# Deel Aa: documenten DGRR

Ministerie van Justitie en Veiligheid

DGRR / DRC

**Minister van Justitie en Veiligheid**
DGRR_DRC-GC

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverhe d.nl/jenv

**Contactpersoon**
10 2 e

T 070 10 2 e
F 070 370 79 39

**Datum**
3 juni 2019

**Ons kenmerk**
2619263

# nota

Gespreksnota Interceptie OTT diensten

**Conciplënt**
10 2 e
Datum/eindparaaf

## Doel

De aard en omvang van elektronische communicatie tussen personen is in de afgelopen tien jaar snel veranderd. Zo maken we - vooral met het omvangrijke aantal smartphones en tablets dat in omloop is[1] - steeds meer gebruik van versleutelde over-the-top communicatiediensten (OTT), zoals WhatsApp. Doel van deze nota is om u te informeren over de praktische problemen waarmee opsporings- en veiligheidsdiensten door deze ontwikkeling worden geconfronteerd bij het kunnen aftappen, uitluisteren en opvragen van gegevens van elektronische communicatiediensten en de juridische dillema's die voorvloeien uit het ondervangen daarvan. Daarnaast wordt u een advies gegeven over de mogelijke oplossingen om dit probleem te ondervangen.

Onderstaande nota is uitgewerkt conform het beleidsvoornemen dat in het jaarplan DGRR 2019 is opgenomen en is opgesteld door DRC (F&O en C&V) in samenwerking met politie, OM, bureau PIDS, EZK, AIVD, MIVD, NCTV en DGPenV. Het advies aan het einde van deze nota wordt door deze organisaties ambtelijk ondersteund.

## Aanleiding: ontwikkelingen in elektronische communicatie

De manier waarop via elektronische wijze wordt gecommuniceerd is de afgelopen 10 jaar sterk veranderd en doet dat, in lijn met de

[1] Volgens onderzoek van Ericsson is het aantal abonnementen voor devices (waaronder telefoons en tablets) toegenomen van een kleine 2 miljard in 2013 tot ruim 7,9 miljard in 2019 (Bron: Ericsson Mobility Report Q4 2018 update).

voortschrijdende digitalisering van ons dagelijks leven, in een blijvend hoog tempo. Zo gaat communicatie via mobile devices (telefoons, ipad, etc.) steeds meer via over-the-top (OTT) diensten – ze gaan over het elektronische datanetwerk van aanbieders (het internet) - zoals WhatsApp, Snapchat, Twitter en vele andere diensten. Zie ter illustratie figuur 1 over de toename van het WhatsApp gebruik in Nederland en Duitsland. Het gebruik van gewone telefoniediensten voor spraak en tekstberichten neemt sterk af en de verwachting is dat over niet al te lange tijd (komende 5 jaar), zeker als 5G breed is geadopteerd, elektronische communicatie grotendeels via software over het datanetwerk (over-the-top) zal verlopen.[2]

Over The Top diensten

De geschetste ontwikkeling heeft een aantal consequenties voor de opsporing en het bewaken van de nationale veiligheid, die nu al een invloed hebben op de effectiviteit hiervan.

1. Allereerst maken veel OTT diensten gebruik van end-to-end encryptie: aanbieders van de diensten hebben in sommige gevallen dan zelf geen mogelijkheid meer om de berichten te ontcijferen, dat kan enkel door de zender en de ontvanger. Dat is goed voor de bescherming van inhoud en privacy, maar zorgt er ook voor dat de overheid bij een gerechtvaardigd belang de inhoud van de communicatie niet altijd meer kan inzien; tenzij een device zelf wordt binnengedrongen[3] door de overheid. De bevoegdheid tot binnendringen met gebruik van "hack software" is geregeld met de wet CCIII. Daar zijn hoge eisen gesteld. De devices bevatten veel persoonlijk materiaal, en eenmaal binnengedrongen kan veel meer dan alleen de communicatie over en OTT-dienst worden ingezien. Voorts zijn er strenge voorwaarde gesteld aan de leveranciers van software waarmee device gehackt kunnen worden door de overheid.[4] Daarmee wordt het naar verwachting, de bevoegdheid

[2] Voor OTT-diensten geldt dat er geen exclusieve technische of commerciële koppeling is tussen de aansluiting van het apparaat op internet en de inhoudelijke dienst (de berichtenservice). De dienst is met andere woorden via verschillende aansluitingen op verschillende netwerken van verschillende providers tegelijk en zelfs simultaan toegankelijk.

[3] Mogelijk in gevallen voorzien in de Wet op de Inlichtingen en veiligheidsdiensten en de in het Wetboek van Strafvordering gewijzigde bepalingen volgens de Wet Computercriminaliteit III.

[4] De politieke afspraken met betrekking tot de leveranciers en het aanschaffen van Hack software, die zijn gemaakt bij de invoering van de wet Computercriminaliteit III (CCIII), zullen naar verwachting 11.1
Leveranciers moeten worden gescreend door AIVD (alleen indien er geen dreiging is voor de nationale veiligheid), de leverancier mag niet leveren aan dubieuze regimes en de software

is nog nieuw, praktisch zeer moeilijk om blijvend de juiste software aan te kunnen schaffen. De bevoegdheid tot binnendringen is ook geen structurele oplossing voor het vraagstuk zoals die er nu is met de algemene verplichting voor telecommunicatiediensten om aftapbaar te zijn, cf hoofdstuk 13 van de Telecommunicatiewet. Het is een oplossing gericht op een specifiek geval en niet een 'ordenings' oplossing zoals nu voor het aftappen. 11.1 .

2. Veder is er in tegenstelling tot aanbieders van reguliere telecommunicatiediensten juridisch nog weinig geregeld ten aanzien van OTT diensten. In Nederland worden t.b.v. strafvordering in hoofdstuk 13 van de Telecommunicatiewet verplichtingen voor openbare telcommunicatienetwerken en -diensten geregeld. OTT diensten vallen daar niet onder.[5] Ze leveren echter wel dezelfde diensten/product aan de gebruiker. Er is kortom een 11.1 .

3. Een derde complicerende factor is dat deze communicatiediensten vaak softwarematig zijn en de dienstverlener zich zelden in Nederland bevindt, waardoor medewerkingsbereidheid voor het kunnen aftappen (en ontcijferen), opvragen van gegevens en het grensoverschrijdend kunnen afdwingen (rechtsmacht) geen zekerheid is.
   Omdat veel OTT diensten geen Nederlandse bedrijven zijn of zich in Nederland hebben gevestigd, ligt regulering op EU niveau voor de hand. Door de Europese Commissie is dan ook recent een nieuw wetsontwerp gemaakt om OTT diensten meer te reguleren, onder meer met het oogmerk om een gelijk speelveld te creëren. Deze voorgestelde wetgeving ziet echter alleen op ordeningsvraagstukken als consumentenbescherming en regelt niet de belangen van opsporings- en veiligheidsdiensten.[6] Uit het voorstel volgt dat lidstaten zelf in deze regulering voorzien. De

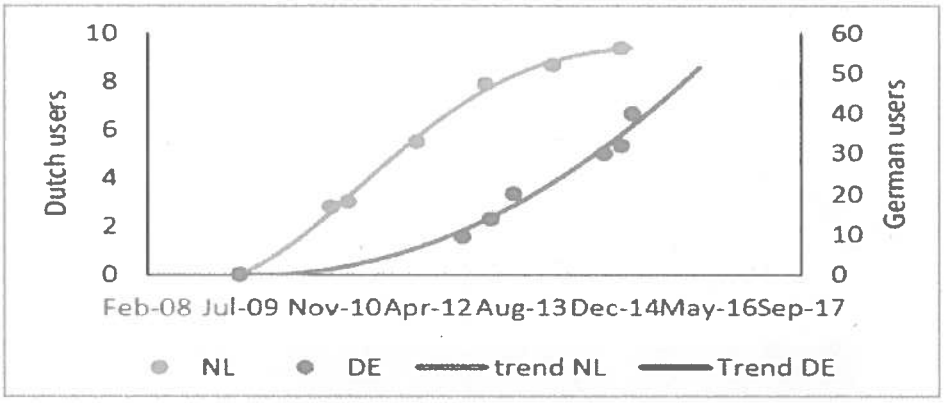
---

mag alleen in een specifieke zaak worden gebruikt/aangeschaft en dus niet generiek worden ingezet.

[5] NB: opsporingsbevoegdheden uit strafvordering zijn wel toepasbaar op OTT diensten.

[6] European Electronic Communications Code (EECC).

vraag is echter of 11.1 Om dit vraagstuk op te lossen is in het voorstel voor de e-evidence richtlijn door de EC gekozen om te werken met een legal representatives van bedrijven binnen de EU, waar verzoeken worden ingediend en de verplichtingen gehandhaafd kunnen worden.




figuur 1: aantal personen in miljoenen dat dagelijks WhatsApp gebruikt in NL en DE[7]

**Balans van gerechtvaardigde belangen**

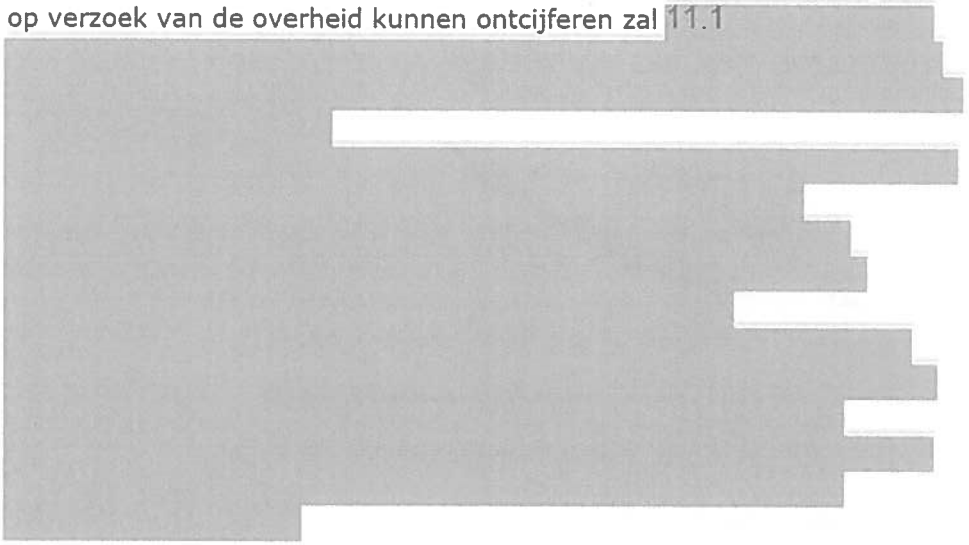
De uitdaging bij dit vraagstuk is er niet zozeer een van techniek: die schrijdt voort en daar waar nieuwe technische uitdagingen komen zijn ook altijd technische oplossingen te vinden. De essentie van het vraagstuk is het vinden en kunnen blijven bijstellen van de balans tussen de volgende belangen:

1. opsporing (dreiging, opsporing en inlichtingen);
2. privacy en beveiliging (encryptie ter beveiliging, proportionaliteit en subsidiariteit);
3. en economisch (concurrentie, bescherming van bedrijfsgevoelige gegevens, eerlijke markt met level playing field).

11.1

[7] Bron: TNO e.a. (2016). Study on future trends and business models in communication services. EU DG Home. Brussels.

11.1 . Het kabinet geeft daarin aan 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. De vraag of het belang van de opsporing bij het kunnen afluisteren van OTT diensten opweegt tegen het defacto verlangen dat aanbieders van OTT diensten hun diensten ten alle tijden op verzoek van de overheid kunnen ontcijferen zal 11.1

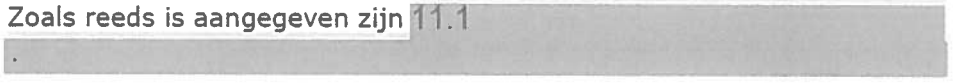


**Wat regelt CCIII wel en niet**

Met CCIII wordt geregeld dat daartoe aangewezen opsporingsambtenaren onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk kunnen binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Het binnendringen van een geautomatiseerd werk vindt plaats ter voorbereiding van onderzoekshandelingen in het opsporingsonderzoek 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.

Zoals reeds is aangegeven zijn 11.1



11.1 [redacted]

## Andere landen en de EU

België: Skype zaak

Volgens de Belgische overheid valt een OTT-dienst – aanbieden van een elektronische communicatiedienst op het grondgebied - onder de verplichtingen die in de Telecommunicatiewet worden gesteld, ook als deze alleen diensten aanbiedt in België en daar niet is gevestigd. Dat de telecomwet zo moet worden uitgelegd is recent, op 19 februari 2019, bevestigd in een arrest van het Hof van Cassatie (hoogste rechter). In deze casus ging het om het volgende: in een opsporingsonderzoek hebben de Belgische autoriteiten Skype gevraagd mee te werken aan het aftappen van gesprekken. Dit heeft het bedrijf geweigerd. Op basis daarvan is een strafrechtelijk onderzoek naar Skype ingesteld voor een mogelijke schending van de Telecommunicatiewet. Het arrest van de hoogste rechter in deze zaak komt er op neer dat Skype inderdaad mee had moeten werken aan een tap, ook al is het bedrijf niet in België gevestigd.[8]

Europese Unie

Ter verkenning van de uitwerking van de problematiek en de mogelijke oplossingen is door dgrr, samen met de politie en MIVD, een verkennend bezoek gebracht aan 10.2.a en 10.2.a . 11.1 [redacted]

In EU verband wordt wel gewerkt aan een voorstel dat inhoudelijke parallellen vertoont met het onderhavige onderwerp: de e-evidence richtlijn. Kort gezegd beoogt deze concept richtlijn te regelen dat opsporingsdiensten grensoverschrijdend en zonder rechtshulp digitaal bewijs kunnen vorderen bij aanbieders/houders van dat bewijs. Onder die richtlijn zullen ook OTT diensten vallen. 11.1 [redacted]

[8] Hof van Cassatie: Arrest (België). RG P.17.1229.N

Australische wet

Een recent in Australië aangenomen wet regelt dat aanbieders bij een verzoek van de autoriteiten medewerking moeten verlenen en de mogelijkheid moeten creëren om informatie te ontcijferen.[9]
Doel van de wet is om het probleem van "going dark" aan te pakken. Doordat mensen steeds meer gebruik maken van versleutelde (communicatie)diensten, hebben opsporings- en inlichtingendiensten minder toegang tot informatie. Na lange (politieke) discussie is de wet in de eerste week van december jl. aangenomen door het parlement.
Met deze wet kunnen opsporingsdiensten op drie manieren aanspraak maken op de hulp van bedrijven:

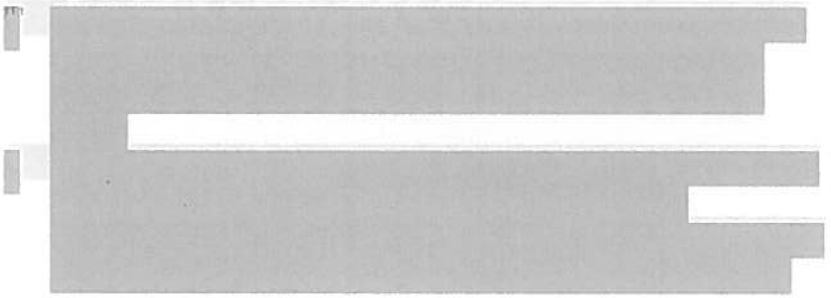
1. Technical assistance request: een opsporingsdienst doet een verzoek aan een bedrijf om bepaalde (versleutelde) informatie over te dragen.
2. Technical assistance notice: een opsporingsdienst dwingt een bedrijf om bepaalde (versleutelde) informatie over te dragen, waar het bedrijf al bij kan.
3. Technical capability notice: een opsporingsdienst dwingt een bedrijf om een capaciteit te ontwikkelen om de versleuteling van bepaalde informatie op te heffen en over te dragen.

