie het aannemelijk vindt dat deze onbekend is, dan wordt een besluit genomen om te melden, of toestemming te vragen om hiermee te wachten.
- Er is geen termijn vastgesteld voor het melden van een onbekende kwetsbaarheid. Zodra dit redelijkerwijs mogelijk is zal de kwetsbaarheid worden gemeld of zal de officier van justitie het gewenste uitstel van de melding voorleggen.

Q: Wanneer is het aannemelijk dat een kwetsbaarheid nog onbekend is bij de fabrikant?

- Er zijn kwetsbaarheden die niet meer bestaan na bepaalde updates of nieuwe versies van een product. Daarvan kan worden aangenomen dat ze bekend zijn, omdat ze zijn verholpen.
- Daarnaast is veel informatie over kwetsbaarheden op internet toegankelijk en dan bij een breder publiek bekend. De politie mag er van uit gaan dat de producent deze informatie ook tot zich neemt.
- Het is niet de bedoeling dat de politie de opsporingscapaciteit inzet om te bezien of kwetsbaarheden wel of niet bekend zijn.

Q: Wie besluit er of een kwetsbaarheid wordt gemeld?
(OM-OPTIE)

- In beginsel wordt een onbekende kwetsbaarheid altijd gemeld aan de fabrikant van de software. Dat kan de politie of de officier van justitie besluiten.
- Alleen in uitzonderlijke gevallen kan de melding worden uitgesteld. Daarvoor is goedkeuring nodig van het College van Procureurs-Generaal van het Openbaar Ministerie. Voor dat besluit laat het College zich adviseren door de gespecialiseerde officieren van justitie van het Landelijk Parket, te weten de Landelijk Officier Cybercrime en de Landelijk Rechercheofficier die kijkt naar de noodzaak van bepaalde opsporingsmiddelen.
- Ook kunnen experts van buiten de opsporingsautoriteiten worden bevraagd, zoals het Nationaal Cyber Security Centrum van het Ministerie van V&J.

Q: De rechter-commissaris moet volgens het amendement-Recourt een machtiging geven voor het laten bestaan van een onveiligheid oor de samenleving. Dit heft weinig met een individuele strafzaak te maken. Ligt dit niet erg ver van de traditionele rol van de rechter-commissaris af?

(RC-OPTIE)

- De rechter-commissaris heeft nu vooral een zaaksgebonden rol. Het besluit om de melding van een kwetsbaarheid uit te stellen kan het belang van de individuele strafzaak overstijgen.
- Samen met de rechterlijke macht zal ik in overleg treden hoe aan deze nieuwe rol van de rechter-commissaris inhoud kan worden gegeven.
- Daarbij zal ik ook aandacht besteden aan de expertise van de rechter-commissaris en de mogelijkheden hem daarin te ondersteunen, bijvoorbeeld dor de inzet van technische experts.

Q: Wat is de rol van het NCSC? Zij zijn toch verantwoordelijk voor de veiligheid van het Nederlandse internet?

- Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland.
- Het NCSC vergroot de weerbaarheid van de samenleving in het digitale domein.
- De expertise van het NCSC kan worden benut voor een inschatting van het maatschappelijk risico van het uitstellen van een melding van een onbekende kwetsbaarheid.

Q: Hoe vaak gaat de politie een onbekende kwetsbaarheid tegenkomen?

- Dat is niet bekend, maar de verwachting is niet dat dit heel vaak zal gebeuren.
- Het uitgangspunt is dat als dit gebeurt, de onbekende kwetsbaarheid aan de fabriaknt wordt gemeld.
- Het is ook niet bekend welke nieuwe producten de komende jaren op de markt komen die het voor de opsporing lastig maken om bewijs te vergaren.
- Het voortschrijden van de techniek zorgt er voor dat steeds nieuwe producten op de markt komen, waarin oude kwetsbaarheden zijn verholpen en soms weer nieuwe kwetsbaarheden in zitten.

Q: Kunt u toezeggen dat de politie geen gebruik zal maken van kwetsbaarheden?

- Nee. Voor het binnendringen in een geautomatiseerd werk is vaak het gebruik van een kwetsbaarheid nodig.
- Het zal overigens vaak om een kwetsbaarheid gaan die bij de fabrikant al bekend is.

Q: Hoe vaak gaat de politie onbekende kwetsbaarheden gebruiken?

- Naar verwachting niet vaak.
- Ik hecht eraan te onderstrepen dat het niet melden van onbekende kwetsbaarheden een uitzonderingssituatie betreft.
- Het is de verwachting dat de politie vooral gebruik zal maken van bekende kwetsbaarheden.

Q: Vindt u het gebruik van kwetsbaarheden geen inbreuk op de privacy?

- Het uitstel van het melden van onbekende kwetsbaarheden betreft geen privacyinbreuk. Het betreft ook niet het gebruik van een opsporingsbevoegdheid. Door het niet melden ervan wordt de privacy door de politie niet aangetast.
- De afweging betreft eerder twee vormen van veiligheid. De politie heeft tot taak de veiligheid te vergroten door strafbare feiten op te sporen en de pakkans voor criminelen te verhogen. Aan de andere kant willen burgers en organisaties veilig het internet gebruiken. Daarvoor moeten we voorkómen dat criminelen gebruik kunnen maken van kwetsbaarheden.

Q: Wat doet u met de kwetsbaarheden die al gemeld zijn?

- Kwetsbaarheden die al zijn gemeld hoeven niet nogmaals te worden gemeld.
- Het is vervolgens de verantwoordelijkheid van de producent om de kwetsbaarheid te verhelpen.

Q: Geldt de regeling voor het uitstellen van het melden van kwetsbaarheden ook voor de I&V-diensten? Waarom niet?

- Nee. Voor de AIVD en de MIVD geldt een ander wettelijk kader, namelijk de Wet op de Inlichtingen- en Veiligheidsdiensten uit 2002.
- Volgens deze wet dragen het hoofd van de AIVD en de directeur van de MIVD zorg voor de geheimhouding van gegevens die daarvoor in aanmerking komen.
- Ik ben niet verantwoordelijk voor de diensten, dus ik kan geen uitspraak doen over de voorwaarden waaronder zij bepaalde gegevens bekend maken.

Q: Vindt u ook niet dat de schimmige markt voor onbekende kwetsbaarheden moet worden tegengegaan? Waarom stimuleert u deze markt dan?

- Het beperken van onderzoek naar kwetsbaarheden vind ik niet wenselijk. Kennis van kwetsbaarheden kan bijdragen aan de veiligheid van het internet.
- Wel is de verkoop van die kennis aan bepaalde partijen onwenselijk. Mensen die dergelijke kennis aan criminelen verkopen, zijn uiteraard niet goed bezig.
- Ook bij anonieme verkoop zouden mensen zich moeten realiseren dat die kennis in verkeerde handen kan vallen.
- De verkoop van intrusion software, die gebruik maakt van kwetsbaarheden, is in bepaalde omstandigheden onderhevig aan exportcontrole. De herziening van de dual use-verordening van de EU is op dit moment gaande.

Van: 10.2.e @politie.nl>
Datum: 9 december 2016 17:25:54 CET
Aan: Berg, Jannine van den (J.A.) 10.2.e @politie.nl>, 10.2.e f@politie.nl>,10.2.e t@politie.nl>, 10.2.e politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, Plas, Theo van der (T.G.) 10.2.e @politie.nl>, 10.2.e @politie.10.2.e @politie.nl>, 10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>
Onderwerp: Interview KC Elsevier

Collega's,

Service van de zaak.

Groet,
10.2.e

Van: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Datum: 9 december 2016 23:01:06 CET
Aan: 10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e politie.nl>, 10.2.e @politie.nl>
Onderwerp: Doorst: Interview KC Elsevier

Beste collega's, een mooi artikel in de Elsevier, waar we vanuit de portefeuille ook input voor hebben aangereikt. Een mooi statement en steun voor onze verdere activiteiten !

Groeten en fijn weekend,

Theo

Van: 10.2.e @politie.nl>
Datum: 9 december 2016 23:46:38 CET
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: Antw: Interview KC Elsevier

Ha, zelfs de kop gehaald..... Mooi!

Fijn weekend!

From "Plas, Theo van der (T.G.)"10.2.e @politie.nl>
Subject **Interview Elsevier en CC III**
To "Akerboom, Erik (10.2.e @politie.nl>, "Berg, Jannine van den (J.A.)"
10.2.e @politie.nl>
Date 10 december 2016 0:04:34 CET

Hallo Erik,
Complimenten voor het interview in Elsevier. Een mooi en sterk statement, dat door het korps en door de portefeuille Digitalisering en Cybercrime zeker wordt gewaardeerd en zal helpen in de verdere ontwikkeling. Ook het noemen van een onderzoek als 26koper zorgt voor een andere beeldvorming; een andere, eigentijdse politie.

Dinsdag staat de behandeling van CC III op de agenda. In overleg met Jannine heb ik de voorbereiding in gang gezet, om dinsdag een reactie klaar te hebben staan op het wel of niet aannemen van het wetsvoorstel. In het voortraject hebben we afgewogen om - net als eerder de AIVD deed - in de media onze behoefte nog eens te benadrukken. Daar hebben we tot nog toe van af gezien, omdat het er in de politiek nu even om spant en om V en J niet in de wielen te rijden.
Ik begreep van communicatie (10.2.e dat je overweegt om voor dinsdag extern over CC III te communiceren. Kunnen we daarover even overleg hebben, zodat je onze overwegingen daarin kunt betrekken ?
Groeten en fijn weekend, Theo

Van: 10.2.e
Verzonden op: zaterdag 10 december 2016 11:40
Aan: "Plas, Theo van der (T.G.)"
Onderwerp: Re: Antw: Interview KC Elsevier

Hallo Theo,

Ik heb 10.2.e dus gesproken. Het was volgens mij haar idee dat ze even kort tegen Erik aan heeft gehouden. Die had aangegeven er niet tegen te zijn maar dit zelf niet te willen doen. En vroeg zich ook af of Pfh dat moest doen. Ik heb haar aangegeven dat:

12-14

Voor je overleg met erik:
Het gaat dus om een amendement van de pvda voor een onafhankelijke toets op een eventueel besluit van OM om 0-days niet te melden.
Voorstel om besluit bij college PG's te leggen met rol CTC en advies NCTV op maatschappelijk effect blijkt niet voldoende. Wordt nu misschien belegd bij RC....
Is nog niet opgelost volgens mijn laatste info.