Met andere woorden: bedrijven kunnen dus gedwongen worden om een programma te ontwikkelen dat de beveiliging van specifieke informatie op hun eigen product opheft. Dit mag niet leiden tot een 'systemic risk' – bedrijven kunnen niet gedwongen worden om iets te ontwikkelen wat de beveiliging van een hele categorie van hun producten aantast.

**Speelveld**

Hieronder worden de verschillende standpunten van de relevante partijen verwoord, die de waardespanning op enkele punten inzichtelijk maken:

- De bedrijven:



[9] Bron: Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018. A Bill for an Act to amend the law relating to telecommunications, computer access warrants and search warrants, and for other purposes.

- 11.1

- OM, IenV en opsporingsdiensten:
  - 11.1
- Cybersecurity
  - Door te eisen dat communicatie ontcijferd kan worden, kan van invloed zijn op de bescherming van de communicatie en privacy.
  - Het encryptiestandpunt is na intensief politiek-bestuurlijk overleg tot stand gekomen, vraag si of 11.1
- Economische Zaken
  - 11.1

**Advies:**

- Minister informeren over de problemen die het toegenomen gebruik van OTT diensten als communicatiemiddel opleveren voor de opsporing en het bewaken van onze nationale veiligheid en 11.1
- Voor te leggen dat er drie handelingsopties zijn, 11.1 11.1
  1. Een nationale wettelijke regeling die aanbieders van elektronische communicatiediensten verplicht om bij een vordering in het kader van opsporing of nationale veiligheid ontcijferd de inhoud van communicatie aan te kunnen leveren. Belangrijke uitdaging hierbij is het juridisch kunnen afbakenen welke diensten onder de noemer elektronische communicatiediensten vallen en welke niet. Daarnaast worden bedrijven met een dergelijke verplichting mogelijk indirect verplicht om encryptie aan te passen, hetgeen mogelijk indruist tegen de afspraken in het encryptiestandpunt van het Kabinet.

2. Een Europese regeling die de onder 2 benoemde verplichting regelt. 11.1 [redacted]
3. Verschuiving van de focus op de aanbieder van communicatiediensten naar de maker van apparaten waarmee wordt gecommuniceerd. Dit kan een grotere inbreuk op de privacy opleveren omdat daarmee een toegang wordt gecreëerd op een niveau (het apparaat) dat grotere consequenties heeft als daar misbruik van wordt gemaakt. 11.1 [redacted]
4. Niets doen op dit moment en wachten totdat zich andere landen op Europees niveau regelgeving gaan entameren en/of de keuze maken om het aftappen als opsporingsinstrument vele malen minder in te zetten. Dit vergt politieke acceptatie van de risico's en beperkingen bij de opsporing en bewaking van de nationale veiligheid.

NB: 11.1 [redacted]

Ministerie van Justitie en Veiligheid

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veilighe d
Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverhe d.nl/jenv

**Datum**
24 augustus 2019
**Ons kenmerk**

Cybercrime unit

# nota

Gespreksnota Interceptie OTT diensten

## 1. Doel nota

Doel van deze nota is om besluitvorming te krijgen op de handelingsoptie 11.1 voor het adresseren van de praktische problemen bij het aftappen, uitluisteren en opvragen van gegevens van elektronische communicatiediensten.

## 2. Aanleiding, gevraagde actie(s) en advies

De aard en omvang van elektronische communicatie tussen personen is in de afgelopen tien jaar snel veranderd. Zo maken we steeds meer gebruik van versleutelde over-the-top communicatiediensten (OTT), zoals WhatsApp. Het gebruik van gewone telefoniediensten voor spraak en tekstberichten neemt sterk af en de verwachting is dat over niet al te lange tijd (komende 5 jaar), zeker als 5G breed is geadopteerd, elektronische communicatie grotendeels via software over het datanetwerk (over-the-top) zal verlopen.

Dat elektronische communicatie grotendeels via software van OTT's verloopt heeft nadelige consequenties voor de aftap en uitluister mogelijkheden voor opsporings- en veiligheidsdiensten, alsook het opvragen van elektronische communicatie doordat:

- Dankzij End-to-end encryptie van berichtgeving dienstverleners zelf geen mogelijkheid meer hebben deze berichten te ontcijferen.
- De dienstverlener zich zelden in Nederland bevinden.
- Het juridisch kader voor aftap en uitluister bevoegdheden is geregeld voor (traditionele) telecommunicatiediensten en niet voor OTT's.

Tijdens departementale afstemming zijn enkele handelingsopties geïdentificeerd, 11.1

1. Een nationale wettelijke regeling die aanbieders van elektronische communicatiediensten verplicht om bij een vordering in het kader van opsporing of nationale veiligheid ontcijferd de inhoud van communicatie aan te kunnen leveren. Belangrijke uitdaging hierbij is het juridisch kunnen afbakenen welke diensten onder de noemer elektronische communicatiediensten vallen en welke niet. Daarnaast worden bedrijven met een dergelijke verplichting mogelijk indirect verplicht om encryptie aan te passen, hetgeen mogelijk indruist tegen de afspraken in het encryptiestandpunt van het Kabinet.

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
24 augustus 2019

**Ons kenmerk**

2. Een Europese regeling die verplichtingen OTT's regelt in lijn van de huidige verplichtingen die nu gelden voor telecommunicatiediensten. 11.1 [redacted]
3. Verschuiving van de focus op de aanbieder van communicatiediensten naar de maker van apparaten waarmee wordt gecommuniceerd. Dit kan een grotere inbreuk op de privacy opleveren omdat daarmee een toegang wordt gecreëerd op een niveau (het apparaat) dat grotere consequenties heeft als daar misbruik van wordt gemaakt. 11.1 [redacted]
4. Niets doen op dit moment en wachten totdat zich andere landen op Europees niveau regelgeving gaan entameren en/of de keuze maken om het aftappen als opsporingsinstrument vele malen minder in te zetten. Dit vergt politieke acceptatie van de risico's en beperkingen bij de opsporing en bewaking van de nationale veiligheid.

Het kiezen 11.1 [redacted] vraagt van uw departement om het initiatief te nemen 11.1 [redacted] die genoemd juridisch kader regelt.

## 3. Toelichting op het advies

Bij bovenstaand advies spelen vier overwegingen een rol.

*1. De noodzaak.* Deze toont zich in de toename van het gebruik van communicatie via software. Het gebruik van Whatsapp is bijvoorbeeld gegroeid van minimaal in juli 2009 tot rond de 10 miljoen gebruikers in december 2014.

2. *De waardenspanning.* Technisch kan allicht veel mogelijk zijn om het aftappen en afluisteren beter mogelijk te maken, maar rekening moet worden gehouden met gerechtvaardigde belangen:

A. opsporing (dreiging, opsporing en inlichtingen);
B. privacy en beveiliging (encryptie ter beveiliging, proportionaliteit en subsidiariteit);
C. en economisch (concurrentie, bescherming van bedrijfsgevoelige gegevens, eerlijke markt met level playing field).

11.1 [redacted]

3. *Welke alternatieven bestaan er?* Mogelijk kan worden gewezen naar de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk (CCIII). Hierbij wordt toegang verkregen tot het apparaat, dus voordat de end-to-end encryptie wordt toegepast. Dit is echter een zodanige specialistische bevoegdheid met een dermate hoge strafvordelijke drempel dat dit 11.1 [redacted].
Daarnaast bestaat de E-evidence verordening die nu wordt onderhandeld, deze

richt zich op opgeslagen data, niet 'stromende' data die nodig is voor de tap en afluisterbevoegdheid.

4. *Wat doen andere landen?* Volgens de Belgische overheid valt een OTT-dienst – aanbieden van een elektronische communicatiedienst op het grondgebied - onder de verplichtingen die in de Telecommunicatiewet worden gesteld, ook als deze alleen diensten aanbiedt in België en daar niet is gevestigd. Dit volgt uit het Skype arrest, dat erop neer komt dat Skype mee had moeten werken aan de tap (ook als het bedrijf niet in België was gevestigd.

10.2.a 11.1

Een recent in Australië aangenomen wet regelt dat aanbieders bij een verzoek van de autoriteiten medewerking moeten verlenen en de mogelijkheid moeten creëren om informatie te ontcijferen. Doel van de wet is om het probleem van "going dark" aan te pakken.

Voor een meer uitgebreide analyse verwijs ik u naar de bijlage.

## 4. Politieke en bestuurlijke context

De politieke en bestuurlijke context speelt met name een rol bij de waardespanning. Dit kan zich met name voordoen op de waarde van privacy en veiligheid gegeven de mogelijke gevolgen voor encryptie. Het huidige encryptiestandpunt van het kabinet houdt in 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. De vraag of het belang van de opsporing bij het kunnen afluisteren van OTT diensten opweegt tegen het defacto verlangen dat aanbieders van OTT diensten hun diensten ten alle tijden op verzoek van de overheid kunnen ontcijferen.

## 5. Communicatie

n.v.t.

## 6. Afstemming

Onderstaande nota is uitgewerkt conform het beleidsvoornemen dat in het jaarplan DGRR 2019 is opgenomen en is opgesteld door DRC (F&O en C&V) in samenwerking met politie, OM, bureau PIDS, EZK, AIVD, MIVD, NCTV en DGPenV. Het advies aan het einde van deze nota wordt door deze organisaties ambtelijk ondersteund.

Directoraat-Generaal
Rechtspleging en
Rechtshandhaving
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
24 augustus 2019

Ons kenmerk

## 7. Bijlagen

**1. Speelveld**
**2. Nadere probleem schets**
**3. Balans van gerechtvaardigde belangen**
**4. Andere landen en de EU**

## 1. Speelveld

Hieronder worden de verschillende standpunten van de relevante partijen verwoord, die de waardespanning op enkele punten inzichtelijk maken:

- De bedrijven:
  - 11.1
- OM, IenV en opsporingsdiensten:
  - 11.1
- Cybersecurity
  - Door te eisen dat communicatie ontcijferd kan worden, kan van invloed zijn op de bescherming van de communicatie en privacy.
  - Het encryptiestandpunt is na intensief politiek-bestuurlijk overleg tot stand gekomen, vraag si of 11.1
- Economische Zaken
  - 11.1

Directoraat-Generaal
Rechtspleging en
Rechtshandhaving
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Criminaliteit en Veiligheid

Datum
24 augustus 2019

Ons kenmerk

- 11.1 [redacted]

## 2. Nadere probleem schets

De geschetste ontwikkeling heeft een aantal consequenties voor de opsporing en het bewaken van de nationale veiligheid, die nu al een invloed hebben op de effectiviteit hiervan.

1. Allereerst maken veel OTT diensten gebruik van end-to-end encryptie: aanbieders van de diensten hebben in sommige gevallen dan zelf geen mogelijkheid meer om de berichten te ontcijferen, dat kan enkel door de zender en de ontvanger. Dat is goed voor de bescherming van inhoud en privacy, maar zorgt er ook voor dat de overheid bij een gerechtvaardigd belang de inhoud van de communicatie niet altijd meer kan inzien; tenzij een device zelf wordt binnengedrongen[1] door de overheid. De bevoegdheid tot binnendringen met gebruik van "hack software" is geregeld met de wet CCIII. Daar zijn hoge eisen gesteld. De devices bevatten veel persoonlijk materiaal, en eenmaal binnengedrongen kan veel meer dan alleen de communicatie over en OTT-dienst worden ingezien. Voorts zijn er strenge voorwaarde gesteld aan de leveranciers van software waarmee device gehackt kunnen worden door de overheid.[2] Daarmee wordt het naar verwachting, de bevoegdheid is nog nieuw, praktisch zeer moeilijk om blijvend de juiste software aan te kunnen schaffen. De bevoegdheid tot binnendringen is ook geen structurele oplossing voor het vraagstuk zoals die er nu is met de algemene verplichting voor telecommunicatiediensten om aftapbaar te zijn, cf hoofdstuk 13 van de Telecommunicatiewet. Het is een oplossing gericht op een specifiek geval en niet een 'ordenings' oplossing zoals nu voor het aftappen. 11.1 [redacted]

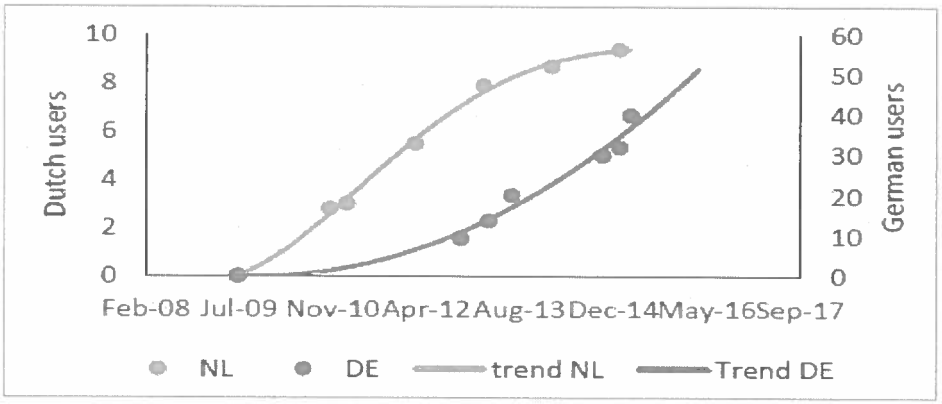
2. Veder is er in tegenstelling tot aanbieders van reguliere telecommunicatiediensten juridisch nog weinig geregeld ten aanzien van OTT diensten. In Nederland worden t.b.v. strafvordering in hoofdstuk 13 van de Telecommunicatiewet verplichtingen voor openbare telcommunicatienetwerken en -diensten geregeld. OTT diensten vallen

[1] Mogelijk in gevallen voorzien in de Wet op de Inlichtingen en veiligheidsdiensten en de in het Wetboek van Strafvordering gewijzigde bepalingen volgens de Wet Computercriminaliteit III.

[2] De politieke afspraken met betrekking tot de leveranciers en het aanschaffen van Hack software, die zijn gemaakt bij de invoering van de wet Computercriminaliteit III (CCIII). zullen naar verwachting 11.1 [redacted]
Leveranciers moeten worden gescreend door AIVD (alleen indien er geen dreiging is voor de nationale veiligheid). de leverancier mag niet leveren aan dubieuze regimes en de software mag alleen in een specifieke zaak worden gebruikt/aangeschaft en dus niet generiek worden ingezet.

daar niet onder.[3] Ze leveren echter wel dezelfde diensten/product aan de gebruiker. Er is kortom 11.1

3. Een derde complicerende factor is dat deze communicatiediensten vaak softwarematig zijn en de dienstverlener zich zelden in Nederland bevindt, waardoor medewerkingsbereidheid voor het kunnen aftappen (en ontcijferen), opvragen van gegevens en het grensoverschrijdend kunnen afdwingen (rechtsmacht) geen zekerheid is.
Omdat veel OTT diensten geen Nederlandse bedrijven zijn of zich in Nederland hebben gevestigd, 11.1
Door de Europese Commissie is dan ook recent een nieuw wetsontwerp gemaakt om OTT diensten meer te reguleren, onder meer met het oogmerk om een gelijk speelveld te creëren. Deze voorgestelde wetgeving ziet echter alleen op ordeningsvraagstukken als consumentenbescherming en regelt niet de belangen van opsporings- en veiligheidsdiensten.[4] Uit het voorstel volgt dat lidstaten zelf in deze regulering voorzien. De vraag is echter of 11.1 Om dit vraagstuk op te lossen is in het voorstel voor de e-evidence richtlijn door de EC gekozen om te werken met een legal representatives van bedrijven binnen de EU, waar verzoeken worden ingediend en de verplichtingen gehandhaafd kunnen worden.




figuur 1: aantal personen in miljoenen dat dagelijks WhatsApp gebruikt in NL en DE[5]

## 3. Balans van gerechtvaardigde belangen

Balans van gerechtvaardigde belangen

[3] NB: opsporingsbevoegdheden uit strafvordering zijn wel toepasbaar op OTT diensten.

[4] European Electronic Communications Code (EECC).

[5] Bron: TNO e.a. (2016), Study on future trends and business models in communication services, EU DG Home, Brussels.

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
24 augustus 2019

**Ons kenmerk**

De uitdaging bij dit vraagstuk is er niet zozeer een van techniek: die schrijdt voort en daar waar nieuwe technische uitdagingen komen zijn ook altijd technische oplossingen te vinden. De essentie van het vraagstuk is het vinden en kunnen blijven bijstellen van de balans tussen de volgende belangen:

1. opsporing (dreiging, opsporing en inlichtingen);
2. privacy en beveiliging (encryptie ter beveiliging, proportionaliteit en subsidiariteit);
3. en economisch (concurrentie, bescherming van bedrijfsgevoelige gegevens, eerlijke markt met level playing field).

11.1 Het kabinet geeft daarin aan 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. De vraag of het belang van de opsporing bij het kunnen afluisteren van OTT diensten opweegt tegen het defacto verlangen dat aanbieders van OTT diensten hun diensten ten alle tijden op verzoek van de overheid kunnen ontcijferen zal 11.1

## 4. Andere landen en de EU

België: Skype zaak

Volgens de Belgische overheid valt een OTT-dienst – aanbieden van een elektronische communicatiedienst op het grondgebied - onder de verplichtingen die in de Telecommunicatiewet worden gesteld, ook als deze alleen diensten aanbiedt in België en daar niet is gevestigd. Dat de telecomwet zo moet worden uitgelegd is recent, op 19 februari 2019, bevestigd in een arrest van het Hof van Cassatie (hoogste rechter). In deze casus ging het om het volgende: in een opsporingsonderzoek hebben de Belgische autoriteiten Skype gevraagd mee te werken aan het aftappen van gesprekken. Dit heeft het bedrijf geweigerd. Op basis daarvan is een strafrechtelijk onderzoek naar Skype ingesteld voor een mogelijke schending van de Telecommunicatiewet. Het arrest van de hoogste

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
24 augustus 2019

**Ons kenmerk**

rechter in deze zaak komt er op neer dat Skype inderdaad mee had moeten werken aan een tap, ook al is het bedrijf niet in België gevestigd.

Europese Unie
Ter verkenning van de uitwerking van de problematiek en de mogelijke oplossingen is door dgrr, samen met de politie en MIVD, een verkennend bezoek gebracht aan 10.2.a en 10.2.a . 11.1 [redacted].

In EU verband wordt wel gewerkt aan een voorstel dat inhoudelijke parallellen vertoont met het onderhavige onderwerp: de e-evidence richtlijn. Kort gezegd beoogt deze concept richtlijn te regelen dat opsporingsdiensten grensoverschrijdend en zonder rechtshulp digitaal bewijs kunnen vorderen bij aanbieders/houders van dat bewijs. Onder die richtlijn zullen ook OTT diensten vallen. 11.1 [redacted]

Australische wet
Een recent in Australië aangenomen wet regelt dat aanbieders bij een verzoek van de autoriteiten medewerking moeten verlenen en de mogelijkheid moeten creëren om informatie te ontcijferen.
Doel van de wet is om het probleem van "going dark" aan te pakken. Doordat mensen steeds meer gebruik maken van versleutelde (communicatie)diensten, hebben opsporings- en inlichtingendiensten minder toegang tot informatie. Na lange (politieke) discussie is de wet in de eerste week van december jl. aangenomen door het parlement.
Met deze wet kunnen opsporingsdiensten op drie manieren aanspraak maken op de hulp van bedrijven:

1. Technical assistance request: een opsporingsdienst doet een verzoek aan een bedrijf om bepaalde (versleutelde) informatie over te dragen.
2. Technical assistance notice: een opsporingsdienst dwingt een bedrijf om bepaalde (versleutelde) informatie over te dragen, waar het bedrijf al bij kan.
3. Technical capability notice: een opsporingsdienst dwingt een bedrijf om een capaciteit te ontwikkelen om de versleuteling van bepaalde informatie op te heffen en over te dragen.

Met andere woorden: bedrijven kunnen dus gedwongen worden om een programma te ontwikkelen dat de beveiliging van specifieke informatie op hun eigen product opheft. Dit mag niet leiden tot een 'systemic risk' – bedrijven kunnen niet gedwongen worden om iets te ontwikkelen wat de beveiliging van een hele categorie van hun producten aantast.

## Input interview Nieuwsuur – kabinetsstandpunt Encryptie

1) Spreeklijn:

- Afweging tussen het belang van digitale veiligheid en het belang van opsporing is een kwetsbaar en complex dilemma.
- Sociale media platformen (zoals Facebook) hebben daarin een bijzondere verantwoordelijkheid. Ze moeten zorgen voor een evenwichtig beleid waarbij beide belangen worden bediend.
- Het opsporingsbelang is *geen sluitstuk*: het besluit van Facebook om encryptie in te voeren, moet hand in hand gaan met handelingsperspectief om opsporingsdiensten te blijven helpen.
- Wanneer dit evenwicht bewaard blijft, wordt het internet geen vrijplaats voor criminelen en blijft het een omgeving waar elke Nederlander zich graag en veilig op begeeft.

2) Benadrukken:

- Er bestaat een maatschappelijk opsporingsbelang en encryptie bemoeilijkt de uitvoering van deze wettelijke taak.
  -encryptie maakt vaak integraal deel uit van de internetdiensten, het breken van versleuteling is in steeds minder gevallen mogelijk en ontsleutelde gegevens zijn steeds minder beschikbaar bij het ICT-bedrijf.
  -Dat bemoeilijkt, vertraagt, of maakt het onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de opsporing van strafbare feiten.

- Er is een effectieve en rechtmatige toegang tot gegevens voor de opsporing nodig.
  -Noodzakelijk voor de fysieke en digitale veiligheid.
  -Encryptie vormt hierin een belemmering, bijv de gevolgen van encryptie voor de bestrijding van kinderporno: Een flinke afname van het aantal meldingen over kinderpornografische content (Facebook meldt nu als één van de besten. Een halvering van het aantal meldingen is denkbaar).

- Oplossingen voor een effectieve en rechtmatige toegang moeten in gezamenlijkheid worden vormgegeven.
  -Aanbieders van ICT-producten en –diensten,
  -De opsporings-, inlichtingen-, en veiligheidsdiensten,
  -In overleg met de NCTV en andere vakdepartementen.

- Initiatief voor de oplossing ligt bij de ICT-bedrijven.

- Het belang van encryptie voor cybersecurity, de persoonlijke levenssfeer en de digitale economie
  -Communicatie en dienstverlening tussen overheid, bedrijf en burger (digID, belastingaangiftes)
  -Vertrouwelijkheid van communicatie (vrijheid van meningsuiting en communicatie journalisten)
  -Vertrouwen in veilige communicatie en opslag van data is essentieel voor de groeipotentie van de Nederlandse economie

3) Vermijden:

- 11.1 [redacted]

## QenA

### End-to-end encryptie: Wat zijn de gevolgen voor de bestrijding van kinderporno?

De politie ziet gebruik op grote schaal van de verschillende chat- en messenger applicaties voor het delen van strafbaar materiaal. De gevolgen van encryptie voor de bestrijding van kinderporno:

- Een flinke afname van het aantal meldingen over kinderpornografische content (Facebook meldt nu als één van de besten. Een halvering van het aantal meldingen is denkbaar).
- Een verslechtering van de informatiepositie van politierechercheurs. Bijvoorbeeld slechtere vroeg-signalering van verdachten.
- Vertraging bij het in kaart brengen van slachtoffers.
- Het bemoeilijkt het vinden van daders.

Dit geldt voor de bestrijding van kinderporno, maar ook voor bijvoorbeeld wapenhandel.

### Ontwikkeling van meldingen bij politie/OM

In de laatste jaren nam het totaal aantal meldingen van online seksueel misbruik en kinderpornografie bij politie/OM explosief toe:

- Van ruim 5000 in 2015
- Naar ruim 30.000 in 2018

Ten opzichte van 2017 is de instroom van het aantal meldingen bij politie/OM gestegen met 69%.

Een belangrijke oorzaak van de stijging van het werkaanbod is volgens politie/OM onder meer de digitalisering van het leven mondiaal en het feit dat iedereen 27/7 online is en er dus steeds meer communicatie op het internet is.

In 2018 hebben de politieteams die kinderporno bestrijden 636 interventies uitgevoerd en 185 misbruikte kinderen geïdentificeerd.

## Achtergrond: Kabinetsstandpunt encryptie 4 januari 2016

Conclusie: het kabinet is 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.

De opsporing in het kabinetsstandpunt: opsporings-, inlichtingen- en veiligheidsdiensten

- De bevoegdheden en middelen moeten toegerust zijn op de huidige en toekomstige digitale realiteit.
    - Met effectieve, rechtmatige toegang tot gegevens wordt de veiligheid van de digitale en de fysieke wereld bevorderd

- Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporingsdiensten bij de toegang tot die gegevens.
    - Bijvoorbeeld bij onderzoek naar de verspreiding en opslag van kinderporno,
    - het tegengaan van cyberaanvallen of
    - het voorbereiden van aanslagen door terroristen.

- Het breken van versleuteling is in steeds minder gevallen mogelijk en ontsleutelde gegevens zijn steeds minder vaak bij de dienstverlener beschikbaar. Deze ontwikkelingen nopen tot het zoeken naar nieuwe oplossingen gelet op het belang van de opsporing
    - Gegeven de afhankelijkheid van aanbieder van ICT-producten en diensten, is overleg nodig over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden.

Overwegingen: Cybersecurity, Economische Zaken en Buitenlandse Zaken

- Cybersecuritymaatregelen in organisaties, bijvoorbeeld
    - De veilige opslag van wachtwoorden
    - en het veilig bewaren van backups

- Communicatie en dienstverlening van de overheid met de burgers en bedrijven waarbij vertrouwelijke gegevens worden uitgewisseld, bijvoorbeeld
    - het gebruik van DigiD of
    - het doen van belastingaangifte.

- De eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers, het
    - beschermt de vertrouwelijkheid en integriteit van persoonsgegevens en communicatie
    - is 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.

- De digitale economie,
    - bedrijfsinformatie veilig bewaren en versturen
    - Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie

Ministerie van Justitie en Veiligheid

MJenV

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veilighe d

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverhe d.nl/jenv

**Contactpersoon**
10.2 e
*beleidsadviseur*

T 070 10.2 e
F 070 370 79 00

**Datum**
4 november 2019

**Ons kenmerk**
2742373

# nota

Gespreksnotitie encryptie en OTT

## 1 Doel nota

Akkoord op het traject om te komen tot inzicht in (end-to-end) versleutelde gegevens.

## 2 Aanleiding, gevraagde actie(s) en advies

Op 3 november jl. heeft u in Nieuwsuur te kennen gegeven om te komen tot een ontsleutelplicht voor Over The Top(OTT) diensten als Facebook. In het DGRR stafoverleg van 4 november jl. heeft u aangegeven verder te willen spreken over een ontsleutelplicht. Hoe deze ontsleutelplicht vorm zou krijgen is afhankelijk van de gesprekken die zullen worden gevoerd.

U wordt geadviseerd opdracht te geven om

1. Op ambtelijk niveau in gesprek te gaan met relevante private partijen over een juridische verplichting voor OTT-diensten om gegevens ontsleuteld aan te kunnen leveren, waarbij de technische mogelijkheden hiervoor gezamenlijk worden verkend.
2. De partners van het kabinetsstandpunt encryptie van januari 2016 (AIVD, MIVD, BZ, BZK, DEF, OM, Politie, PIDS) te informeren over het traject. Na de inventarisatie wordt het gesprek aangegaan of een mogelijke herijking/ interpretatie van het standpunt en de belangenweging aangewezen is. In het bijzonder gaat het om interpretatie van 'beperkende wettelijke maatregelen ten aanzien van het gebruik van encryptie,' 'verzwakking in algemene zin' en in hoeverre sleutelmanagement binnen de scope van het standpunt valt;
3. Te blijven inzetten op regelgeving op Europees niveau voor de opsporing van diverse strafbare feiten, waaronder kinderporno;
4. De lopende inventarisatie van de wenselijkheid van een Europese aanpak in enkele grotere EU-lidstaten voort te zetten. Een gezamenlijke aanpak vergroot de slagingskans.
5. Ook de VS te bevragen over mogelijke en wenselijke oplossingen.

Dit beleidsveld kent vele publieke en private belangen waardoor ambitieus én behoedzaam vormgegeven wordt aan een ontsleutelplicht. In het stafoverleg heeft u aangegeven verder te willen praten over de materieel strafrechtelijke reikwijdte en mogelijke middelen om tot de ontsleuteling te komen.