Had jij 10.2.e nog gesproken?

Met vriendelijke groet,

10.2.e
Staf Korpsleiding Politie
Directie Operatien
Verzonden vanaf mijn Blackberry

Van: Plas, Theo van der (T.G.)
Verzonden: zondag 11 december 2016 16:34
Aan: 10.2.e (E.K.)
Onderwerp: Antw: Re: Antw: Interview KC Elsevier

thanks, ff lezen. ps morgenmiddag zie ik een afspraak met 10.2.e in mijn agenda. ik zal ahv de besteding kijken hoe het er voor staat en vast aangeven waar verbetering moet. als je punten hebt voor het gesprek, of even bellen tevoren? gr theo.

Van: 10.2.e
Verzonden: zondag 11 december 2016 17:43
Aan: 10.2.e BD/DRC/CV'
CC: 10.2.e - BD/DGPOL/PBT/PT'; 10.2.e ; 10.2.e (Landelijk Parket Rotterdam); 10.2.e (Parket-Generaal) 10.2.e @om.nl); 10.2.e BD/DRC/CV; 10.2.e
Onderwerp: FW: E-mail verzenden: Aanvullende spreektekst en QA kwetsbaarheden.docx
Bijlagen: Aanvullende spreektekst en QA kwetsbaarheden.docx

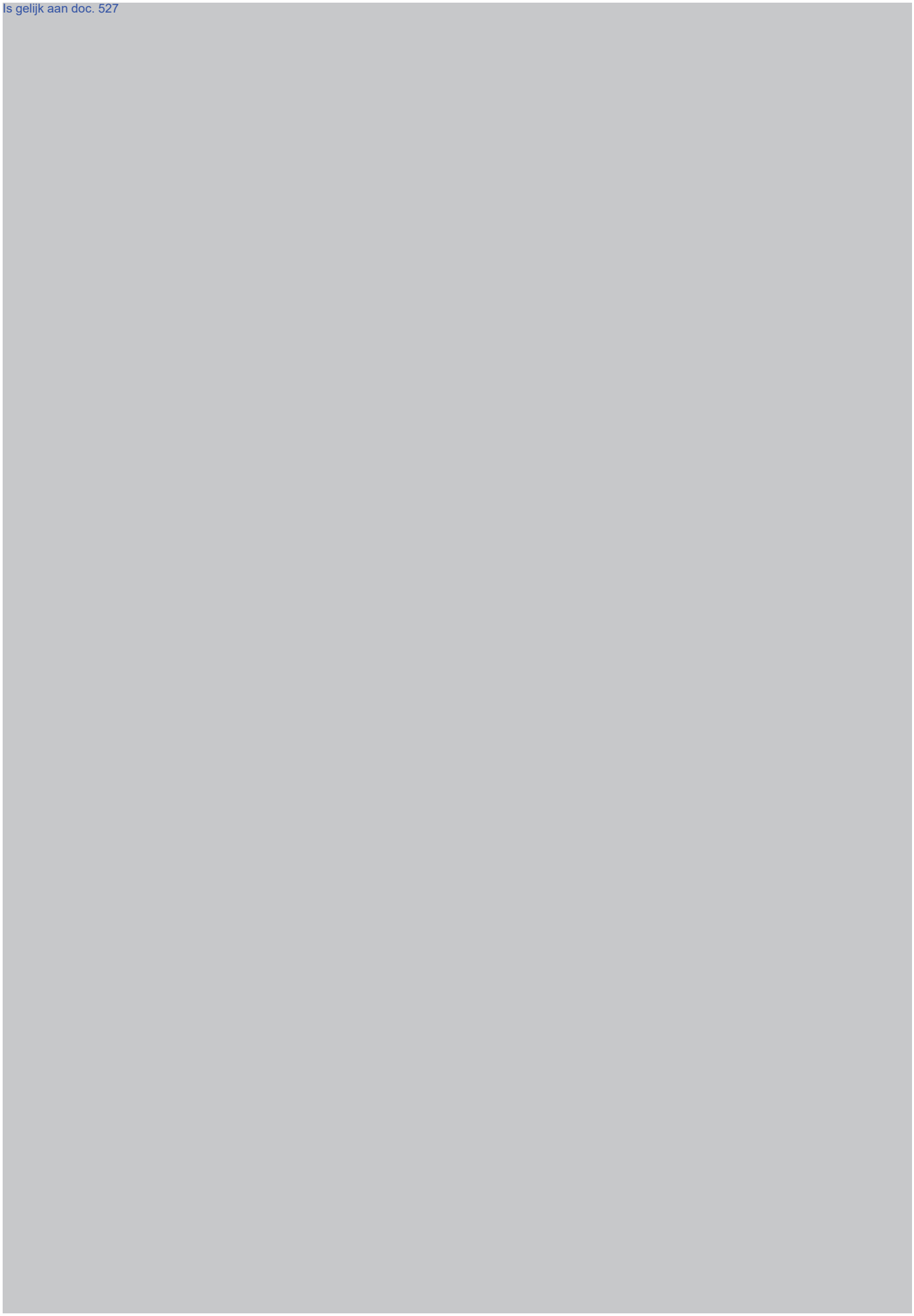
Hallo collega's,

Hierbij een paar opmerkingen over de teksten.

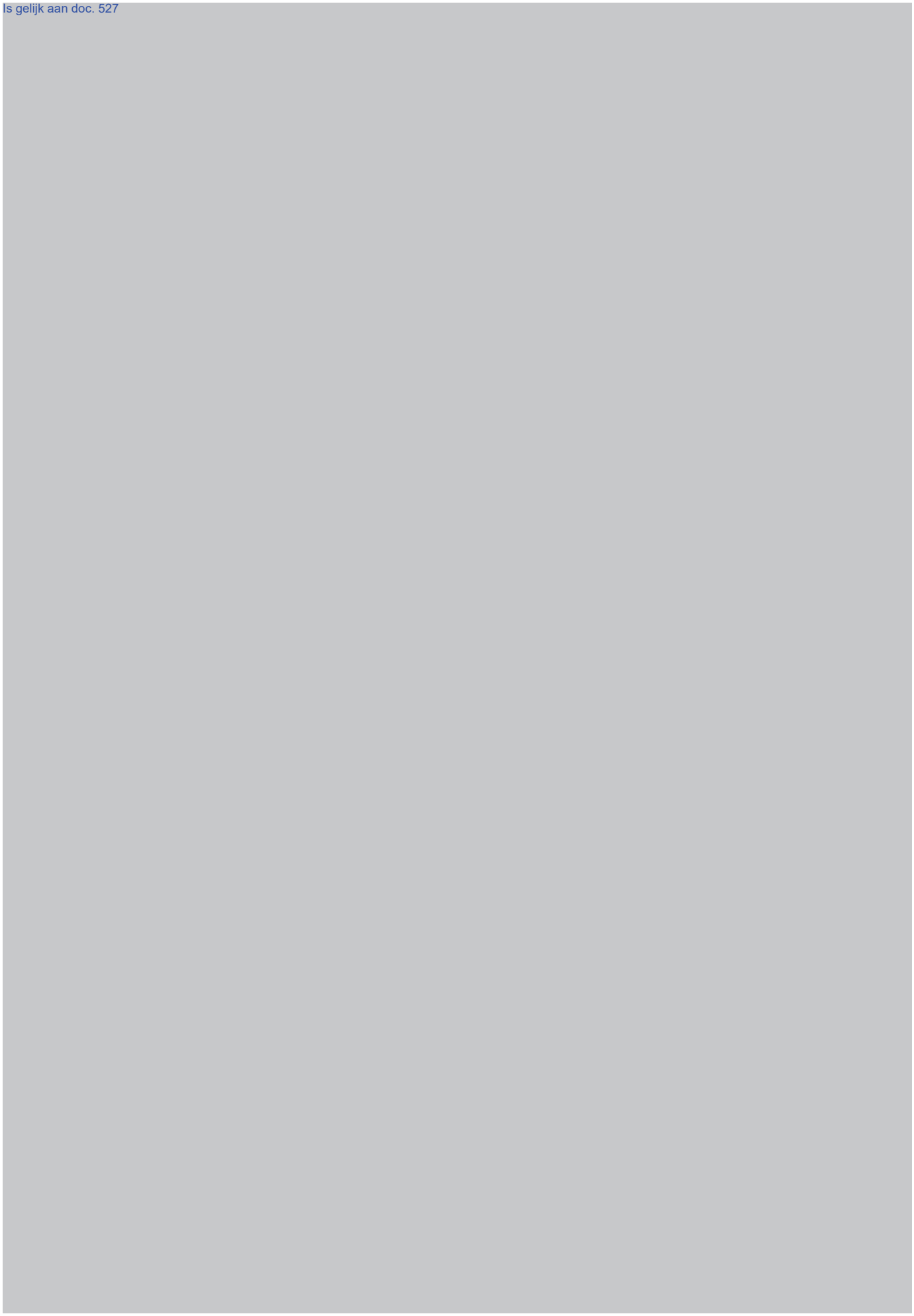
Groet,

10.2.e

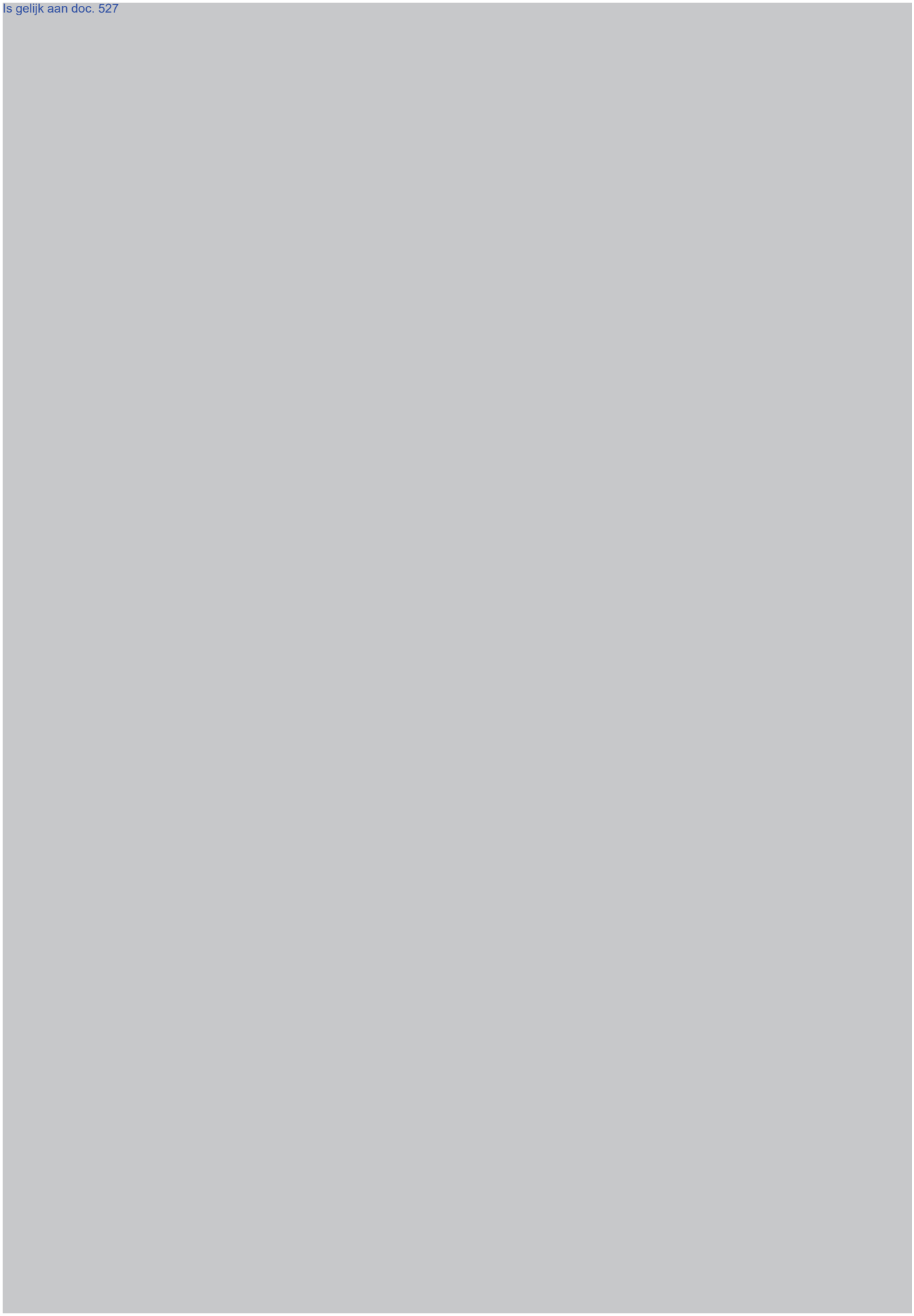
Is gelijk aan doc. 527



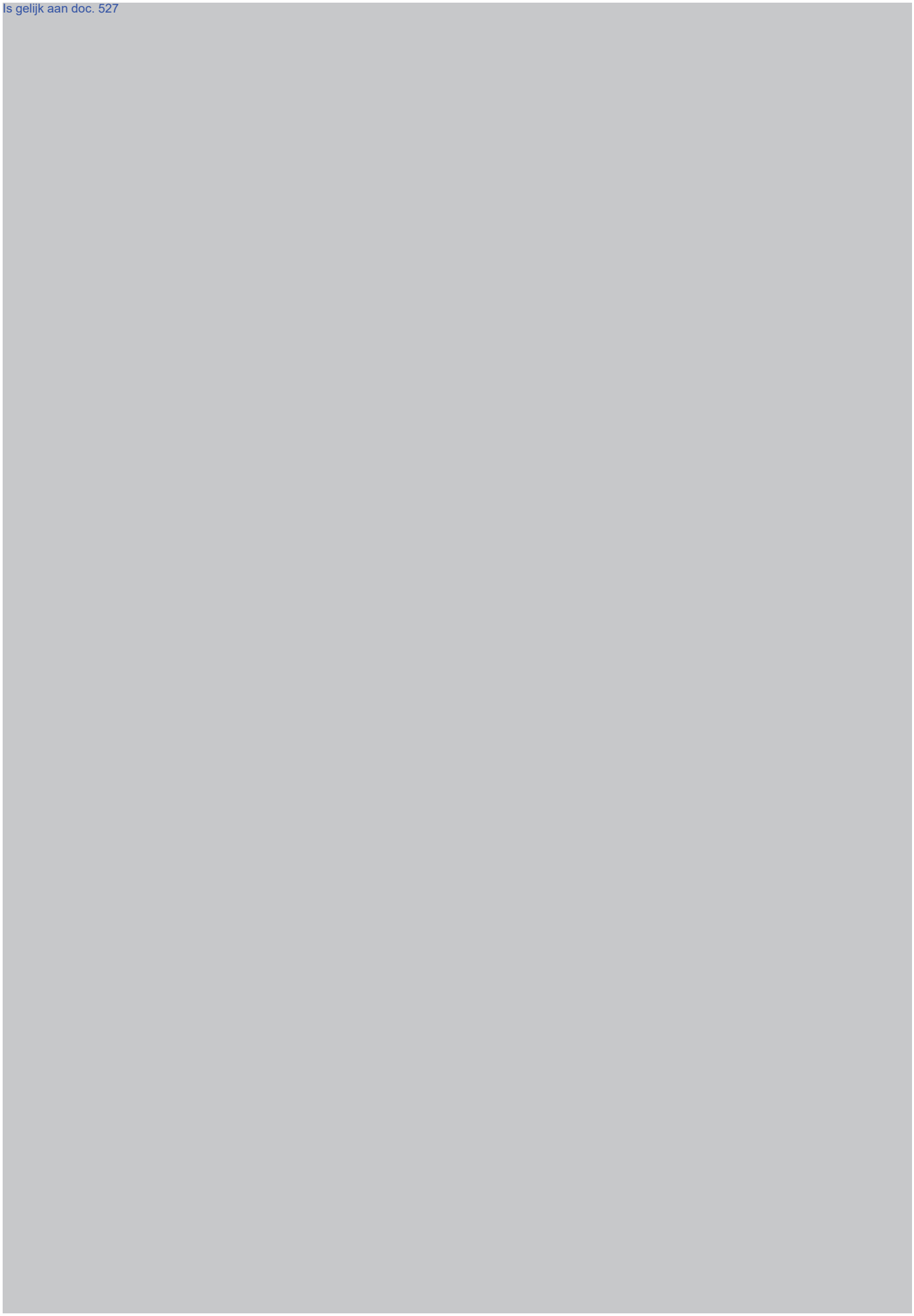
Is gelijk aan doc. 527



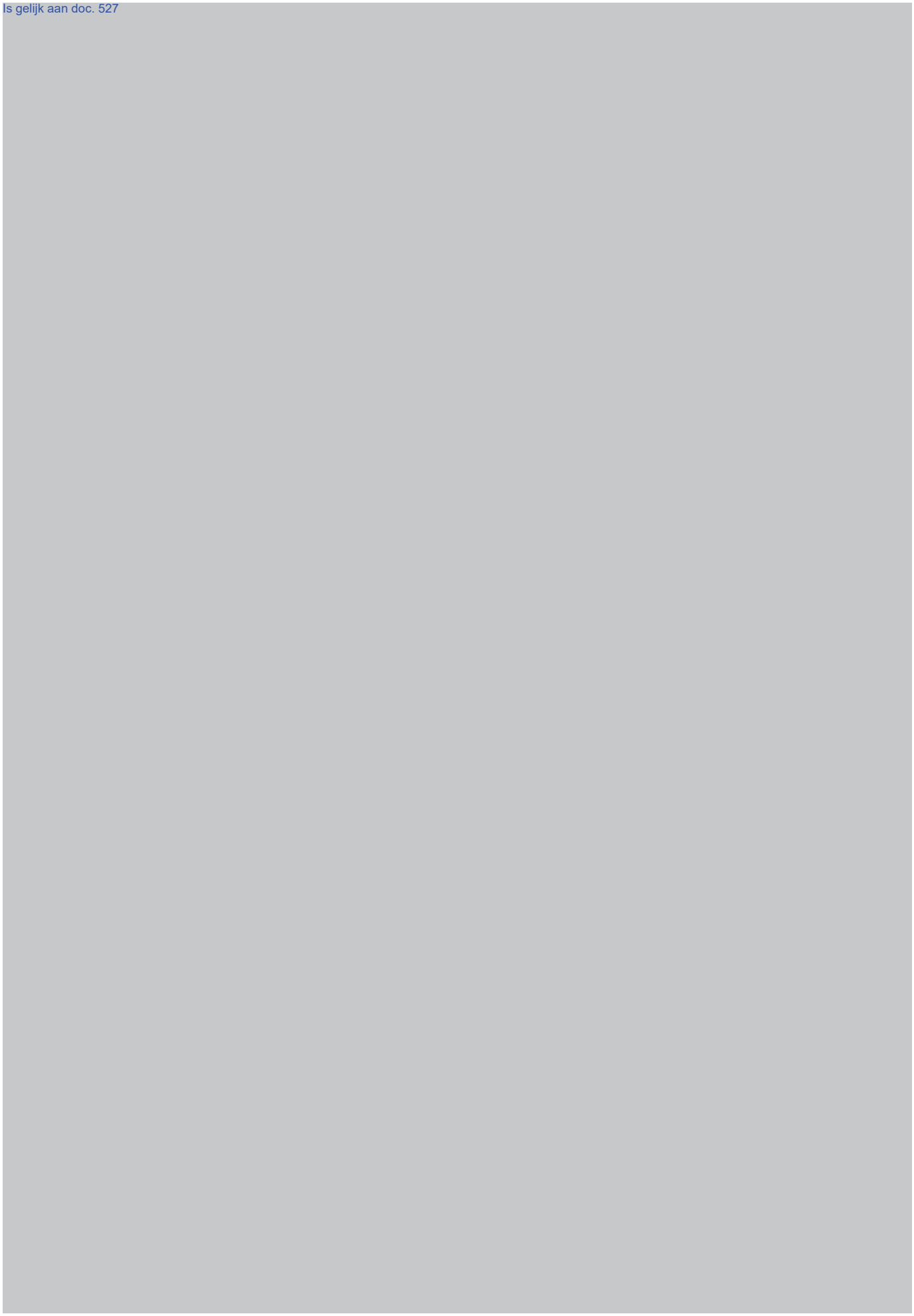
Is gelijk aan doc. 527



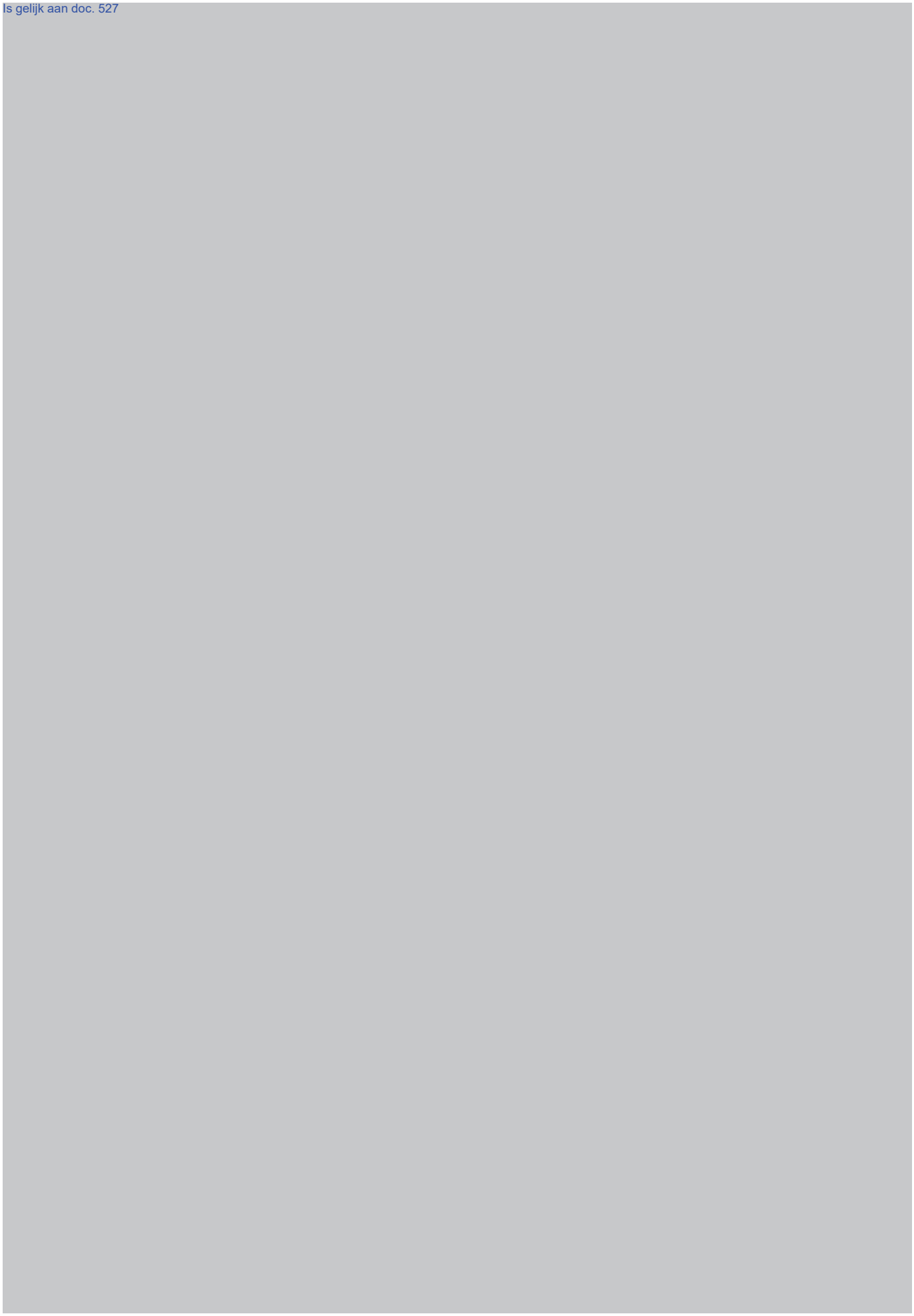
Is gelijk aan doc. 527



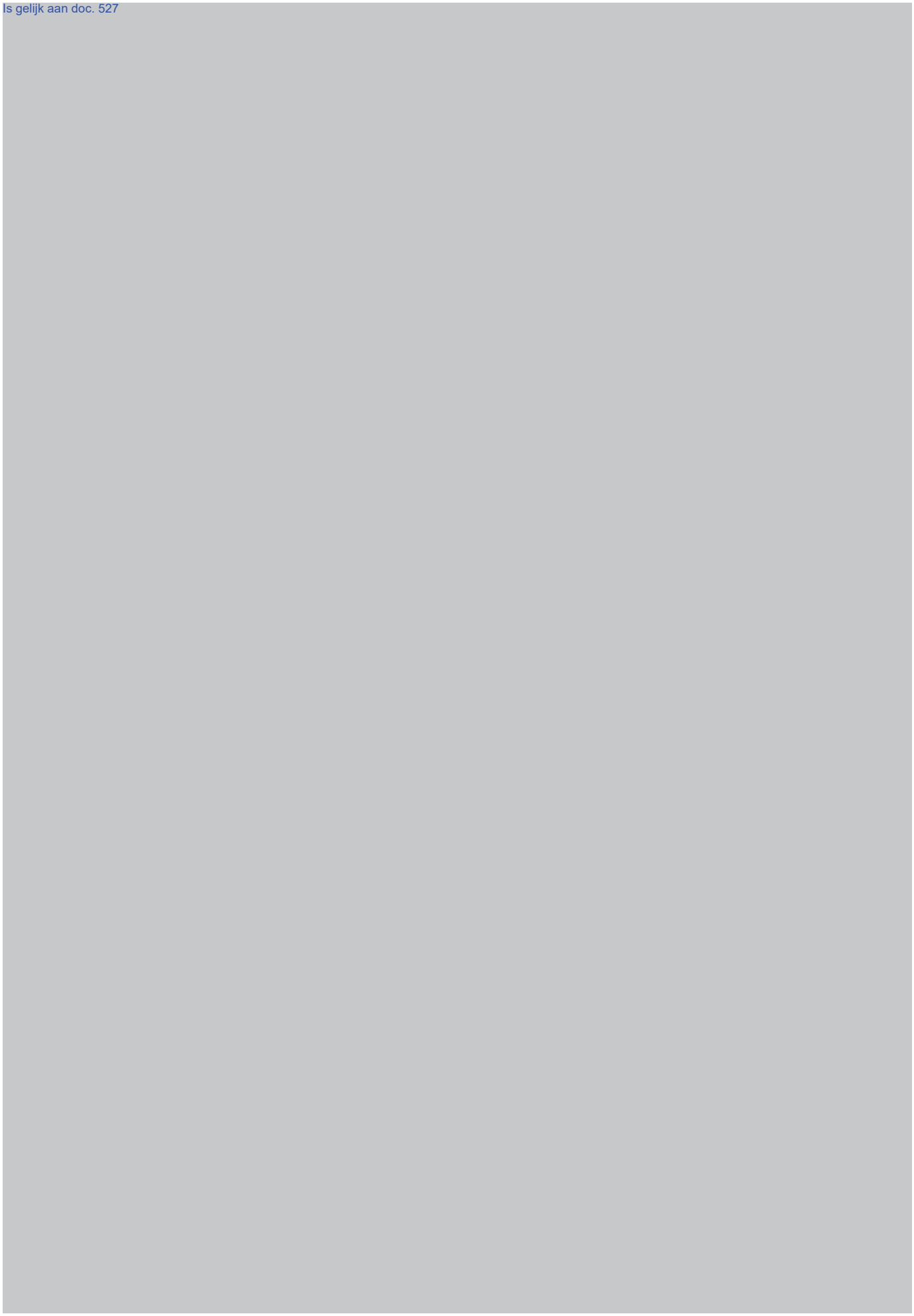
Is gelijk aan doc. 527



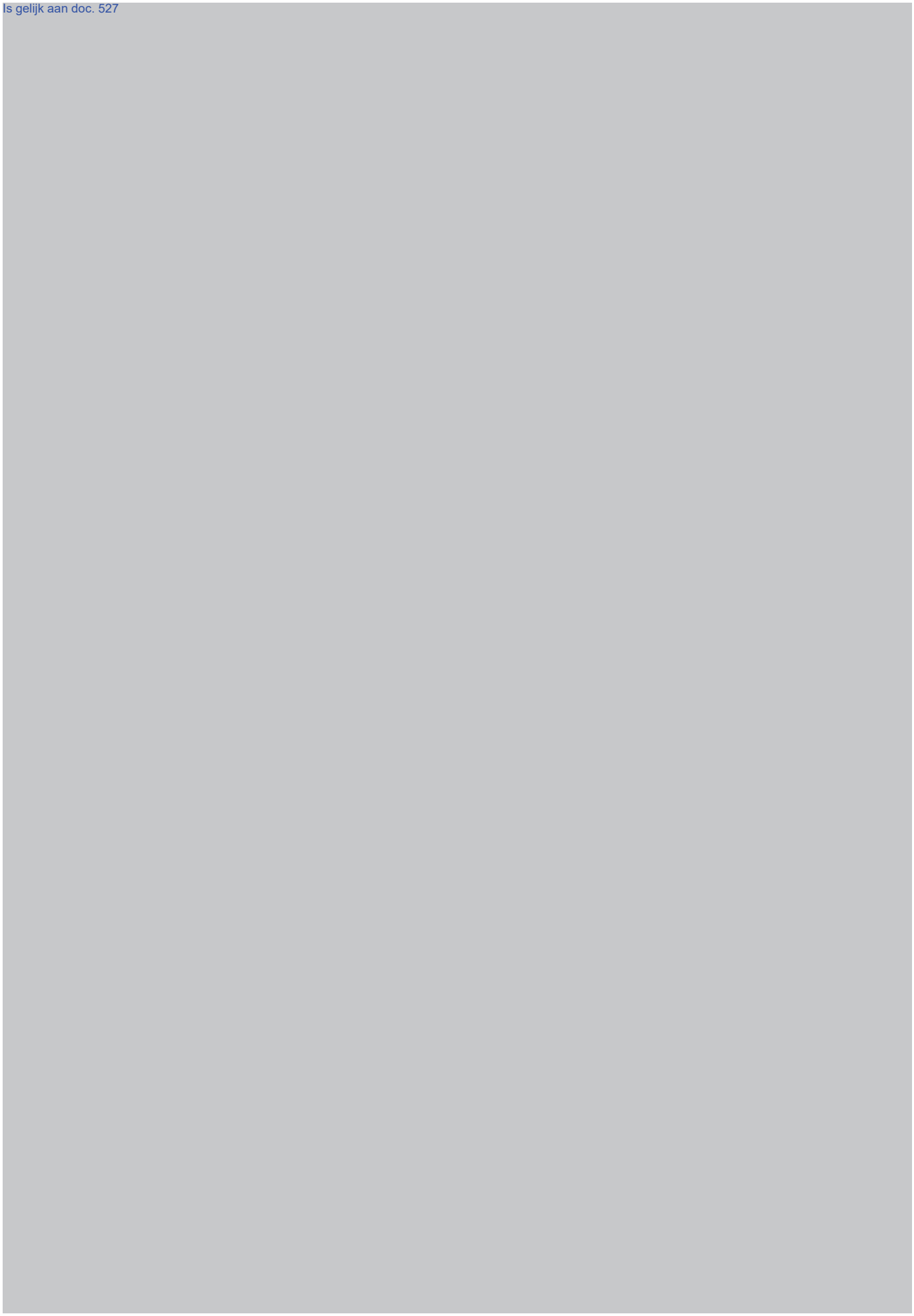
Is gelijk aan doc. 527



Is gelijk aan doc. 527

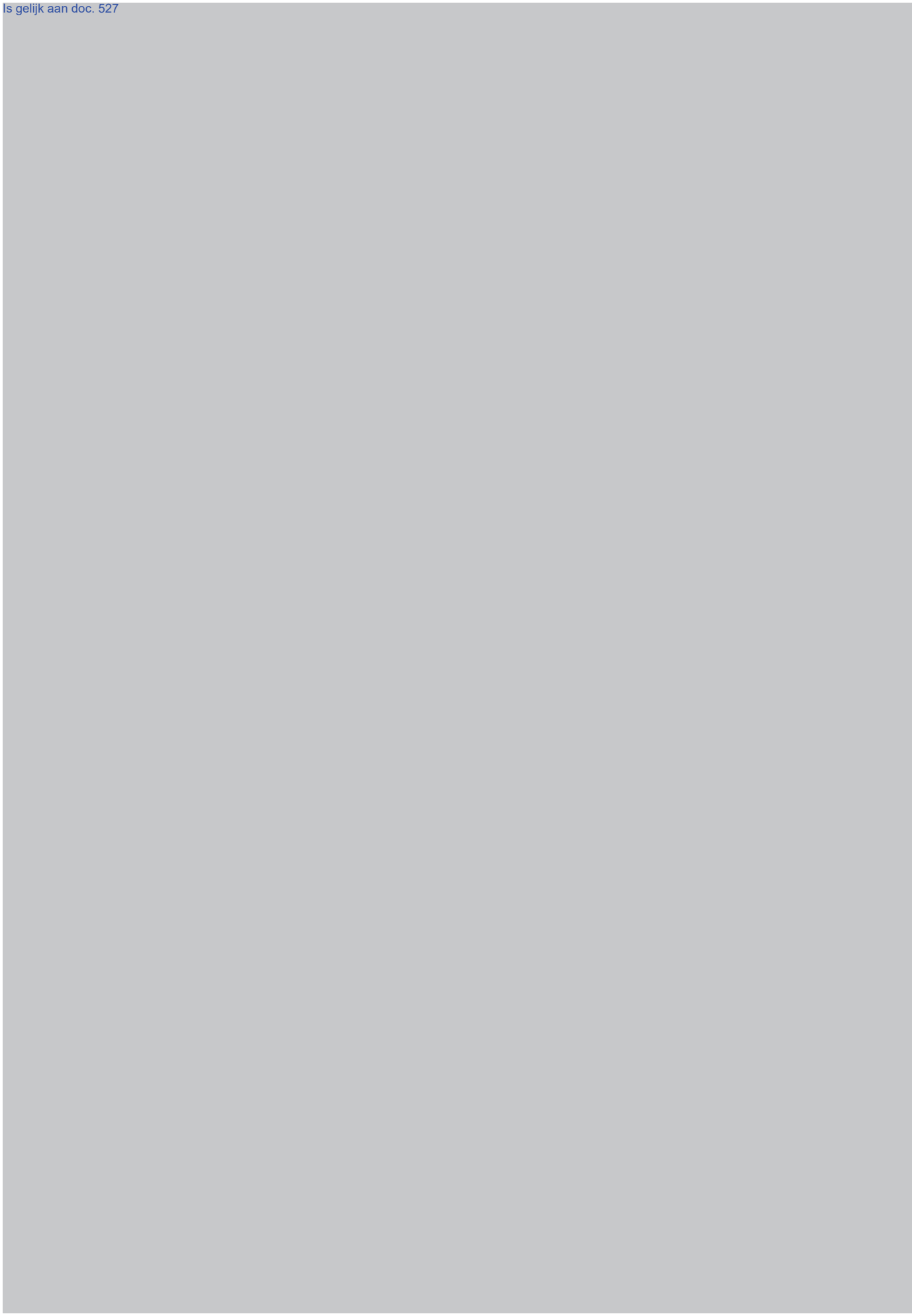


Is gelijk aan doc. 527



Is gelijk aan doc. 527

Is gelijk aan doc. 527



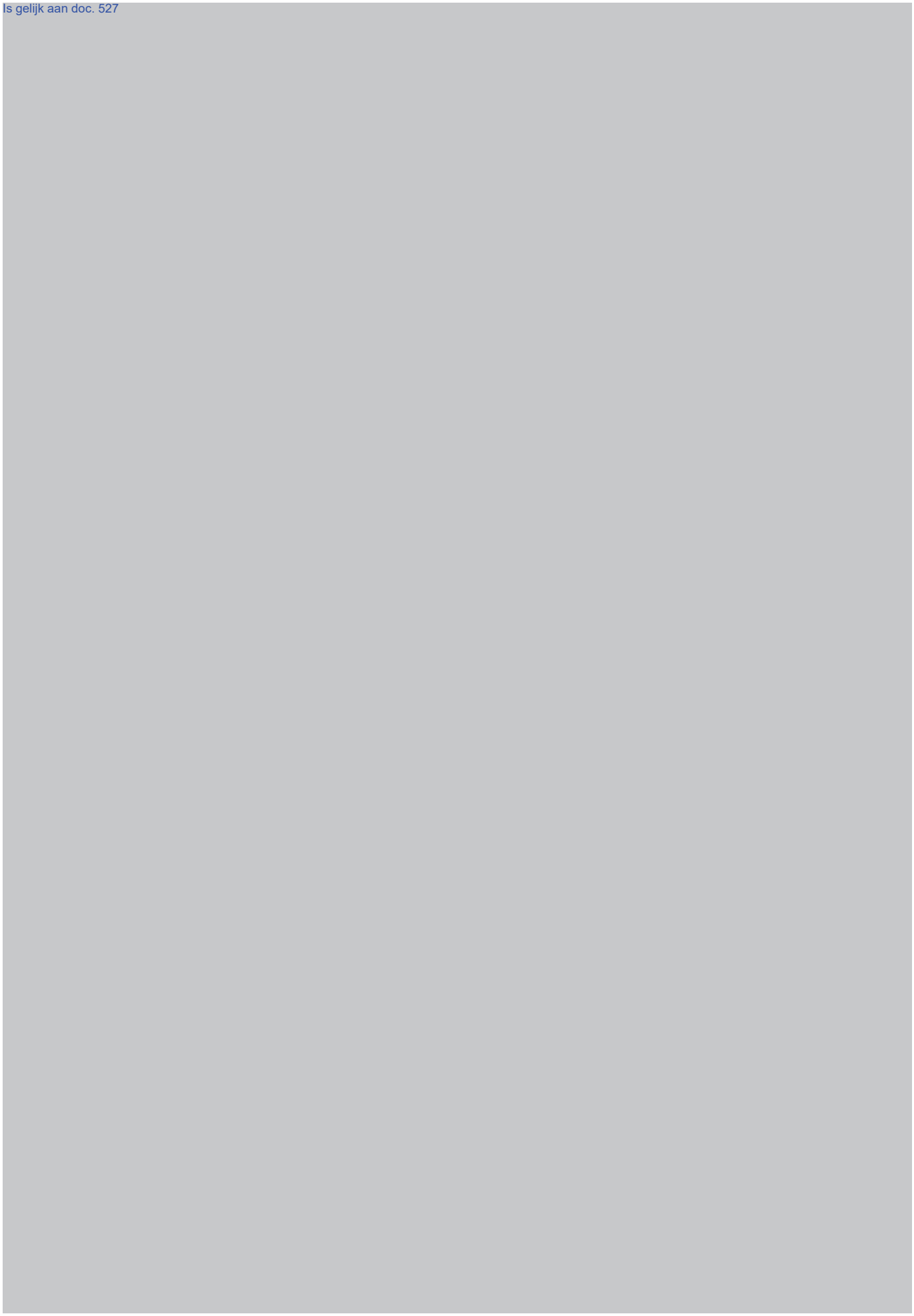
Is gelijk aan doc. 527

Is gelijk aan doc. 527

Is gelijk aan doc. 527

Is gelijk aan doc. 527

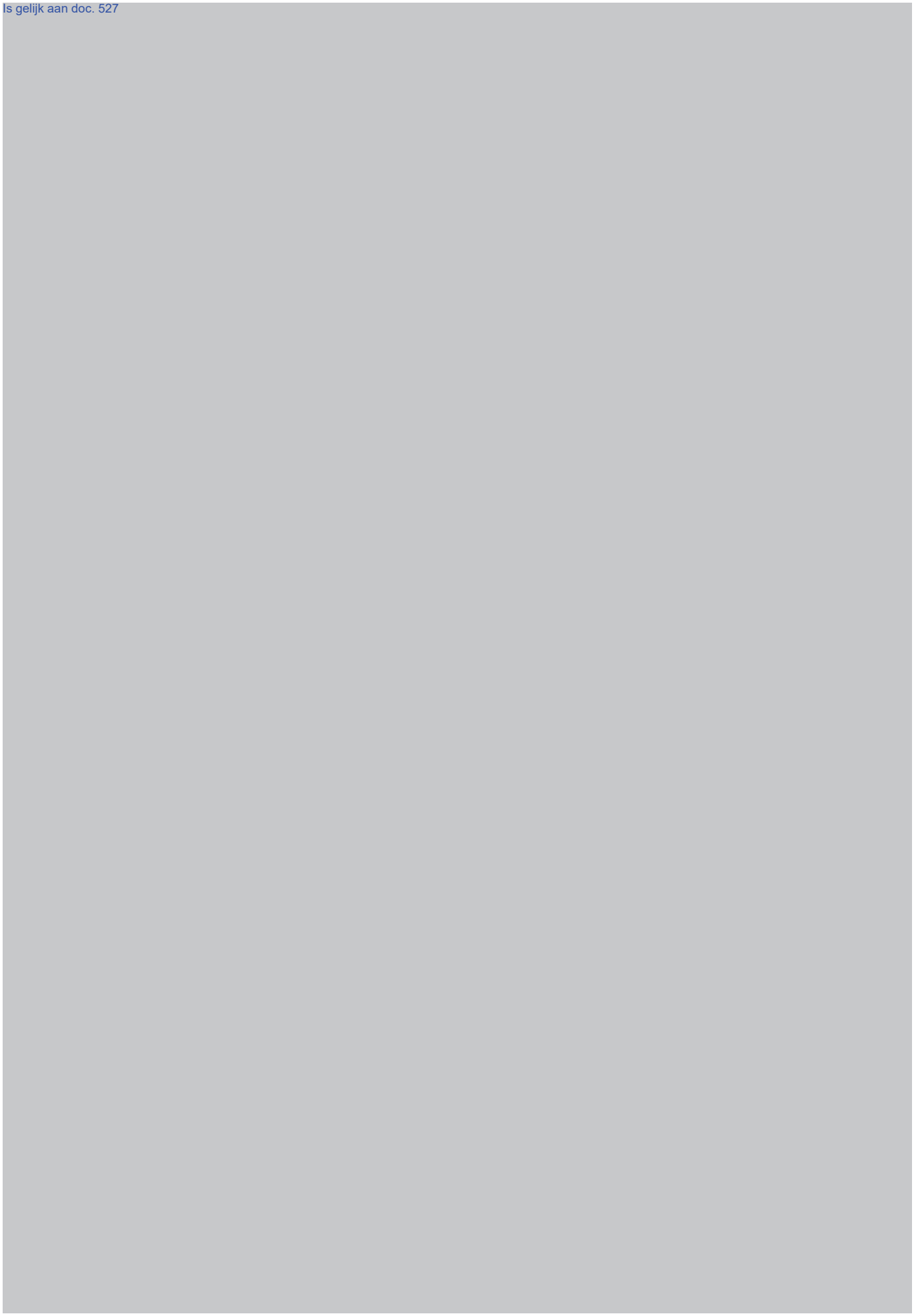
Is gelijk aan doc. 527



Is gelijk aan doc. 527

Is gelijk aan doc. 527

Is gelijk aan doc. 527



Van: 10.2.e
Verzonden: zondag 11 december 2016 22:09
Aan: 10.2.e
Onderwerp: CCIII
Bijlagen: Sprekerslijst[1].pdf

Opvolgingsmarkering: FollowUp
Markeringsstatus: Voltooid

Tweede Kamer
DER STATEN-GENERAAL

SPREKERSLIJST

Dinsdag 13 december 2016

Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III) (34 372)			
Naam:		Fractie:	Spreektijd:
1.	O.C. Tellegen	VVD	10 min
2.	M.M. van Toorenburg	CDA	15 min
3.	K. Verhoeven	D66	60 min
4.	L. van Tongeren	GroenLinks	30 min
5.	L.M.J.S. Helder	PVV	20 min
6.	S.M.J.G. Gesthuizen	SP	20 min

VVD = Volkspartij voor Vrijheid en Democratie
PvdA = Partij van de Arbeid
SP = Socialistische Partij
CDA = Christen Democratisch Appèl
PVV = Partij voor de Vrijheid
D66 = Democraten 66
ChristenUnie
GroenLinks
SGP = Staatkundig Gereformeerde Partij
PvdD = Partij voor de Dieren
50PLUS
GrKÖ = Groep Kuzu/Öztürk
GrBvK = Groep Bontes/Van Klaveren
Houwers
Klein
Monasch
Van Vliet

Van: 10.2.e
Verzonden: zondag 11 december 2016 22:11
Aan: 10.2.e
Onderwerp: 34372,_bijgewerkt_t_m_nr._7_(NvW_d.d._8_november_2016)[1].docx
Bijlagen: 34372,_bijgewerkt_t_m_nr._7_(NvW_d.d._8_november_2016)[1].docx

Opvolgingsmarkering: FollowUp
Markeringsstatus: Voltooid

Bijgewerkt t/m nr. 7 (nota van wijziging d.d. 8 november 2016)

34 372 **Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)**

Nr. 2 **VOORSTEL VAN WET**