Materieel strafrechtelijke reikwijdte: 11.1

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
4 november 2019

**Ons kenmerk**
2742373

11.1 [redacted]

Middel: Bij de keuze van het middel geldt als uitgangspunt dat encryptie niet structureel verzwakt mag worden, maar ontsleutelde gegevens worden verkregen in het specifieke geval. Hoe hier het beste vorm aan kan worden gegeven moet blijken uit een sonderingsronde langs de Over The Top diensten, andere partners en andere lidstaten. Er is reeds contact met collega's uit 10.2.a en 10.2.a die ook zelfstandig bezig zijn met interceptie van OTT's. Gezamenlijke dilemma's als decryptie, effectiviteit, level playing field, en handhaafbaarheid zouden ook gezamenlijk kunnen worden opgelost. Dit vergroot de slagingskans. Relevant is daarbij dat het creëren van een ontsleutelplicht voor niet in Nederland gehuisveste bedrijven, daarmee tegelijk voor alle (buitenlandse) mogendheden ter beschikking komt, onafhankelijk van evt. nationale beperkingen tot bepaalde delicten. Dit is een verschil tussen reguliere telco's (gehuisvest in NL/EU) en OTTs die wereldwijd hun diensten leveren. Het doel staat centraal: toegang verkrijgen tot ontsleutelde data.

## 3 Toelichting op het advies

In deze discussie komen een aantal trajecten samen.

- Op 2 oktober heeft u met DRC en de NCTV de interceptie van OTT diensten besproken. Deze interceptie heeft alleen zin als de informatie ontsleuteld toegankelijk is. In dit overleg heeft u aangegeven om Europees te inventariseren of er behoefte is aan een Europese aanpak.
- Op 4 oktober stuurden de Britse Secretary of State for the Home Department, de Amerikaanse Attorney General en Secretary of Homeland Security en de Australische Minister for Home Affairs een open brief aan Facebook met de oproep om toegang te blijven behouden tot gegevens, vooral ten behoeve van de strijd tegen kinderporno. In de brief is aangegeven dat de technische experts van de overheid er vertrouwen in hebben dat een oplossing kan worden gevonden waarbij de cyber security wordt beschermd en technologische innovatie wordt ondersteund.
- Op 4 januari 2016 hebben de Minister van Veiligheid en Justitie en de Minister van Economische Zaken het kabinetsstandpunt over encryptie aan de Kamer gestuurd. Het standpunt stelt dat het niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. Hierin worden het belang van nationale veiligheid, cyber security, privacy, en het belang van de opsporing en I&V diensten in de uitvoering van hun wettelijke taak allen erkend. Overleg met ICT-bedrijven is nodig om te komen tot een oplossing.
- Verder loopt uw programmatische aanpak van kinderporno, waarin verschillende PPS-acties en een bestuursrechtelijk traject samenkomen.

De belangen waarmee rekening wordt gehouden betreffen:

- 11.1 [redacted]

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
4 november 2019

**Ons kenmerk**
2742373

11.1 [redacted]

Met het traject om te komen tot een ontsleutelrecht wordt invulling gegeven aan de oproep in het kabinetsstandpunt om ten behoeve van de opsporing- en I&V diensten oplossingen te vinden bij de uitvoering van de wettelijke taak en in samenwerking met de ICT-bedrijven.

## 4 Dilemma's

Het algemene beleid van JenV is er altijd op gericht geweest dat de afscherming van communicatie belangrijk is, maar niet absoluut. 11.1 [redacted]

Communicatienetwerken en -diensten die in Nederland worden aangeboden zouden daarom te bevragen moeten zijn en leesbare resultaten moeten produceren. Het kabinetsstandpunt staat hier niet bij voorbaat aan in de weg, als het maar niet de ontwikkeling, beschikbaarheid en het gebruik van encryptie structureel belemmert. Of het kabinetsstandpunt moet worden herijkt hangt af van de uitkomst van de inventarisatie.

Gezien het internationale karakter van het internet is het voor criminelen mogelijk een wettelijke regeling te omzeilen door te kiezen voor OTT-diensten die vanuit het buitenland worden aangeboden. Door (ook) regelgeving op EU-niveau aan te nemen kunnen dergelijke uitwijkmogelijkheden worden beperkt. Idealiter voeren andere landen van waaruit veel OTT-diensten worden aangeboden, zoals de VS, soortgelijke regelgeving in. Het volledig uitsluiten van de uitwijkmogelijkheden is naar verwachting niet mogelijk. OTT-diensten die moedwillig criminaliteit faciliteren kunnen kiezen voor landen waar de overheid geen maatregelen neemt. Bovendien blijft er software die vrij beschikbaar is (open source) bestaan op basis waarvan personen (en criminelen) hun eigen private communicatie ook end-to-end kunnen versleutelen, en criminele communicatie kan zich dan verplaatsen van de openbare OTTs naar private netwerken.

## 5 Politieke en bestuurlijke context

D66 is een bevlogen voorvechter van encryptie en is zeer alert op voorstellen die aan het encryptiestandpunt raken. In de nota zijn reeds de interdepartementale belangen geschetst. Verder heeft u ook aangegeven dit onderwerp te willen bespreken tijdens uw werkbezoek aan de VS.

U kunt ook overwegen om een werkbezoek te brengen aan de politie (Amsterdam). Hierbij kan interceptie centraal staan waarbij ook de problematiek van interceptie van OTT diensten in de praktijk kan worden getoond en de werking verder beschreven.

## 6 Communicatie

Geen, de nota wordt wel gedeeld met DCOM.

## 7 Afstemming

In deze instantie is deze memo intern JenV afgestemd met de NCTV en DWJZ. Na het gesprek zullen andere partners worden aangeschreven. AIVD, MIVD, BZ, BZK, DEF, OM, Politie, PIDS zullen over dit traject worden geïnformeerd. Het voorstel is om de inventarisatie van oplossingen ook met partners te bespreken en de uitkomsten ervan met hen af te stemmen t.b.v. bespreking met u en in de relevante onderraad/ -raden.

## 8 Bijlagen

Geen.

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veiligheid

**Datum**
4 november 2019

**Ons kenmerk**
2742373

# 1. Oplegger Mondelinge Vraag

| | |
|---|---|
| **Onderwerp:** Encryptie en het opsporingsbelang: 'Minister bezorgd om versleuteling Facebook'.<br>**Bewindspersoon:** MRB, in afwezigheid van MJenV<br>**Naam dossierhouder:** 10.2.e<br>**Telefoonnummer en e-mailadres dossierhouder:** 10.2.e @minjenv.nl | |
| Kern van het mediabericht | Facebook wil zijn chatdienst en Instagram net zo beschermen als zijn andere dienst WhatsApp (end-to-end encryption). De Amerikaanse minister van Justitie, samen met zijn collega's uit het VK en Australië, vreest dat dit criminelen in de kaart speelt. De MJenV vindt de zorg begrijpelijk en heeft gesteld dat privacy nooit een schil mag worden voor criminelen. Hij gaat dit bespreken met zijn collega in Washington en met internetbedrijven. |
| Kernboodschap van de bewindspersoon | • Het encryptiestandpunt wordt gevolgd, dit sluit niet uit dat gesproken kan worden met internetbedrijven over mogelijkheden om negatieve effecten te beperken voor opsporings-, inlichtingen- en veiligheidsdiensten. |
| Argumentatie | • Erkennen van de spanning tussen het belang van encryptie en het belang van opsporings-, inlichtingen- en veiligheidsdiesnten (cf encryptiestandpunt).<br>• Begrip tonen voor de eventuele oproep vanuit de VS aan Facebook om met de publieke autoriteiten om tafel te gaan en te zoeken naar een oplossing. Ook dit is mogelijk onder het huidige standpunt, zo lang het niet de veiligheid van digitale systemen en van encryptie compromiteert.<br>• Onderstrepen van het kabinetsstandpunt: het kabinet vindt het op dit moment nog steeds niet wenselijk om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.<br>• Herhalen van het uitgangspunt van MJenV: Privacy mag nooit het schild worden van criminelen. |
| Feiten en cijfers | • Encryptie wordt steeds meer toegepast en is belangrijk voor het vertrouwen in digitale producten en diensten en voor de Nederlandse economie in snel ontwikkelende digitale maatschappij<br>• Encryptie vormt een belemmering voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer kwaadwillenden hiervan gebruikmaken.<br>• Overleg is nodig met aanbieders over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.<br>• In de tijd van schrijven van het standpunt was er geen zicht op mogelijkheden die in algemene zin encryptieproducten te verzwakken zonder daarmee de veiligheid van digitale systemen en van encryptie gebruik te maken te comprimenteren. Dit lijkt vooralsnog onveranderd.<br>• Het encryptiestandpunt beperkt zich tot het nemen van wettelijke maatregelen waarbij ook is aangegeven dat het 'op dit moment' niet wenselijk is. Dit wordt op dit moment nog steeds onderschreven. |
| Politieke afspraken | Het kabinetsstandpunt dateert van 4 januari 2016 en is daarmee totstandgekomen onder Rutte II, het is nog wel staand beleid. D66 is de meest uitgesproken voorstander voor sterke encryptie. De toenmalige bewindspersonen (Van der Steur en Kamp) weerspreken het gerechtvaardigd belang van opsporingsdiensten niet, maar verkozen het belang van een sterke encryptie. |
| Overig | • Er is **geen** officiele versie van de brief bekend.<br>• De MJenV heeft begrip getoond voor het initiatief van de VS en aangegeven dit met hen te bespreken tijdens zijn werkbezoek naar de VS.<br>• Dit kabinet is geen voorstander van achterdeurtjes die encryptie verzwakken.<br>• Dit kabinet kan wel de roep ondersteunen om met internetdienstverleners in gesprek te gaan over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden.<br>• Het belang van opsporings-, inlichtingen- en veiligheidsdiensten wordt samen genomen, u kunt zich beperken tot de opsporing. |

## 2. Spreektekst

- In onze digitale samenleving staan vaak vier waarden centraal: 1. het opsporingsbelang, 2. het veiligheid belang, 3. het economisch belang en 4. mensenrechten.

- Bij het aanpassen van wet- en regelgeving moeten deze belangen tegen elkaar worden afgewogen.

- In het kabinetsstandpunt van 2016 inzake encryptie is dit gebeurd:
    - Ja, encryptie belemmert het verkrijgen van informatie die noodzakelijk is voor opsporingsdiensten wanneer kwaadwillenden hiervan gebruik maken.
    - Maar tevens is encryptie van belang voor het vertrouwen in digitale producten en diensten.
    - Daarop is besloten geen beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, beschikbaarheid en gebruik van encryptie binnen Nederland. Dit is nog steeds staand beleid.

- Om de balans te behouden is het belang van de opsporing in het kabinetsstandpunt erkend:
    - De noodzaak tot rechtmatige toegang tot gegevens en communicatie wordt onderstreept.
    - De steeds sterkere encryptie en het steeds grootschaligere gebruik, noopt tot het zoeken naar oplossingen.
    - Hierbij wordt het gesprek met internetbedrijven aangemoedigd.

- In de woorden van mijn collega: *"Privacy mag geen schild worden voor criminelen"*
- Wanneer dit gebeurt is de balans zoek.

- Het gesprek over oplossingen moet niet worden verstomd en het zoeken naar oplossingen niet worden gestaakt.
- Zolang deze oplossingen de veiligheid van digitale systemen die van encryptie gebruik maken niet schaden.

- Daarom herhaal ik het begrip dat mijn collega heeft uitgesproken voor de uitnodiging van het Amerikaanse ministerie van Justitie om samen met de private sector tot oplossingen te komen.

# 3. Factsheet

3.1 Het kabinetsstandpunt encryptie

| | |
|---|---|
| Encryptie stelt 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. Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Dit komt de volgende toepassingen ten goede: | |
| 1. | De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups. |
| 2. | Overheidscommunicatie met haar burgers en diensten waarbij vertrouwelijke gegevens worden uitgewisseld |
| 3. | De bescherming van de communicatie binnen de overheid (diplomatiek berichtenverkeer en militaire communicatie) |
| 4. | Veilig te kunnen bewaren en versturen van bedrijfsinformatie. Encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat. |
| 5. | Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers |

| | |
|---|---|
| Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die gegevens. Dit kan worden onderverdeeld in: | |
| 1. | Belemmeringen wanneer opsporings-, inlichtingen- en veiligheidsdiensten 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. |
| 2. | Criminelen, terroristen en tegenstanders in gewapende conflicten hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. |
| 3. | Het 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. |
| 4. | Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook Criminelen, terroristen en tegenstanders in gewapende conflicten gebruik kunnen maken. |

| | |
|---|---|
| Conclusie: | |
| 1. | 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. |
| 2. | 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. |
| 3. | 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. |
| 4. | 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. |

3.2 Brief van het Amerikaanse Ministerie van Justitie

- Er is geen officiële versie van de brief beschikbaar, alleen een gelekt concept.
- Het concept spreekt zich uit vóór encryptie, inclusief de toegevoegde waarde voor de veiligheid van diensten als het bankwezen, commerciële activiteiten en communicatie. Alswel de gerechtvaardigde verwachting van burgers dat hun privacy wordt beschermd.
- Ook wordt benoemd dat het beter beveiligen van de digitale wereld de daadwerkelijke samenleving meer kwetsbaar kan maken.
- Er wordt opgeroepen tot een balans tussen het beschermen van data en de maatschappelijke veiligheid waarbij misdrijven moeten kunnen worden onderzocht en toekomstige misdrijven moet worden voorkomen.
- Bedrijven zouden geen systemen moeten ontwerpen waarbij enige vorm van toegang tot gegevens wordt geblokkeerd. Dit maakt burgers kwetsbaar, maar kan ook de mogelijkheid van het bedrijf schaden om misdrijven te detecteren en daarop te acteren. Misdrijven die worden genoemd zijn: kinderporno, terrorisme en ongewenste buitenlandse beïnvloeding.
- Het schaadt ook de opsporing naar deze en andere serieuze misdrijven.
- In de brief wordt de samenwerking met Facebook ook geroemd:

| **Samenwerking met het US National Center for Missing & Exploited Children' (NCMEC) in 2018** | |
|---|---|
| 16.8 miljoen meldingen | Van Facebook aan NCMEC (meer dan 90% van het totaal aantal meldingen dat jaar) |
| 8.000 meldingen | Van pogingen voor grooming, sexting of ontmoetingen. |
| 2.500 arrestaties | In het Verenigd Koninkrijk (geschat door de National Crime Agency) |
| 3.000 kinderen veiliggesteld | In het Verenigd Koninkrijk (geschat door de National Crime Agency) |
| **Uit het Transparency report van Facebook** | |
| 26 miljoen berichten over terrorist content | Hierop heeft Facebook geacteerd tussen oktober 2017 en maart 2019 |
| | |
| 99% van de gevallen waarin Facebook actie onderneemt gebeurt dit doordat de dreiging is erkend door Facebook zijn eigen veiligheidssysteem, niet meldingen van gebruikers. Bij end-to-end encryptie verliest het bedrijf dus inzicht in deze data. NCMEC schat in dat 70% van de meldingen (12 miljoen wereldwijd) verloren gaan. | |

| Facebook wordt opgeroepen om: | Waardering van de aanbevelingen |
|---|---|
| *Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;* | 11.1 [redacted] |
| *Enable law enforcement to obtain lawful access to content in a readable and usable format;* | 11.1 [redacted] |
| *Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and* | 11.1 [redacted] |
| *Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.* | 11.1 [redacted] |

## 4. Questions and Answers

**Q: Onderschrijft de minister het kabinetsstandpunt inzake encryptie?**

A: Ja, 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, bedrijven, en burgers,
- en voor de Nederlandse economie.