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om geautomatiseerde werken op afstand heimelijk binnen te kunnen dringen met het oog op de opsporing van ernstige misdrijven, gegevens op doeltreffende wijze ontoegankelijk te kunnen doen maken ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten, de strafbaarheid van grooming en van verleiding van een minderjarige tot ontucht te verruimen alsmede het wederrechtelijk voorhanden hebben of bekend maken van door misdrijf verkregen gegevens en de online handelsfraude strafbaar te stellen;

Zo is het, dat Wij, de Afdeling advisering van Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

Het Wetboek van Strafrecht wordt als volgt gewijzigd:

A

Artikel 54a komt te luiden:

Artikel 54a

Een tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan als zodanig niet vervolgd indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering.

B

Artikel 80sexies komt te luiden:

Artikel 80sexies

Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.

C

Na artikel 138b wordt een artikel ingevoegd, luidende:

Artikel 138c

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt.

D

Artikel 139f komt te luiden:

Artikel 139f

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.

E

Artikel 139g komt te luiden:

Artikel 139g

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die niet-openbare gegevens:

a. verwerft of voorhanden heeft, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen;

b. ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregen gegevens betreft.

2. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang het verwerven, voorhanden hebben, ter beschikkingstellen, bekendmaken of gebruik van de gegevens, bedoeld in het eerste lid, vereiste.

F

Artikel 248a komt te luiden:

Artikel 248a

Hij die door giften of beloften van geld of goed, misbruik van uit feitelijke verhoudingen voortvloeiend overwicht of misleiding een persoon die de leeftijd van achttien jaren nog niet heeft bereikt of iemand die zich voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt, opzettelijk beweegt ontuchtige handelingen te plegen of zodanige handelingen van hem te dulden, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.

G

Artikel 248e komt te luiden:

Artikel 248e

Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst aan een persoon die de leeftijd van zestien jaren nog niet heeft bereikt of iemand die zich voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met een persoon die de leeftijd van zestien jaren nog niet heeft bereikt te plegen of een afbeelding van een seksuele gedraging waarbij een persoon die de leeftijd van zestien jaren nog niet heeft bereikt is betrokken te vervaardigen, wordt, indien hij enige handeling onderneemt tot het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of een geldboete van de vierde categorie.