Maar blijft ook oog hebben voor de effecten die dit heeft op de opsporings-, inlichtingen- en veiligheidsdiensten.

**Q: Hoe verhouden de uitlatingen van de MJenV zich tot het kabinetsstandpunt van encryptie.**

A: Minister Grapperhaus heeft begrip getoond voor de zorgen van de Amerikanen, Britten en Australiërs voor de opsporing wanneer Facebook twee andere diensten end-to-end encrypt.

Wanneer privacy een schild wordt voor criminelen is dit zorgelijk. Het zijn ernstige strafbare feiten waarvan de opsporing wordt bemoeilijkt: kinderporno, terrorisme en zware criminaliteit.

In de conceptbrief wordt opgeroepen om:
1)het maatschappelijk effect van dit soort beslissingen mee te wegen in de besluitvorming en
2) in gesprek te gaan over mogelijkheden om het negatief effect op de opsporing tot een minimum beperken.

Deze dialoog en het gezamenlijk vinden van oplossingen juich ik van harte toe, binnen het kader van het encryptiestandpunt.

In dit licht lees ik de conceptbrief.

**Q: wat wordt de inzet van de MJenV richting zijn collega's in Washington?**

**A:** Onderdeel van het kabinetsstandpunt is ook dat het encryptiestandpunt internationaal wordt uitgedragen.

Ik kan mij niet anders voorstellen dat mijn collega zich aan het kabinetsstandpunt houdt.

**Q: Kunt u aangeven welke 'oplossingen voor encryptie' u wél acceptabel vindt.**

**A:** Op dit moment heb ik ook nog niet de oplossing.

Ik juich de dialoog van harte toe en zal de uitkomsten beoordelen aan de hand van het encryptiestandpunten.

5. Relevante achtergrondinformatie

-het mediabericht

-het kabinetsstandpunt encryptie

-het gelekte concept van het Amerikaanse ministerie van Justitie

-Tweet het lid Verhoeven:

Actualiteit Facebook en encryptie
**Achtergrond:**

Het lid Verhoeven heeft op 7 okt jl. een Mondelinge vraag gesteld over het bericht: 'Minister bezorgd om versleuteling Facebook', nadat deze Mondelinge vraag niet is goedgekeurd zijn 9 okt. jl. schriftelijke vragen ontvangen.

**Kern:**

Het lid maakt zich zorgen over effecten die het initiatief van de VS, VK en AUS kan hebben op encryptie. Hij vraagt zich af hoe uw 'begrip' voor dit initiatief zich verhoudt tot het Nederlandse encryptiestandpunt en wat de inzet wordt van het gesprek dat u gaat voeren in Washington.

## Spreeklijn:

Ik onderschrijf het encryptiestandpunt. Ik erken het belang van encryptie voor de veiligheid van digitale communicatie tussen overheid, bedrijf en burger, en de bescherming van de persoonlijke levenssfeer.

Echter, zoals ook helder in het encryptiestandpunt is verwoord, zijn de effecten op de opsporingscapaciteit niet gering. Zeker niet wanneer je beseft dat het opsporingsonderzoeken naar kinderporno, contra terrorisme en zware criminaliteit raakt. Alsook de I&V diensten.

Daarom sluit het encryptiestandpunt het zoeken naar oplossingen niet uit en wordt het gesprek met bedrijven aangemoedigd, zolang het maar niet de encryptie structureel verslechtert.

Ik ben nog steeds tegen achterdeurtjes in encryptie, ik wil geen beperkende wettelijke maatregelen ten aanzien van de ontwikkeling, de

beschikbaarheid en het gebruik van encryptie binnen Nederland.

Ik hoor wel graag wanneer er oplossingen beschikbaar zijn die in lijn zijn met het encryptiestandpunt.

# Interceptie en OTT

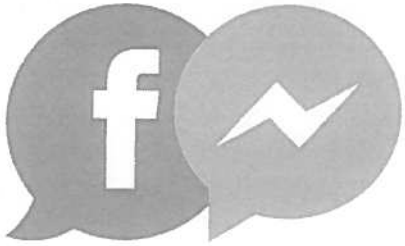
# Interceptie in de opsporing

| Indicatoren Unit Landelijke interceptie | | | | | | |
|---|---|---|---|---|---|---|
| | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** |
| Aantal nummers waarvoor een bevel tot aftappen is gegeven | 26.150 | 25.181 | 24.063 | 24.850 | 24.900 | 23.458 |
| Gemiddeld aantal taps per dag | 1.391 | 1.386 | 1.415 | 1.423 | 1.421 | 1.397 |

# *Over-the-top* (OTT) diensten

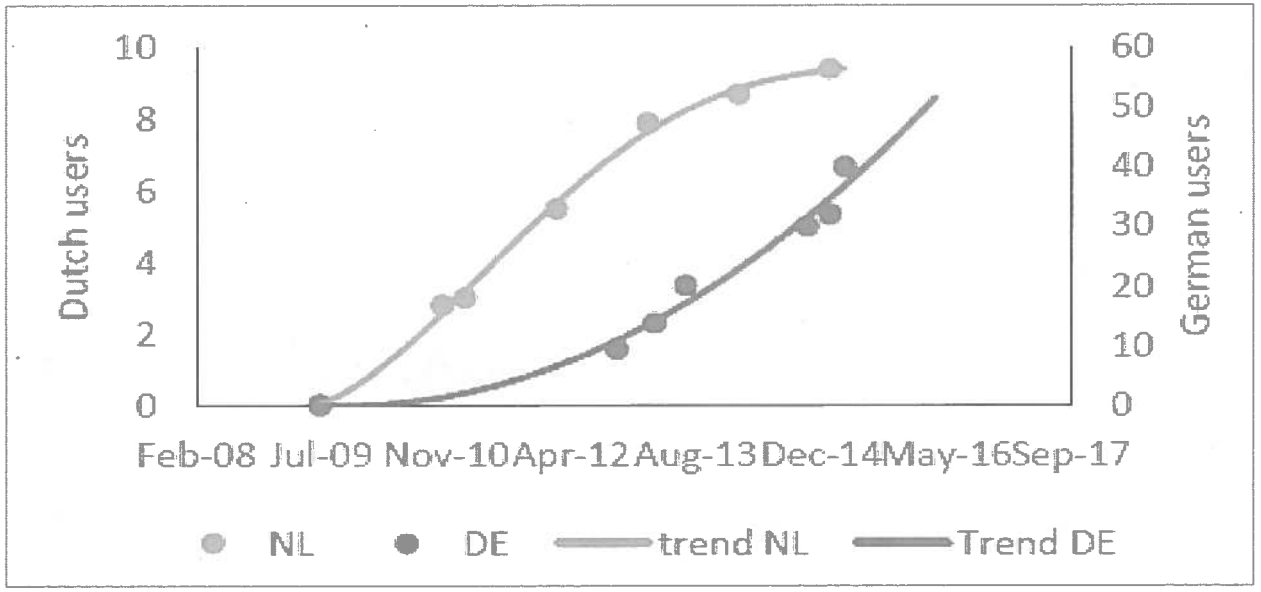




# Voorbeeld ontwikkeling OTT gebruik

- Gebruikers van Whatsapp



# Waarom een probleem?

- End-to-end encryptie
- Aanbieder zelden in NL
- Juridisch kader voor (traditionele) telecomaanbieders ≠ OTT's

# Handelingsopties

- Een nationale wettelijke regeling
- Een Europese regeling
- Verandering focus van aanbieder naar maker van de apparaten
- Niets doen

# Overwegingen

- De noodzaak
- De waardenspanning
- Welke alternatieven
- Wat doen andere landen

# De waardenspanning

## Opsporing

dreiging, opsporing en inlichtingen

## Privacy en beveiliging

encryptie ter beveiliging, proportionaliteit en subsidiariteit

## Economie

concurrentie, eerlijke markt met level playing field

# Alternatieven?

- CCIII
- E-evidence

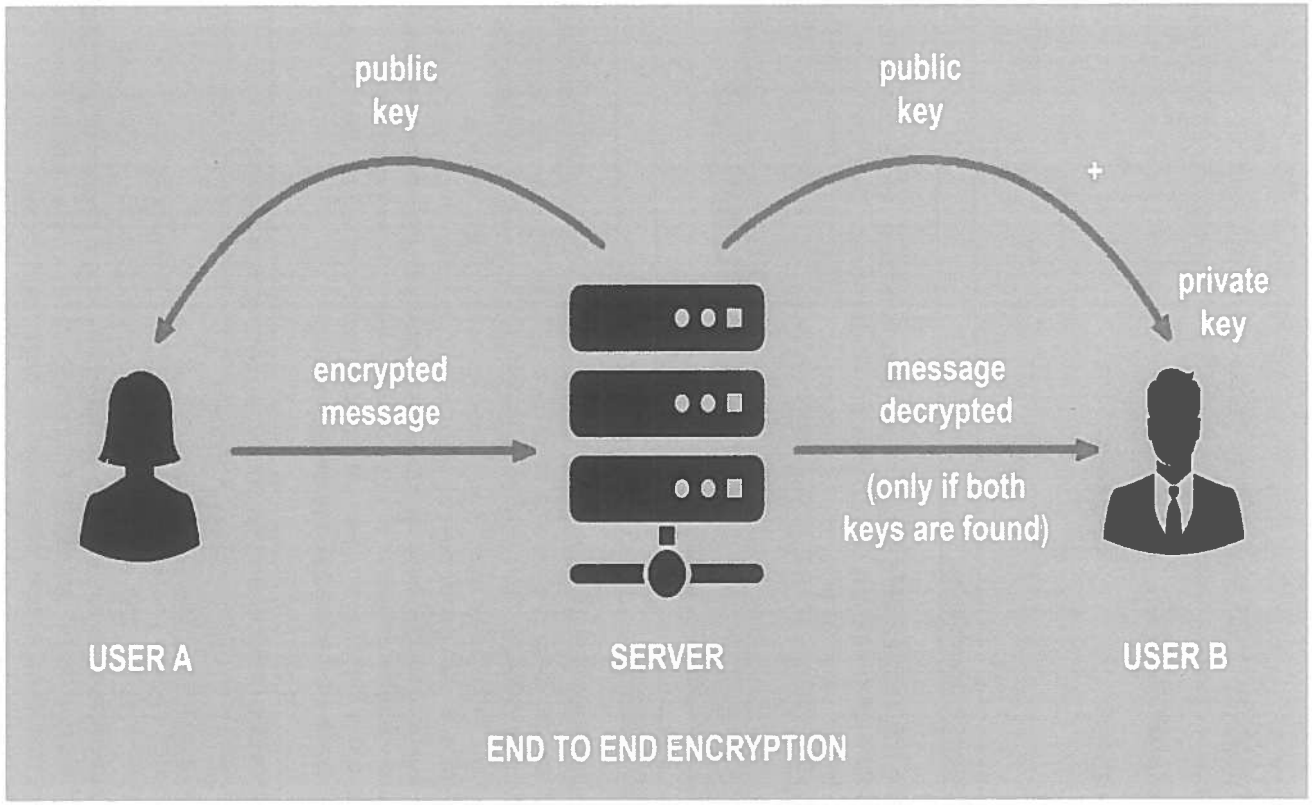
# Andere landen?

- België
- 10.2.a [redacted]
- Australië

# Way forward

- Den Haag

- Brussel


public
key
public
key
+
private
key
encrypted
message
message
decrypted
(only if both
keys are found)
USER A
SERVER
USER B
END TO END ENCRYPTION

Ministerie van Justitie en Veiligheid

Directie: DRC

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
10.2.e

T 070
M 10.2.e
10.2.e @minjenv.nl

Datum
XX-XX-2019

# Encryptie Facebook

Gesprekspartner(s): 10.2.a

Gelegenheid: A-deux

Datum:

## 1. Essentie boodschap

Toegang tot versleutelde gegevens is een noodzaak in de opsporing naar zware criminaliteit, terrorisme en kinderporno. Daarom kunt u begrip tonen voor de brief die is verzonden. 11.1

## 2. Achtergrond

In Nederland zijn we bezig met het uitwerken van de ontsleutelplicht. U heeft eerder begrip getoond voor de brief van Barr en zijn Britse en Australische collega. Met publiek private partners wordt onderzocht hoe in een specifieke zaak inzicht kan worden verkregen in data.

Encryptie is van groot belang voor cybersecurity en de communicatie tussen burger, bedrijf en overheid. Encryptie kan ook bijdragen aan de nationale veiligheid waar het bijvoorbeeld berichtgeving of vitale infrastructuur beschermt, aan de andere kant kennen de I&V-diensten vergelijkbare problematiek als de opsporing.

## 3. Spreekpunten in Engels (tenzij anders aangegeven)

- 11.1
- I support strong encryption because of the importance to cybersecurity, the digital economy, correspondence between government, business and civilians and the freedom of expression.
- On the other hand access to encrypted data is essential in the fight against child abuse, terrorism en organized crime.
- In the Netherlands we strife to find a solution where the strength of encryption is not structurally weakened.
- The aim is to gain access to usable data in a specific case.
- I would gladly keep close contact along the way and share our findings.

## 4. Afgestemd met

-

Ministerie van Justitie en Veiligheid

# Encryptie Facebook

Gesprekspartner(s): 10.2.a

Gelegenheid: Werkbezoek

Datum: December

Directie: DRC

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
10.2.e

T 070
M 10.2.e
10.2.e @minjenv.nl

Datum
XX-XX-2019

## 1. Essentie boodschap

- Toegang tot versleutelde gegevens is een noodzaak in de opsporing naar zware criminaliteit, terrorisme en kinderporno. Daarom kunt u begrip tonen voor de brief die is verzonden door Barr en zijn collega's uit het VK en Australië. Uw boodschap is vergelijkbaar. U pleit beide voor sterke encryptie, maar in de opsporing naar ernstige strafbare feiten zoals kinderporno, moet inzicht kunnen worden verkregen in versleutelde data.
- 11.1

## 2. Achtergrond

Encryptie is van groot belang voor cybersecurity en de communicatie tussen burger, bedrijf en overheid. Encryptie kan ook bijdragen aan de nationale veiligheid waar het bijvoorbeeld berichtgeving of vitale infrastructuur beschermt, aan de andere kant kennen de I&V-diensten vergelijkbare problematiek als de opsporing. U heeft eerder begrip getoond voor de brief van Barr en zijn Britse en Australische collega. Encryptie bemoeilijkt, vertraagt of maakt het in zijn geheel onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten. In het zoeken naar een oplossing wordt ernaar gestreefd om binnen de kaders van het huidige encryptiestandpunt te blijven.

In antwoord op Kamervragen van Verhoeven heeft u aangegeven de diverse betrokken belangen en de conclusie uit het kabinetsstandpunt dat het niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland onder de aandacht brengen.

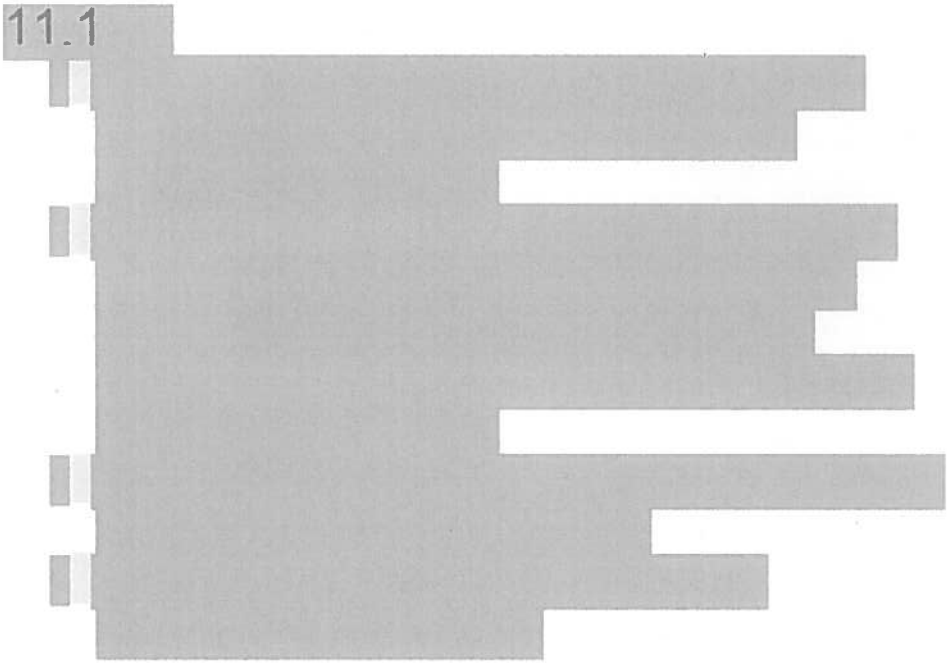
3. Spreekpunten in Engels (tenzij anders aangegeven)

- 11.1 [redacted]
- I support strong encryption because of the importance to cybersecurity, the digital economy, correspondence between government, business and civilians and the freedom of expression.
- On the other hand access to encrypted data is essential in the fight against child abuse, terrorism en organized crime.
- In the Netherlands we strive to find a solution where the strength of encryption is not structurally weakened.
- The aim is to gain access to usable data in a specific case.
- I would gladly keep close contact along the way and share our findings.

4. Afgestemd met

-

11.1



11.1

11.1

**Q: Wil de minister internationaal overleg voeren om toegang te krijgen tot versleutelde gegevens?**

**A:** Encryptie vertraagt en bemoeilijkt het (tijdig) verkrijgen van inzicht in communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten, of maakt dit in zijn geheel onmogelijk.

Dit probleem is niet beperkt tot de Nederlandse opsporing.

In antwoorden op Kamervragen van het lid Verhoeven over versleuteling ben ik ingegaan op mijn initiatief om te komen tot een oplossing voor dit probleem.

Onderdeel van dit initiatief is dat in gesprek wordt gegaan met andere landen en lidstaten over de manier waarop zij met deze problematiek omgaan en welke oplossingen zij voorzien.

Daarvoor is samenwerking en overleg met publieke en private belanghebbenden noodzakelijk.

[In mijn beantwoording van het lid Verhoeven geef ik aan dat ik streef naar oplossingen binnen de kaders van het kabinetsstandpunt en die recht doen aan de belangen van de opsporing en de nationale veiligheid.]

Ministerie van Justitie en Veiligheid

MJenV

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
Criminaliteit en Veilighe d

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverhe d.nl/jenv

**Contactpersoon**
10.2 e
*beleidsadviseur*

T 070 10.2 e
F 070 370 79 00

**Datum**
16 oktober 2019

**Ons kenmerk**

Overleg met 10.2.g

## Aanleiding

Op 17 oktober heeft u een overleg met 10.2.g buiten reikwijdte

## Onderwerpen

Bijgevoegd vindt u de voorbereiding op:

Buiten reikwijdte

Buiten reikwijdte 10.2.g Buiten reikwijdte

-Facebook en de voorgenomen encryptie.

Hieronder vindt u per onderwerp een spreeklijn. QenA en eventuele factsheets vindt u in de bijlagen.

Buiten reikwijdte

- Buiten reikwijdte

- Buiten reikwijdte

**Actualiteit Encryptie Facebook**

- Ik onderschrijf het encryptiestandpunt. Ik erken het belang van encryptie voor de veiligheid van digitale communicatie tussen overheid, bedrijf en burger, en de bescherming van de persoonlijke levenssfeer.

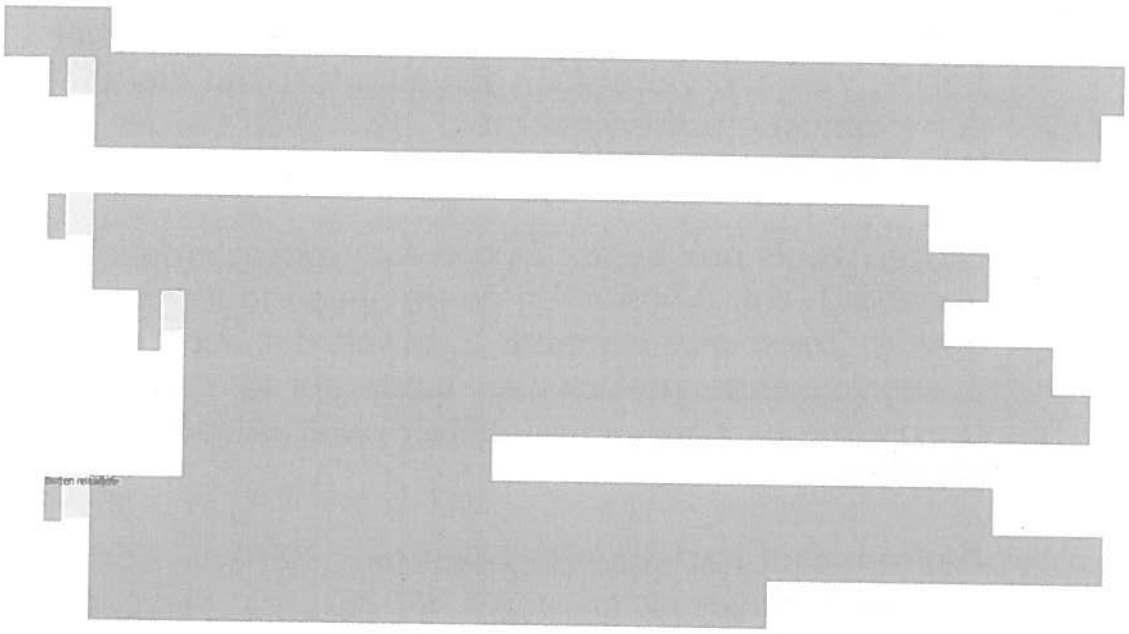
- Echter, zoals ook helder in het encryptiestandpunt is verwoord, zijn de effecten op de opsporingscapaciteit niet gering. Zeker niet wanneer je beseft dat het opsporingsonderzoeken naar kinderporno, contra terrorisme en zware criminaliteit raakt. Alsook de I&V diensten.

- Daarom sluit het encryptiestandpunt het zoeken naar oplossingen niet uit en wordt het gesprek met bedrijven aangemoedigd, zolang het maar niet de encryptie structureel verslechtert.

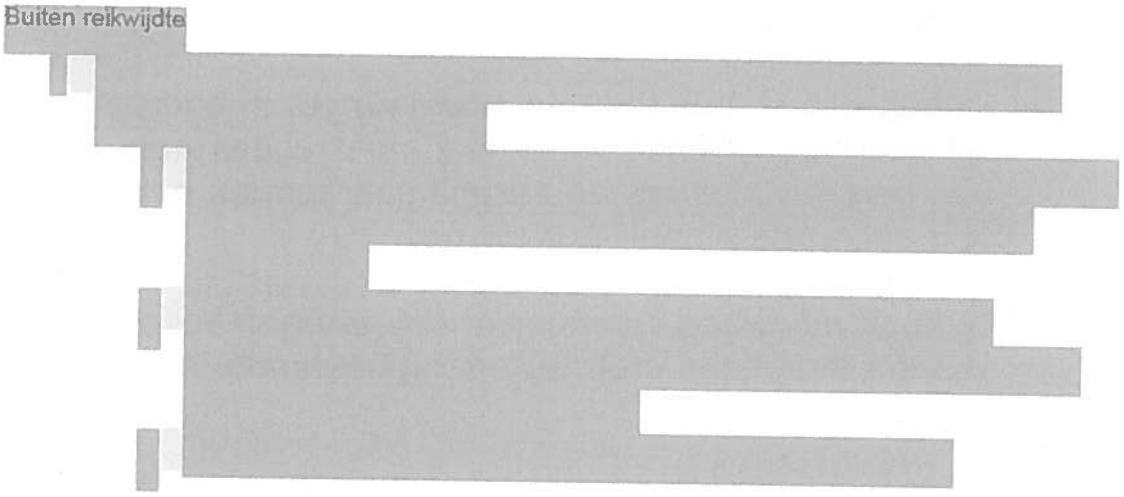
- Ik ben nog steeds tegen achterdeurtjes in encryptie, ik wil geen beperkende wettelijke maatregelen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.

- Ik hoor wel graag wanneer er oplossingen beschikbaar zijn die in lijn zijn met het encryptiestandpunt.

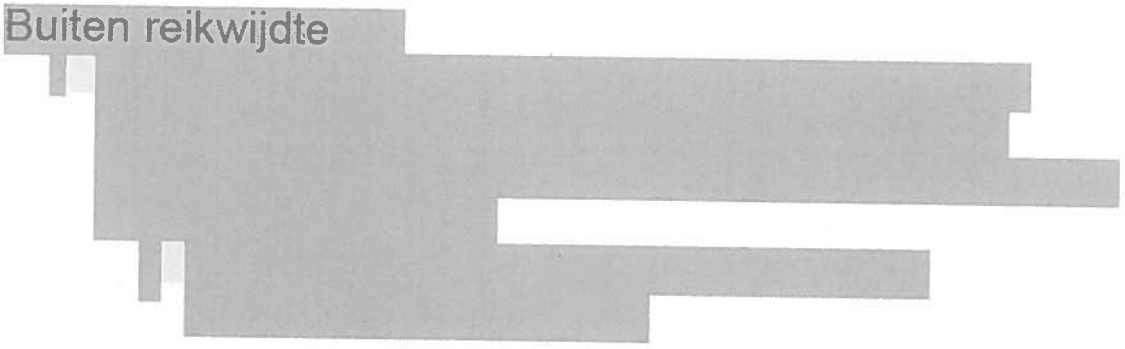
Buiten reikwijdte



Buiten reikwijdte



Buiten reikwijdte



Ministerie van Justitie en Veiligheid

Directie:

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
10.2.e

10.2.e
10.2.e @minjenv.nl

Datum
07-01-2020

# Encryption and lawful access

Gesprekspartner(s): 10.2.e en 10.2.a

Gelegenheid: Bezoek 10.2.e en 10.2.a aan Nederland

Datum: 16 januari 2020

## 1. Essentie boodschap

U deelt de zorg over de uitdagingen die end-to-end-encryptie voor de opsporing met zich mee brengt. 11.1

## 2. Achtergrond

Op 20 december jl. heeft u na overleg met DEIA besloten aan

*Nadere achtergrond*
Op 4 oktober hebben ministers uit de VS, het VK en Australië een open brief aan Facebook gestuurd waarin zij het besluit om end-to-end-encryptie toe te passen in Facebook Messenger bekritiseren, omdat dit de strijd tegen online kinderpornografie bemoeilijkt. Op 3 november heeft u in een uitzending van Nieuwsuur gemeld dat u bij over-the-top-diensten zoals Facebook Messenger in specifieke gevallen versleutelde informatie wilt kunnen ontsleutelen. Tijdens uw bezoek van 4 tot en met 7 december aan de VS 10.2.a

Naar aanleiding van de nota van 4 november en het daaropvolgende gesprek is encryptie besproken met 11.1

11.1 . Daarnaast worden de technische mogelijkheden verkend met overheidsorganisaties. In december heeft bovendien informeel laagambtelijk overleg plaatsgevonden met 10.2.a, 10.2.a , 10.2.a , 10.2.a , 10.2.a en 10.2.a 11.1

## 3. Spreekpunten in Engels (tenzij anders aangegeven)

- I share the concern of the US, UK and Australia regarding the issue of encryption for law enforcement.
- 11.1

## 4. Afgestemd met

DEIA, NCTV

**SPEECH FERDINAND GRAPPERHAUS**
**CSIS TECHNOLOGY POLICY PROGRAM**
**'Global partnerships to combat cybercrime & the challenge of going dark'**
**5 December 2019**
**Washington DC**

Ladies and gentlemen,

Less than a mile from here, in the Library of Congress, you can find a unique treasure: the first map of the world to use the name America. It was made by the German cartographer Martin Waldseemüller and first published in 1507. To be honest: the name America is placed on what is now known as Latin-America, but it was proof that the Roman poet Virgil was right. That there was a land "*that lies beyond the stars, beyond the paths of the year and the sun, where Atlas the heaven-bearer turns on his shoulder the axis of the world set with blazing stars*".
Waldseemüller based his map on the travels and discoveries of Ptolemy, Amerigo Vespucci and – no surprise – Christopher Columbus.
Explorers who sailed the seven seas in order to discover new trade routes, new products, new trade partners.
Yes, money made the world go round…
These men – yes, all men, sorry -, these explorers and cartographers, made the unknown into the known.
Because in the unknown, there were dragons…

Their world was a world of land, sea and air.
Dangerous, but visible, definable, finite.
But in the last 70 years, we expanded that known world in two directions: up and everywhere.
We went up in space in the sixties, in the words of president John F. Kennedy: "*we choose to go to the moon in this decade and do the other things. Not because they are easy, but because they are hard.*"
And then we went beyond what is there, into an new – this time manmade 'everywhere': which is cyberspace.
Invisible, indefinable, infinite.
And just as dangerous – or even more so - than the old world.

Because cyberspace is not a place on a map.
Cyberspace, digitalisation is everywhere.
Over the course of just a few decades, the world has entered a digital age in which people from all over the world are connected online.

In 1996, only 36 million people used the internet, less than a per cent of the world population. In 2017, that figure had risen to 3.7 billion, nearly half the world's population. Individuals and businesses, governments and NGO's, financial institutions and think tanks: they – we - are all connected. We all use the endless resources, the endless possibilities of cyber space. And I think that is a good thing.

Because digitalisation brought us e-learning, e-health, unlimited information and shared knowledge, social media and the internet of things. And the possibilities seem endless: talking refrigerators, self-driving cars and robots that dream. But digitalisation also brought us ransomware and fake news, the dark web and cyberstalking, digital espionage and cyberattacks. And maybe even some Manchurian candidates we don't know about yet. Killers, instructed through the internet, somewhere out there. Yes, cyberspace brought us cybercrime and the need for cybersecurity.

And to be honest, our society has become totally dependent on digital resources. Critical processes like telecoms, water supplies and financial transactions are now completely reliant on digital systems and processes. If one link in the digital chain breaks, it soon may have a domino effect. It will have direct consequences on critical processes in business and government, the earning power of companies and the daily lives of our citizens. Not to mention indirect consequences.