H

Artikel 273d wordt gewijzigd als volgt:

1. In het eerste lid wordt “openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst” vervangen door: openbaar communicatienetwerk of een openbare communicatiedienst.

2. In het tweede lid wordt “niet-openbaar telecommunicatienetwerk of een niet-openbare telecommunicatiedienst” vervangen door: niet-openbaar communicatienetwerk of een niet-openbare communicatiedienst.

I

Na artikel 326c wordt een artikel ingevoegd, luidende:

Artikel 326d

Hij die een beroep of een gewoonte maakt van het door middel van een geautomatiseerd werk verkopen van goederen of verlenen van diensten tegen betaling met het oogmerk om zonder volledige levering zich of een ander van de betaling van die goederen of diensten te verzekeren, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

ARTIKEL II

Het Wetboek van Strafvordering wordt als volgt gewijzigd:

A

In artikel 67, eerste lid, onderdeel b, wordt na “139d, eerste en tweede lid,” ingevoegd: 139g,.

B

In artikel 67a, tweede lid, onder 3°, wordt na “326a” ingevoegd: 326d.

C

Aan artikel 125m wordt een lid toegevoegd, luidende:

5. Degene tot wie een bevel, als bedoeld in artikel 125k, eerste lid, is gericht neemt in het belang van het onderzoek geheimhouding in acht omtrent al hetgeen hem terzake van de vordering bekend is.

D

Na artikel 125o wordt een artikel ingevoegd, luidende:

Artikel 125p

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie aan een aanbieder van een communicatiedienst als bedoeld in artikel 138e het bevel richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:

a. het strafbare feit;

b. de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens noodzakelijk is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen;

c. welke gegevens ontoegankelijk moeten worden gemaakt.

3. Artikel 125o, tweede en derde lid, zijn van overeenkomstige toepassing.

4. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. De rechter-commissaris stelt de aanbieder tot wie het bevel is gericht in de gelegenheid te worden gehoord. De aanbieder is bevoegd zich bij het horen door een raadsman te doen bijstaan.

E

Artikel 126g, derde lid, tweede volzin, komt te luiden:

Een technisch hulpmiddel wordt niet op een persoon bevestigd, tenzij met diens toestemming dan wel in het geval, bedoeld in artikel 126nba, eerste lid, onder c.

F

Artikel 126la vervalt.