So the chain can break, and there are threats that will happen on purpose. Such purpose comes mainly from two categories of perpetrators: state actors and criminals. Their influence and deviousness of these two sorts is growing and continues to develop.
State actors who try to digitally influence elections, but also reputations and public views. State actors who may even want to influence essential processes in society or sabotage vital infrastructure. Thereby undermining free society.

Criminals present other threats; let us first take a closer look at those. They continue to develop revenue models, such as ransomware. Like in 2017 when organisations across the globe fell victim to a ransomware attack. In the Netherlands one of the largest container terminals in the Port of Rotterdam was attacked, among others. Processes were halted and delayed for days, with severe societal and economical damages. In the United Kingdom in a likewise manner with two large hospitals.

And, criminal organizations who have no technological expertise, can orchestrate a ransom attack: they just hire experts to develop and distribute the ransomware. Easy money, but big social and economic consequences.

They also find those people who can develop and distribute ransomware on the dark web: dark nets where one can find markets for weapons and drugs, assassins and - for me personally one of the worst - child exploitation.

And this is why our governments must put money and means in the investigation and persecution of those Internet criminal organization. As was done in the cooperation between the Dutch, US and German law enforcement to get a hold on Hansa. Hansa was once the largest dark-web market in Europe. There were more than 24,000 drug products on offer, from cocaine to specific sorts of MDMA to heroin, as well as a smaller trade in fraud tools and counterfeit documents. The Dutch investigators started an undercover operation. With fake accounts the Dutch police was able to take full control of the site itself. From that moment they could keep digital eye on Hansa's buyers and sellers. Learn everything about them so they could be identified and even tricked dozens of sellers in revealing their locations.

It was a game-changing police intervention, that packed a real punch against the dark web: millions of dollars worth of confiscated bitcoins, more than a dozen arrests - and counting - of top drug dealers, and a vast database of user information.

And that type of interventions must continue. As must close cooperation. Because to stand up to the increasing threats, we must work with others. With other governments, other agencies, other countries. At political, policy-making and technical but also operational level. Cyberspace knows no borders, so does cybercrime: we have to think global to pack our punches.

For instance, to do that against international networks that distribute child abuse images. That is an important issue for me, for the Netherlands. Because a huge amount of online child sexual abuse is stored on servers in or attributed to locations in the Netherlands. Because we are a digital hub; we have a high-end infrastructure that criminals misuse. And it is my aim to break this spiral; victims deserve no less.

So I started to organise a round table with the large digital companies NGO's and science. The sector itself has developed a self-regulating policy with a notice and takedown-procedure: they will themselves see to remove unlawful content is removed within 24 hours. Secondly we also built a hash-check-service that allows companies to clean their servers. Thirdly a technical University makes a monitoring instrument that provides insight into which company hosts how much child abuse images. Last but not least I started a legislative process to directly impose penalties on companies that do not remove the content in 24 hours after a report of child pornography including everything that goes with it. And certainly also the naming and shaming that will go with it.

To make sure that actually happens they will be supervised by a new independent national authority that will have sufficient enforcement resources at its disposal. Companies or directors who do not defer to this authority will be prosecuted. All actions that will – must - help to slay the dragon of online child sexual abuse.

Slaying these dragons, to be cyber secure, is an integral part of protection against threats in the digital domain, essential for safeguarding national security as well.

However. Challenges to effectively combat cybercrime remain. Especially, the challenge of going dark. In other words how do we maintain access to information and critical tools that our law enforcement needs to find these criminals.

In the Europe and the U.S. we have the same discussion on the use of end-to-end encryption by platforms such as Facebook, Instagram or Whatsapp and others. Everyone agrees that victims of online child abuse should have our societal protection. Everyone agrees that we should do everything to find the heinous criminals and prosecute them. But everyone also agrees that we have a right to privacy and data protection. Everyone agrees that we need to be cyber secure. End-to-end encryption is both a blessing and a curse in prosecuting criminals.

Many of the tech platforms have moved to use end-to-end encryption or are about to. And although I agree with people that end-to-end encryption is an important feature on privacy protection. But I also see how our law enforcements agencies are struggling with how criminals benefit from this shield of privacy. We need to find a balances approach, to protect the victims and respect ones privacy. And I wish to stress; only to protect victims of those heinous crimes as child abuse en pornography. I propose to continue the dialogue with the tech platforms. And I agree with your attorney General Barr that we need to call upon them, to take their responsibility, to keep the Internet a safe place.

Until now, I've addressed primarily cybercrime, but of course the issue is much broader. We also have to talk about cybersecurity, state actors. Because everything is connected.

That is why two small cities in the Netherlands are on a United States list. Not because they are on the Lonely Planet's list of places you must visit, but because they are crucial security targets.

But because at Beverwijk and Katwijk, undersea telecommunications cables land on the shore. Fiber optic cables that are used for telephones, internet and television, that connect Europe with America through the

Amsterdam internet exchange. An attack on those cables can have serious consequences for international Internet and telephone traffic. In November 2003, for example, a relatively modest defect of one of the cables caused major Internet disruptions in the United Kingdom. A coordinated attack on multiple cables might paralyze half the world. And as we see state actors of various geographical and political background have been willing to try to influence our cyber-dependant systems to destabilize, or as I have pointed out before, to even sabotage our society. It makes us realise how vulnerable we are. How vulnerable we all are.

For this reason I presented a national Cyber Security Agenda in the Netherlands. A free society needs a basic level of cybersecurity to increase our resilience against cybercrime and cyberattacks.
We have to ensure that our capabilities and resources to address threats are working. As the question is no longer if a disruption will take place but when. We have to be prepared for that. Always.

We have to make sure that cybersecurity is a basic consideration in the further development of our digital processes. Against those criminals but also against state actors. We have to make sure that citizens, businesses and public authorities improve their digital security and that the government fulfils its protective duty in the digital domain.

I can ensure you, I will raise the awareness to the public. It is one of my more difficult tasks as a minister. That means that we have to work together, that we need public and private cooperation, national and international. Current practice in this cooperation shows that there is a need for a clear division of responsibilities.

We cannot just rely on existing laws and regulations on security. Cyber has its own dimensions, one could even say that cyber in itself adds a new dimension in our universe. That does not mean that we need a whole new set of rules and regulations. Absolutely not. But as a society we must reconcile the specific aspects of cyber with existing rights and regulations we have.

In that respect: new does not automatically mean 'different'; cyberspace is not automatically the exception, does not have special status.
So we do not need to reinvent everything, we must explore what isn't there yet.

We must take upon us the challenge to become the cartographers of cyberspace. We, that is society, involving everyone who has an interest or involvement in cyber.

It is clear that – although we cannot be a 100% responsible – the government has to take the lead. We have to commit to a secure and stable country by recognizing threats to critical interests and increase the resilience of those interests. We have to be prepared for attacks and crimes, crises and incidents that threaten our society. We also have to take the lead in gathering and sharing information and knowledge.
For instance by stimulating fundamental and applied research into cybersecurity. Not only to strengthen our own security, but also to enhance our national and international knowledge position and our digital autonomy. And the government has to take the lead in public-private cooperation. In the Netherlands, that cooperation has already led to many great initiatives and results.

We have created the Digital Trust Center, in order to help businesses increase their cybersecurity. And we have developed a national system to facilitate the exchange of cybersecurity information. There is now a Cybersecurity Council and a Cybersecurity Alliance where public bodies, private organisations and the research community work together to make strategic and practical improvements to cybersecurity in our country.

But public-private partnerships alone won't be enough to respond to the ever mounting threats. When it comes to addressing security concerns, we are finding a new balance. Because security can no longer be an afterthought. Remember that I said; it is not if it is gonna happen, but when. As a government we must act earlier and more assertively.
And, maybe even more importantly: we have to work together. Cybersecurity is not restricted to national borders.

As I said earlier, the Netherlands has internationally crucial digital infrastructure, that means whatever we do, cannot only be seen at a national level. We need international cooperation. Together with several partners such as the EU, we have taken a number of steps to keep up and become more resilient. However, due to rapid technological developments and on the other hand, the transboundary risks and threats, it is necessary to take the next step in international cooperation. To increase security in the international, digital domain. The Netherlands and the US shoudl work even more together, we are natural partners in this respect.

As a Dutchman I admire the American approach. Your approach to cybersecurity can lead as an example on how we can develop even further. For example the way the Americans handle critical infrastructure and supply chain risk management illustrates the possibilities and necessity of a common approach and cooperation.

On the other hand, you are also the land of the free and the home of the brave. Freedom of fundamental rights are your DNA. In my youth I was much inspired by Steve Miller. His song - Fly Like an Eagle - was about hope for the future. "There's a solution", was the reoccurring line. And you know what? They call him the Space Cowboy: always positive searching for answers. I certainly would hope the USA would be willing to take up the role as the future Cyberspace Cowboy.

We need the USA if we want fruitful international progress on cyber. As I said it will only be possible to enhance cybersecurity through international cooperation and international legislation.

You all know that the Netherlands are a relatively small country – although we are thirteen times bigger that your smallest state: Rhode Island. On Waldseemüller's map of the world we were not even named, as we were then just a collection of low counties by the sea. But that sea, the threats and possibilities of all that water, learned us to cooperate. With public and private partners, nationally and internationally. With an especially strong reputation in ensuring maritime cyber security.

Maritime cyber security sets a good example of the cooperation between our two countries. In this area the US and the Netherlands took the first step in creating a partnership. We have many shared interests when it comes to maritime cyber security. Creating a synergy in this sector, by sharing information and best practices, is the only way to keep our ships and ports digitally safe. And I'm very pleased to see that now other countries joining the two us in the cooperation such as Denmark, Germany, France and the UK.

So finally, whether on land or sea, cyberspace is a world we are still exploring. A world we have to map out, define, regulate. But there are still plenty of dragons at the edges of the map. We have the tradition in slaying those dragons: we have lots of explorers, adventurers and cartographers in our history to be proud of.

We just missed out on discovering America, but we were the first to discover Australia, long before James Cook sailed along. A Dutch cartographer, Adriaen Block, was – in 1614 - the first European to draw a map of your East Coast, with the island Manhattan, or New Netherland as it became known then. And ok, we should never have sold New York, but what can you do? People make mistakes right? But as they say, failures achieved in the past offer no guarantees for future lessons learned. Of course, results achieved in the past offer no guarantee for the future. So we should consider cyberspace as a whole new challenge. A challenge that is difficult to know, difficult to grasp, difficult to map. A challenge we have to face together, working together, talking together. Like we are doing during my visit here. That is the role we all have to play. Together we will take the next steps.

Thank you.

# Deel Ab: mails en mailbijlages DGRR

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** vrijdag 22 november 2019 15:22
**Aan:** 10.2.e BD/DEIA/EU; 10.2.e @minbuza.nl 10.2.e BD/DEIA/EU; 10.2.e - BD/DBAenV/IenK
**CC:** 10.2.e BD/DEIA/IBP; 10.2.e BD/DRC/CV; 10.2.e - BD/DCOM/P&B
**Onderwerp:** RE: Facebook

11.1 Een voorproefje hebben we gekregen na Nieuwsuur.

**Van:** 10.2.e - BD/DEIA/EU
**Verzonden:** vrijdag 22 november 2019 15:20
**Aan:** 10.2.e - BD/DRC/CV ; 10.2.e @minbuza.nl; 10.2.e BD/DEIA/EU ; 10.2.e BD/DBAenV/IenK
**CC:** 10.2.e - BD/DEIA/IBP ; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Facebook

Ha 10.2.e, 11.1 Als we het eens zijn met de brief en andere lidstaten zich ook aansluiten, weegt dan de druk van de private partijen en de perceptie zwaar genoeg? Hoe erg is de fall out volgens jou als MJV toch mee wil doen met Barr?

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** vrijdag 22 november 2019 13:18
**Aan:** 10.2.e @minbuza.nl; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook

Beste allen,
Informatie tot nu toe is dat er vanuit 10.2.a een overleg plaatsvindt/heeft plaatsgevonden richting met een oproep om mee te ondertekenen: 10.2.a 10.2.a en mogelijk de 10.2.a .
Dit gegeven wordt voorgelegd aan de minister, zonder ambtelijk van advies te wijzigen. 11.1

11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** woensdag 20 november 2019 18:58
**Aan:** 10.2.e @minbuza.nl; 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook

Mijn 10.2.a collega hier (afdelingshoofd JBZ) had nog niets hierover gehoord uit 10.2.a

**From:** 10.2.e @minbuza.nl>
**Sent:** woensdag 20 november 2019 16:11
**To:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e /DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Cc:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Subject:** RE: Facebook

Collega's,
Zojuist met kabinet van 10.2.a gesproken. Hierbij een terugkoppeling:
- Ik heb de NL positie conform het onderstaande toegelicht.
- 10.2.a wil tekenen, bij voorkeur met 10.2.a .
- 10.2.a heeft nog geen standpunt ingenomen. 10.2.a zal ons contacteren wanneer 10.2.a een positie heeft ingenomen.
- Ik heb 10.2.a gevraagd om ons sowieso te contacteren op het moment dat 10.2.a op korte termijn stappen gaat zetten. 10.2.a heeft dit toegezegd.

Groeten,
10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** dinsdag 19 nov. 2019 11:35 AM
**Aan:** 10.2.e @minbuza.nl>, 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>, 10.2.e 10.2.e @minbuza.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>, 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook

Hallo 10.2.e
Dank je. Het startpunt is duidelijk: bij de inventarisatie naar oplossingen om toegang te krijgen tot versleutelde data wordt gestreefd om binnen de kaders van het kabinetsstandpunt te blijven. Dat wil zeggen geen structurele verzwakking in encryptie. Daarin is dus niets veranderd. Hoe de geïnventariseerde oplossingen zich verhouden tot het kabinetsstandpunt zal tzt moeten worden bezien.
Wat dit betekent voor de brief is dat 11.1 Mocht 10.2.a aan ons verzoeken of we samen met 10.2.a de brief willen ondertekenen dan zal dat moeten worden voorgelegd aan de minister.
Zoals je weet hebben we deze week begrotingsbehandeling, dus dat zal niet op korte termijn kunnen.
Vanmiddag bellen is prima, hoe laat? 10.2.e ben jij op kantoor?
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** dinsdag 19 november 2019 11:01
**Aan:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook

Collega's,

Ik zit in overleg en heb me nog niet kunnen bellen maar in reactie op de kamerbrief kreeg ik de onderstaande reactie.