G

In Titel IVA van het Eerste Boek wordt, onder vernummering van de Achtste tot de Negende afdeling, een afdeling ingevoegd, luidende:

ACHTSTE AFDELING ONDERZOEK IN EEN GEAUTOMATISEERD WERK

Artikel 126nba

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;

b. de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;

c. de uitvoering van een bevel als bedoeld in artikel 126g, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd;

en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:

a. het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;

b. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;

c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;

d. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;

e. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;

f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;

g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;

h. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

3. Het bevel, bedoeld in het eerste lid, wordt gegeven voor een periode van ten hoogste vier weken. Het kan telkens voor een periode van ten hoogste vier weken worden verlengd.

4. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is.

5. Het bevel, bedoeld in het eerste lid, kan schriftelijk en met redenen omkleed worden gewijzigd, aangevuld, verlengd of beëindigd, met dien verstande dat de officier van justitie voor wijziging, aanvulling of verlenging een machtiging van de rechter-commissaris behoeft. Bij dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven. De officier van justitie en de rechter-commissaris stellen deze in dat geval binnen drie dagen op schrift.

6. Nadat het onderzoek is beëindigd wordt het technische hulpmiddel verwijderd. Indien het technische hulpmiddel niet of niet volledig kan worden verwijderd en dit risico's oplevert voor het functioneren van het geautomatiseerde werk stelt de officier van justitie de beheerder van het geautomatiseerde werk daarvan in kennis en stelt de nodige informatie ter beschikking ten behoeve van de volledige verwijdering. Het bepaalde in artikel 126cc, eerste lid, is van overeenkomstige toepassing.

7. Het toezicht op de uitvoering van het bevel, bedoeld in het eerste lid, door de ambtenaren, bedoeld in artikel 141, onderdeel d, en de personen, bedoeld in artikel 142, eerste lid, onderdeel b, wordt uitgeoefend door de inspectie, bedoeld in artikel 65 van de Politiewet 2012, overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012.

8. Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent:

a. de autorisatie en deskundigheid van de opsporingsambtenaren die kunnen worden belast met het binnendringen en het onderzoek, bedoeld in het eerste lid, en de samenwerking met andere opsporingsambtenaren;

b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.

9. Bij algemene maatregel van bestuur kunnen regels worden gesteld over de toepassing van de bevoegdheid, bedoeld in het eerste lid, in de gevallen waarin niet bekend is waar de gegevens zijn opgeslagen.

H

In artikel 126ng, eerste lid, wordt "artikel 126la" vervangen door: artikel 138e.

I

In artikel 126ni, tweede lid, wordt "artikel 126la" vervangen door: artikel 138e.

J

Artikel 126o, derde lid, tweede volzin, komt te luiden:

Een technisch hulpmiddel wordt niet op een persoon bevestigd, tenzij met diens toestemming dan wel in het geval, bedoeld in artikel 126uba, eerste lid, onder c.

K

In artikel 126t, eerste lid, wordt “artikel 126la” vervangen door: artikel 138e.

L

Na artikel 126ub wordt een artikel ingevoegd, luidende:

Artikel 126uba

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat in gebruik is bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;

b. de uitvoering van een bevel als bedoeld in de artikelen 126s en 126t;

c. de uitvoering van een bevel als bedoeld in artikel 126o waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd;

en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:

a. een omschrijving van het georganiseerd verband en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven;

b. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;

c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;

d. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;

e. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;

f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;

g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;

h. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

3. Artikel 126nba, derde tot en met negende lid, is van overeenkomstige toepassing.

M

Artikel 126zd, vierde lid, tweede volzin, komt te luiden:

Een technisch hulpmiddel wordt niet op een persoon bevestigd, tenzij met diens toestemming dan wel in het geval, bedoeld in artikel 126zpa, eerste lid, onder c.

N

In artikel 126zg, eerste lid, wordt “artikel 126la” vervangen door: artikel 138e.

O

In artikel 126zi, eerste lid, wordt “artikel 126la” vervangen door: artikel 138f.

P

In artikel 126zo, eerste lid, wordt “artikel 126la” vervangen door: artikel 138e.

Q

Na de Derde afdeling A wordt een Derde afdeling B ingevoegd, luidende:

DERDE AFDELING B ONDERZOEK IN EEN GEAUTOMATISEERD WERK

Artikel 126zpa

1. In geval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat in gebruik is bij een persoon en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:

a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;

b. een bevel als bedoeld in de artikel 126zg;

c. een bevel als bedoeld in artikel 126zd, eerste lid, onder a, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd;

en, ingeval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;

d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

2. Het bevel vermeldt, behalve de gegevens, bedoeld in artikel 126za, tevens:

a. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;

b. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;

c. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;

d. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;

e. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;

f. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.

3. Artikel 126nba, derde tot en met negende lid, is van overeenkomstige toepassing.

R

In artikel 126bb, tweede lid, onderdeel b, wordt “bedoeld in artikel 126m, derde lid, onderdeel c, artikel 126t, derde lid, onderdeel c, en artikel 126zg, tweede lid, onderdeel a” vervangen door: bedoeld in artikel 126m, tweede lid, onderdeel c, artikel 126t, tweede lid, onderdeel c, en artikel 126zg, tweede lid, onderdeel a.

S

In Titel VD komt het opschrift van de Derde afdeling te luiden:

DERDE AFDELING DE BEWARING EN DE VERNIETIGING VAN PROCESSEN-VERBAAL EN ANDERE VOORWERPEN, HET GEBRUIK VAN GEGEVENS VOOR EEN ANDER DOEL EN DE ONTOEGANKELIJKMAKING EN VERNIETIGING VAN GEGEVENS.

T

Aan artikel 126cc worden twee leden toegevoegd, luidende:

5. Indien bij een onderzoek in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Het bepaalde in artikel 125o, tweede en derde lid, is van overeenkomstige toepassing.

6. Zodra blijkt dat gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk van geen betekenis zijn voor het onderzoek, worden zij vernietigd. Artikel 125n, tweede lid, is van toepassing.

U

Artikel 126ee, aanhef en onderdelen a en b, komt te luiden:

Bij algemene maatregel van bestuur worden regels gesteld omtrent:

a. De opslag, verstrekking, plaatsing en verwijdering van de technische hulpmiddelen, bedoeld in de artikelen 126g, derde lid, 126l, eerste lid, 126nba, eerste lid, 126o, derde lid, 126s, eerste lid, 126uba, eerste lid, 126zd, eerste lid, 126zf, eerste lid, en 126zpa, eerste lid, alsmede van de technische hulpmiddelen bedoeld in de artikelen 126m, eerste lid, 126t, eerste lid, en 126zg, eerste lid, voor zover het bevel, bedoeld in artikel 126m, derde of vierde lid, onderscheidenlijk de artikelen 126t, derde of vierde lid en 126zg, derde of vierde lid, ten uitvoer wordt gelegd zonder medewerking van de betrokken aanbieder;

b. de technische eisen waaraan de hulpmiddelen voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen of, in geval van toepassing van artikel 126nba, 126uba of 126zpa, de vastgelegde gegevens, en met het oog op het voorkomen van misbruik door derden;.

V

Na artikel 138d worden twee artikelen ingevoegd, luidende:

Artikel 138e

Onder aanbieder van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

Artikel 138f

Onder gebruiker van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst.

W

Artikel 354 wordt als volgt gewijzigd:

1. In het eerste lid wordt ”artikel 125o” vervangen door: de artikelen 125o of 126cc, vijfde lid,.

2. Er wordt een lid toegevoegd, luidende:

3. In de gevallen, bedoeld in artikel 353, eerste lid, neemt de rechtbank tevens een beslissing over het bevel, bedoeld in artikel 125p, indien een dergelijk bevel nog niet is opgeheven.

X

Artikel 552a wordt als volgt gewijzigd:

1. Het eerste lid wordt als volgt gewijzigd:

a. De zinsnede “over de vordering medewerking te verlenen aan het ontsleutelen van gegevens,” wordt vervangen door: over het bevel toegang te verschaffen tot een geautomatiseerd werk of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens dan wel kennis omtrent de beveiliging daarvan ter beschikking te stellen,.

b. ”Artikel 125o” wordt vervangen door: de artikelen 125o en 126cc, vijfde lid.

c. Er worden twee volzinnen toegevoegd, luidende: De belanghebbenden kunnen zich voorts schriftelijk beklagen over een bevel tot het ontoegankelijk maken van gegevens, bedoeld in artikel 125p. Over het beklag, bedoeld in de vorige volzin, beslist het gerecht zo spoedig mogelijk.

2. In het derde lid wordt na de zinsnede “ontoegankelijkmaking van de gegevens” ingevoegd: of het bevel, bedoeld in de artikelen 125k en 125p,.

3. In het vierde lid, eerste volzin, wordt na de zinsnede “is geschied” ingevoegd: of het bevel, bedoeld in de artikelen 125k en 125p, is gegeven.

4. Er wordt een lid toegevoegd, luidende:
9. Acht het gerecht het beklag, bedoeld in het eerste lid, tweede volzin, gegrond, dan kan het het bevel geheel of gedeeltelijk opheffen.

Y

In artikel 552fa, eerste lid, wordt “artikel 125o” vervangen door: de artikelen 125o of 126cc, vijfde lid,.

Z

In artikel 552ww, derde lid, wordt “artikel 126la” vervangen door: artikel 138f.

AA

In artikel 552ddd, derde lid, wordt “artikel 126la” vervangen door: artikel 138f.

BB

In artikel 577bb, eerste lid, onder c, wordt “artikel 126la” vervangen door: artikel 138e.

CC

In artikel 577be, eerste lid, wordt “artikel 126la” vervangen door: artikel 138f.

DD

In artikel 577bf, eerste lid, wordt “artikel 126la” vervangen door: artikel 138e.

EE

Artikel 592, tweede lid, eerste volzin, komt te luiden: De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 125k, 126m, 126n, 126na, 126nc tot en met 126ni, 126t, 126u, 126ua, 126uc tot en met 126ui, 126zg, 126zh, 126zi en 126zja tot en met 126zp kunnen de betrokkene uit ’s Rijks kas worden vergoed.

ARTIKEL IIa

Aan artikel 7 van de Wet op de bijzondere opsporingsdiensten wordt een nieuw lid toegevoegd, luidende:

4. Het bepaalde in het eerste lid laat het bepaalde in artikel 126nba, achtste lid, van het Wetboek van Strafvordering onverlet.

ARTIKEL III

Onze Minister zendt binnen vijf jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag over de doeltreffendheid en effecten van deze wet in de praktijk.

ARTIKEL IV

1. Indien het voorstel van wet van de leden Gesthuizen en Van Oosten tot wijziging van Boek 6 van het Burgerlijk Wetboek in verband met het tegengaan van acquisitiefraude door het doen van misleidende mededelingen jegens diegenen die handelen in de uitoefening van hun beroep, bedrijf of organisatie en wijziging van het Wetboek van Strafrecht in verband met de strafbaarstelling van acquisitiefraude (33 712), tot wet is of wordt verheven, en artikel II van die wet eerder in werking is getreden of treedt dan de artikelen I, onderdeel I, en II, onderdeel B, van deze wet, worden deze wet als volgt gewijzigd :

a. In artikel I, onderdeel I, wordt “artikel 326c” gewijzigd in: artikel 326d;

b. In artikel I, onderdeel I, wordt “Artikel 326d” gewijzigd in: Artikel 326e;

c. In artikel II, onderdeel B, wordt “326d” gewijzigd in: 326e.

2. Indien het bij koninklijke boodschap van 24 november 2014 ingediende voorstel van wet tot wijziging van het Wetboek van Strafvordering en de Wet op de economische delicten in verband met het gebruik van elektronische processtukken (digitale processtukken Strafvordering) (34 090), tot wet is of wordt verheven, en artikel I, onderdelen F en P, van die wet eerder in werking is getreden of treedt dan artikel II, onderdelen H, I, K, N,O, P, V, Z, AA, BB, CC en DD, wordt artikel II van deze wet als volgt gewijzigd:

a. In de onderdelen H, I, K, N, P, V, BB, en DD wordt “artikel 138e” vervangen door: artikel 138g;

b. In de onderdelen O, V, Z, AA en CC wordt “artikel 138f” vervangen door: artikel 138h;

c. In onderdeel V wordt “artikel 138d” vervangen door: artikel 138f;

d. In onderdeel X, subonderdeel 4, wordt de aanduiding “9” vervangen door: 10.

3. Indien het bij koninklijke boodschap van 21 november 2014 ingediende voorstel van wet tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met een herziening van de wettelijke regeling van de

tenuitvoerlegging van strafrechtelijke beslissingen (Wet herziening tenuitvoerlegging strafrechtelijke beslissingen) (34 086), tot wet is of wordt verheven, en artikel I, onderdelen NN en QQ, van die wet eerder in werking is getreden of treedt dan artikel II, onderdelen BB, CC, DD en EE van deze wet wordt:

a. in artikel II, onderdeel BB "artikel 577bb, eerste lid, onder c" vervangen door: artikel 6:4:12, eerste lid, onder c;

b. in artikel II, onderdeel CC "Artikel 577be" vervangen door: artikel 6:4:15;

c. in artikel II, onderdeel DD "artikel 577bf" vervangen door: artikel 6:4:16;

d. in artikel II, onderdeel EE "Artikel 592, tweede lid, eerste volzin" vervangen door: Artikel 531, tweede lid, eerste volzin.

ARTIKEL V

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Staatssecretaris van Veiligheid en Justitie,

Van: 10.2.e
Verzonden: zondag 11 december 2016 23:00
Aan: 10.2.e
Onderwerp: Q&A inkoop
Bijlagen: Document1.docx


Zie versie doc 550

Van: 10.2.e
Verzonden: zondag 11 december 2016 23:15
Aan: 10.2.e @politie.nl>
Onderwerp: Heimelijke inkoop

Hi 10.2.e ,

Ik heb dinsdagavond debat CCIII. Het gaat hier mogelijk ook of inkoop van software voor binnendringen. In de Q&A geven we aan dat we dit volgens de geldende inkoopprocessen doen. Hopelijk is dat voldoende, maar ik verwacht wel dat er doorgevraagd wordt.
We gaan dit inkopen via heimelijke inkoop. Ik heb twee vervolg Q&A's gemaakt voor mezelf mochten we een vervolgvraag krijgen. Mara ik weet niet of dit past binnen wat we anders communiceren.

Kun je kijken of dit zo ok is? Heb je nog andere tips?

Groet,
10.2.e

Van: 10.2.e
Verzonden: maandag 12 december 2016 08:25
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>
Onderwerp: FW: Heimelijke inkoop

Hoi 10.2.e ,

Ik denk dat je het best even contact kan leggen met 9 v.w.b. heimelijke trajecten gerelateerd aan middelen. 💻

Gr 10.2.e

Van: 10.2.e
Verzonden: maandag 12 december 2016 13:26
Aan: 10.2.e
CC: Bestuursondersteuning
Onderwerp: RE: amendementen CIII
Bijlagen: 34372-11.pdf; 34372-10.pdf

Amendement 8 van D66-Verhoeven is vervangen door bijgaand amendement 11.
CDA heeft nog een amendement ingediend over evaluatietermijn (over 3 ipv 5 jaar)

Tweede Kamer der Staten-Generaal

1192 2

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 10

AMENDEMENT VAN HET LID VAN TONGEREN

Ontvangen 8 december 2016

De ondergetekende stelt het volgende amendement voor:

In artikel III wordt «vijf jaar» vervangen door: drie jaar.

Toelichting

De Wet Computercriminaliteit III introduceert vergaande opsporingsbevoegdheden. De Afdeling advisering van de Raad van State oordeelt dat de proportionaliteit van de voorgestelde bevoegdheid van het heimelijk binnendringen in een geautomatiseerd werk onbewezen is gebleven. Dat levert spanning op met het grondwettelijk en verdragsrechtelijk erkende recht op eerbiediging van de persoonlijke levenssfeer. Zo beschouwd is het van belang om op korte termijn inzicht te krijgen in de aard en omvang van de toepassing van de in dit wetsvoorstel geïntroduceerde bevoegdheden en de beoordeling van deze toepassing door de strafrechter. Daarom is indiener van mening dat de evaluatiebepaling moet worden aangepast.

Van Tongeren

kst-34372-10
ISSN 0921 - 7371
's-Gravenhage 2016

Tweede Kamer der Staten-Generaal

1193 2

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 11

AMENDEMENT VAN HET LID VERHOEVEN C.S. TER VERVANGING VAN DAT GEDRUKT ONDER NR. 8[1]

Ontvangen 8 december 2016

De ondergetekenden stellen het volgende amendement voor:

In artikel II, onderdeel G, wordt in artikel 126nba in het eerste lid, aanhef, «binnendringt in een geautomatiseerde werk dat bij de verdachte in gebruik is» vervangen door: zonder gebruik te maken van kwetsbaarheden in software een geautomatiseerd werk dat bij de verdachte in gebruik is binnendringt.

Toelichting

Dit amendement beperkt de bevoegdheid voor de politie om geautomatiseerde werken binnen te dringen, er mag namelijk geen gebruik worden gemaakt van kwetsbaarheden in software. Het binnendringen van geautomatiseerde werken zonder gebruik van kwetsbaarheden in software kan bijvoorbeeld door middel van (spear)phishing technieken, oftewel het sturen van een misleidende email of bericht waarmee een verdachte verleid kan worden om een wachtwoord of logingegevens prijs te geven of om een technisch hulpmiddel zoals een keylogger of andere software te installeren, mits zonder het gebruik van kwetsbaarheden, waarmee vervolgens inloggegevens buitgemaakt kunnen worden. Een andere techniek is social engineering, waarmee door middel van psychologische manipulatie het uitvoeren van handelingen of het openbaar maken van vertrouwelijke informatie, zoals een wachtwoord of inloggegevens, uitgelokt kan worden. Daarnaast zijn technieken mogelijk als brute forcing, dictionary attacks of shoulder surfing.

Cybersecurity experts benadrukken vaak het feit dat de mens de zwakste schakel in ICT-systemen is. Volgens de «Cyber Security Intelligence Index 2015» komt 95 procent van alle beveiligingsincidenten voort uit menselijke fouten. Uit meerdere onderzoeken blijkt dat ook de

[1] Vervanging in verband met een wijziging in de ondertekening.

kst-34372-11
ISSN 0921 - 7371
's-Gravenhage 2016

criminelen die zich goed beveiligen steken laten liggen. Een sprekend voorbeeld daarvan is de uitbater van de ondergrondse digitale markt Silk Road.

Het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software is een extra bevoegdheid waarvan de noodzaak niet voldoende aangetoond is. Bovendien is het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software een onwenselijke bevoegdheid. Het maakt mensen onveilig omdat kwetsbaarheden in telefoons, tablets en andere apparaten blijven bestaan, waardoor mensen makkelijker slachtoffer kunnen worden van cybercrime. Hiermee zou de overheid een belang krijgen bij onveilige apparaten, zoals laptops, smartphones, wearables en computers en, gezien de brede definitie van «geautomatiseerde werken», ook pacemakers, auto's en medische apparatuur. Dit zorgt ervoor dat hackers die fouten in software vinden eerder geneigd zullen zijn om gevonden fouten te verkopen aan bedrijven als HackingTeam of Gamma International dan ze te melden aan de maker van de software zodat ze gedicht kunnen worden. Dit kan bijvoorbeeld gaan om een fout in het besturingssysteem van smartphones..

In een tijd waarin vrijwel elk apparaat op het internet wordt aangesloten en onze veiligheid en onze economie steeds meer afhankelijk zijn van veilige ICT-systemen is het belangrijk dat de overheid zich juist inzet voor een veiliger internet. Deze bevoegdheid zou grote schade toebrengen aan onze economie en aan ons vestigingsklimaat. Daarnaast maakt het iedereen gevoeliger voor hacks door criminelen en landen als Rusland en China. Criminelen zullen makkelijker gegevens, zoals medische data, creditcardgegevens of inloggegevens, van gewone mensen buit kunnen maken. Daarom willen de indieners dat de overheid blijft werken aan een veiliger internet, veiligere software en sterke encryptie, alleen dan kunnen mensen veiliger gemaakt worden tegen criminelen en buitenlandse mogendheden.

Verhoeven
Van Tongeren
Gesthuizen

Van: 10.2.e BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: dinsdag 13 december 2016 09:42
Aan: 10.2.e
Onderwerp: FW: Dossier wetsvoorstel computercriminaliteit III (34 372)
Bijlagen: CCIII.dossier02.02.16.docx

Opvolgingsmarkering: FollowUp
Markeringsstatus: Gemarkeerd

10.2.e
Elz

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
SBA
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Is gelijk aan doc 514

Van: 10.2.e
Verzonden: dinsdag 13 december 2016 13:25
Aan: 10.2.e
Onderwerp: RE: Heimelijke inkoop
Bijlagen: Document1_UZ.docx

10.2.e

Hopelijk kun je hiermee uit de voeten.

Groet

10.2.e

10.2.e
Serviceteam AO & B i.o.
Politie – Project BBV
Faunalaan 247, 3972 PP Driebergen
Postbus 100 , 3970 AC Driebergen

Q: Waarom worden de naam van de leverancier(s) en de gebruikte software niet bekend gemaakt door de politie?

12-14

Q: Als de standaard inkoopprocessen van de politie worden gebruikt, wordt dan op die manier bekend welke kwetsbaarheden de politie gebruikt voor het binnendringen?

A: Nee, bij de inkoop worden van opsporingsmiddelen kunnen maatregelen worden getroffen om te voorkomen dat opsporingsmethodieken bekend worden bij criminelen.

10.2.e voor jou informatie:
12-14

A. Wellicht niet zozeer met het enkel bekendmaken van de naam van de leverancier maar wel met het bekendmaken van in gebruik zijnde software (of juist door de combinatie van leverancier en software!) is na te gaan welke methoden en technieken de politie kan gebruiken bij de opsporing. Het opsporingswerk wordt daardoor bemoeilijkt of zelfs onmogelijk gemaakt. Immers, met die kennis zouden criminelen kunnen anticiperen op mogelijke opsporing door de politie.

Q2:
10.2.e voor jou:
standaardproducten worden middels standaard inkoopprocessen (PDC, IKM en PDM) verworden. Voor afgeschermde diensten of producten worden afgeschermde processen gevolgd, dit kan zelfs verwerven onder geheimhouding zijn. De KC tekent dan voordat er besteld mag worden een geheimhoudingsverklaring conform art 2.23 lid 1 sub e AW.

A.Klopt helemaal!