11.1 [redacted]

10.2.e kan ik je vanmiddag voordat ik het kabinet bel nog even met jou bellen/heb je nog een nadere toelichting?
Alvast bedankt!
Groeten,
10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** dinsdag 19 nov. 2019 10:25 AM
**Aan:** 10.2.e @minbuza.nl>, 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>, 10.2.e 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>, 10.2.e 10.2.e @minbuza.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>, 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook
Hallo 10.2.e
Voor 10.2.e zou dat zeker helpen. Misschien hebben zij een beter beeld van wat Europees speelt dan dat wij hebben. De afgelopen drie mails in ieder geval geen inhoudelijke reactie ontvangen. Aanleiding van mijn mail van 28 oktober was dat onze liaison in Washington had vernomen dat 11.1 [redacted]
Hierbij in ieder geval de openbare set Kamervragen en antwoorden. De spreeklijn is dat wordt gestreefd naar toegang tot versleutelde data zonder daarbij encryptie structureel te verzwakken. Hiertoe wordt op dit moment het gesprek aangegaan met publieke en private partners.
Heb je hier iets aan?
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** dinsdag 19 november 2019 09:07
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e /DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Facebook
Goedemorgen 10.2.e
Ik ben graag bereid om nogmaals met [redacted] te bellen om na te gaan of er inmiddels een beslissing is genomen maar dan is het wel goed om te weten waar NL staat. Kan je daar iets meer over zeggen?
Alvast bedankt!
Groeten,
10.2.e

**From:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Sent:** maandag 18 november 2019 16:24
**To:** 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>

**Cc:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl>; 10.2.e 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>
**Subject:** RE: Facebook

Hallo allemaal,
Morgenochtend gaat de dossiernotitie voor Encryptie, Facebook en het overleg met Barr naar de minister.
Is er al een beeld welke LS de brief van Barr mede tekenen/steunen?
11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

.....
**Ministerie van Veiligheid en Justitie**
**Directie Rechtshandhaving en Criminaliteitsbestrijding**
**Cybercrime unit**
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 - BD/DRC/CV
**Verzonden:** zaterdag 9 november 2019 12:10
**Aan:** 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl; 10.2.e BD/DRC/CV 10.2.e @minjenv.10.2.e @minbuza.nl
**Onderwerp:** RE: Facebook

Hallo allemaal,
In opvolging op onderstaand mailtje deel ik de reactie die we van 10.2.e hebben gekregen uit 10.2.a
Wanneer in Europa momentum komt voor de brief zou de minister dit in een vroeg stadium moeten weten. Zo heeft hij in ieder geval de kans kom tot de kopgroep te horen, ipv lidstaat nummer 14.
11.1

Groet,
10.2.e

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 19:58
**Aan:** 10.2.e BD/DEIA/EU; 10.2.e BD/DEIA/EU; 10.2.e BD/DBAenV/IenK
**CC:** 10.2.e - BD/DEIA/IBP; 10.2.e @minbuza.nl
**Onderwerp:** RE: Facebook

Ha 10.2.e
Ja, hoe we het best en het snelst inzicht hierin kunnen krijgen laat ik aan jullie ☺. Ik wil voorkomen dat de minister zo direct lidstaat nummer 11 is dat de keuze maakt om de brief van Barr wel of niet te steunen. Nu zijn we niet voornemens om de brief van Barr volmondig te steunen, maar er wel begrip voor tonen (cf eerdere uitlatingen). 11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
**M** 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>
**Verzonden:** maandag 28 oktober 2019 19:42

**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>;10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>;10.2.e @minbuza.nl
**Onderwerp:** RE: Facebook

Hi 10.2.e en 10.2.e, is het een idee om dat rondje via 10.2.e te laten lopen? Kan me voorstellen dat de PV een beetje regie wil voeren. Zo niet, ga ik met liefde een rondje bellen, let me know. Hoe was jullie stafoverleg vandaag? Kwamen daar nog nieuwe inzichten uit op dit punt?

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** maandag 28 okt. 2019 9:23 AM
**Aan:** 10.2.e BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>, 10.2.e /DEIA/EU 10.2.e @minjenv.nl>, 10.2.e @minbuza.nl 10.2.e @minbuza.nl>
**Onderwerp:** RE: Facebook

Ha 10.2.e
Dankjewel! Van 10.2.e begreep ik dat andere landen ook zijn bevraagd. 10.2.a was bijvoorbeeld vorige week in 10.2.a. Kun je inventariseren bij de collega DEIA's in andere landen welke bewegingen er zijn?
Groet,
10.2.e

**Van:** 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>
**Verzonden:** vrijdag 25 oktober 2019 12:26
**Aan:** 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>;10.2.e @minbuza.nl
**Onderwerp:** FW: Facebook

Collega's,
Wat ik mij nog afvroeg; 11.1

Groet,
10.2.e

**Van:** 10.2.e BD/DBAenV/IenK
**Verzonden:** donderdag 24 oktober 2019 11:59
**Aan:** 10.2.e - BD/DEIA/IBP; 10.2.e BD/DEIA/EU
**Onderwerp:** RE: Facebook

Hierbij de laatste versie van de memo en platte tekst voor openbrief. Dit willen we bespreken in het DGRR-stafoverleg met de minister aanstaande maandag. Groet, 10.2.e

---

Ministry of Justice and Security

---

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

---

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic

transmission of messages.

Ministry of Justice and Security

---

10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 19 november 2019 14:32
**Aan:** 10.2.e - BD/KS; 10.2.e BD/PNDV
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook
**Bijlagen:** Gespreksnota.docx

Hallo 10.2.e

Ik zal de dossiernotitie aanpassen.

Dit is de gespreksnota zoals vastgesteld.

Groet,

10.2.e

**Van:** 10.2.e - BD/KS
**Verzonden:** dinsdag 19 november 2019 14:20
**Aan:** 10.2.e - BD/PNDV ; 10.2.e BD/DRC/CV
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

Hoi 10.2.e en 10.2.e,

Veel dank aan 10.2.e voor het snelle schakelen op de dossiernotitie. 11.1 [redacted]

Verder, 10.2.e
Patricia Zorko wil as. vrijdag graag aansluiten bij het gesprek met de minister.
Komt er voor dat gesprek nog een aparte gespreksnotitie, of moet ik de gespreksnotitie voor [redacted] met Patricia delen? Als er een gespreksnotitie komt, vraag ik graag expliciete aandacht voor de door 10.2.e benoemde twee punten onder C. Als er geen gespreksnotitie komt, stuur je me dan de final version?

Gr 10.2.e

**Van:** 10.2.e - BD/PNDV 10.2.e @nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 17:38
**Aan:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

Hallo 10.2.e

Goed te weten dat er reeds contact is geweest. Met het oog op de krappe deadline had ik het stuk al bij de experts uitgezet. Zie bijgevoegd de reactie die ik kreeg. Zal niet heel anders zijn dan de punten

van 10.2.e vermoed ik, maar gezien het werk dat de collega's er op korte tijd in hebben gestoken stuur ik het bij deze ter info door. 11.1 .

Groet,
10.2.e

A.

- De eerste plaat irt end-to-end encryptie lijkt te suggereren dat de "server" standaard de beschikking heeft over de "privé sleutel" en deze distribueert. Dit is niet hoe end-to-end encryptie over het algemeen (zoals bij WhatsApp) werkt.
- De "servers" hebben juist niet de beschikking over privé sleutels, vandaar end-to-end encryptie
- 11.1

B.

- En andere oplossing die je wel vaker hoort (en mogelijk probeerde iemand die te visualiseren?) is het uitvoeren van een zogenaamde "man-in-the-middle" aanval. Dit wil zeggen dat als 10.2.e en ik communiceren, dat de aanvaller een aangepaste situatie probeert te creëren die een OTT-dienst juist probeert te voorkomen:
  - 10.2.e <-> Aanvaller die doet als of ie 10.2.e is
  - 10.2.e <-> Aanvaller die doet als of ie 10.2.e is.
  - Aanvaller stuurt de berichten heen-en-weer
  - Zowel 10.2.e als ik krijgen hier een melding (waarschuwing) van of in voorkomende gevallen wordt de verbinding tussen Maarten en mij onmogelijk gemaakt.
  - Alleen als de leverancier van de OTT-dienst deze waarschuwing/afbreking zou onderdrukken (in de applicatie) kan dit technisch worden uitgevoerd.

C. maar, nog belangrijker

- 11.1

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** maandag 18 november 2019 16:17
**Aan:** 10.2.e - BD/PNDV 10.2.e @nctv.minjenv.nl>; 10.2.e BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DBAenV/IenK 10.2.e minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken Encryptie en Facebook

Ha 10.2.e

Weet dat 10.2.e eerder contact heeft gehad met 10.2.e over de non-paper. 11.1 Juist vanwege het bestaan van verschillende optieken wordt nut, noodzaak en haalbaarheid onderzocht.

**Van:** 10.2.e - BD/PNDV 10.2.e @nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 16:11
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e -

BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DEIA/IBP 10.2.e i@minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken Encryptie en Facebook

Hallo 10.2.e

We zullen op tijd reageren. 11.1 zie enkele verwijderde typo's in de bijlage.

De diagrammen kan ik zelf niet beoordelen; kijkt een expert nog even naar.

Groet,
10.2.e

---

**Van:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** maandag 18 november 2019 14:58
**Aan:** 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/PNDV 10.2.e @nctv.minjenv.nl>
**CC:** 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Onderwerp:** Dossiernotitie bilaterale bezoeken Encryptie en Facebook

Hallo allen,

Hierbij een voorstel voor het werkbezoek van de minister.

11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2.e
10.2.e @minvenj.nl

10.2.e **BD/DRC/CV**

**Van:** 10.2.e /DRC/CV
**Verzonden:** vrijdag 22 november 2019 11:25
**Aan:** 10.2.e BD/DEIA/EU
**CC:** 10.2.e BD/DRC/CV; 10.2.e - BD/DBAenV/IenK; 10.2.e 10.2.e - BD/DCOM/P&B
**Onderwerp:** RE: dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers 2 december

Zeker. 11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e - BD/DEIA/EU
**Verzonden:** vrijdag 22 november 2019 11:20
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers 2 december
Dag 10.2.e
Let wel dat de minister onderstaande boodschap vandaag in een dossiernotitie meekrijgt. Is hij op de hoogte van zijn standpunt? Ik heb begrepen dat 11.1 en 10.2.a
11.1 en 10.2.a
Groet,
10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 19 november 2019 16:34
**Aan:** 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>
**Onderwerp:** RE: dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers 2 december
Paar kleine aanpassingen.

**Van:** 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 19 november 2019 16:25
**Aan** - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers 2 december
Dag 10.2.e ,
Ik neem je aanvulling over in de essentie boodschap.
Kan ik als passieve spreektekst het volgende opnemen? Mogelijk kan dit korter:
11.1

**Van:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 19 november 2019 16:14
**Aan:** 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>
**CC:** 10.2.e @minbuza.nl; 10.2.e BD/DEIA/EU <10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e BD/DRC/GC 10.2.e @minjenv.nl>
**Onderwerp:** RE: dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers 2 december

Hallo 10.2.e
Encryptie (PASSIEF)
o 11.1 en 10.2.a

11.1

**Van:** 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 19 november 2019 14:37
**Aan:** 10.2.e @knp.politie.nl) 10.2.e @knp.politie.nl) 10.2.e @knp.politie.nl>;10.2.e @politie.nl) 10.2.e @politie.nl>; 10.2.e - BD/DRC/GC 10.2.e @minjenv.nl>;10.2.e n - BD/DGPenV/PPBT/ICA 10.2.e @minjenv.nl>; 10.2.e @minbuza.nl;10.2.e @om.nl
**CC:** 10.2.e BD/CBJ/C 10.2.e @minjenv.nl>; 10.2.e BD/DGPenV/PPBT/ICA 10.2.e @minjenv.nl>; 10.2.e BD/DGPenV/PPBT 10.2.e @minjenv.nl>; 10.2.e BD/DVB/BA 10.2.e @minjenv.nl>; 10.2.e @om.nl; 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** dossiernotitie en vooroverleg minister Grapperhaus bijeenkomst ministers [redacted] 2 december
**Urgentie:** Hoog
Beste mensen,
Buiten reikwijdte

Wat betreft encryptie zullen we nog even apart met 10.2.e (DRC) kijken wat wel of niet opgenomen wordt.

2. Buiten reikwijdte

Buiten reikwijdte

Met vriendelijke groet,
10.2 e

10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 27 november 2019 13:43
**Aan:** 10.2.e BD/DRC/CV
**Onderwerp:** RE: E-evidence: amendementen

Ha 10.2.e

Ja ging goed bij de minister afgelopen vrijdag mbt encryptie. De minister is na wat overleg akkoord gegaan met de lijn in de nota. Dat betekent dat we nu een half jaar hebben bij publiek / private partijen te inventariseren wat technische mogelijkheden zijn om toegang tot (end-to-end) versleutelde data te krijgen en encryptie niet structureel te verzwakken. Daarnaast gaan we ook internationaal de boer op…11.1

11.1

Groeten,

10.2.e

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** woensdag 27 november 2019 10:01
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: E-evidence: amendementen

11.1

Verzonden met BlackBerry Work
(www.blackberry.com)

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 27 november 2019 14:10
**Aan:** 10.2.e - BD/DEIA/EU
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e 10.2.e BD/PNDV
**Onderwerp:** QenA encryptie AO JBZ
**Bijlagen:** QenA encryptie int. samenwerking.docx

Ha 10.2.e

Hierbij een QenA op encryptie voor het AO JBZ.

10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** vrijdag 29 november 2019 16:10
**Aan:** 10.2.e
**CC:** 10.2.e BD/DRC/CV; 10.2.e @minbuza.nl
**Onderwerp:** FW: Mail EU-lidstaten en [redacted] over encryptie

Ha 10.2.e

Nogmaals dank voor al het geregel! Hierbij een suggestie voor de mail die de counselors kunnen uitzetten in hun hoofdstad voor input. We laten het contact met [redacted] wel even via de ambassade lopen hier in DH.

Dear madam/sir,

In 2016, the cabinet position on the use of encryption was published. The cabinet position elaborates on the importance of encryption for communications and the importance of access to unencrypted data for law enforcement and national security purposes.

Earlier this year, Facebook confirmed plans to use end-to-end-encryption for Facebook Messenger. On 4 October 2019, the United Kingdom Secretary of State for the Home Department of the United Kingdom, the United States Attorney General and the Secretary of Homeland Security, and the Australian Minister for Home Affairs sent an open letter to the Chief Executive Officer of Facebook in which they voiced their concerns over this announcement. On 3 November 2019 the Netherlands Minister of Justice and Security publicly stated the need for a possibility for law enforcement to decrypt data in specific cases, under appropriate conditions and safeguards. On 15 November the Minister answered parliamentary questions on this topic. In his answers he underlined both the importance of encryption for safe communications ~~of~~ between individuals, organizations and government, and the importance of access to unencrypted data for national security and law enforcement purposes.

The developments in the use of encryption stress the importance of solutions in the interest of national security and law enforcement. Therefore, we would be interested in discussing possible future solutions, especially those that do not generally weaken encryption, both its use, methods and development. More specifically, we would like to discuss the following questions:

- Does your government have general views you can share on the issue of encryption related to the interests of security of communications, national security and law enforcement?
- What technical possibilities do you consider possible without weakening encryption in general?
- What are the biggest obstacles to finding a solution in your experience?
- Does your government have specific technical, operational and/or legal solutions in place to tackle encryption in the interest of national security and law enforcement?
- What solutions does your government see as desirable or does your government foresee to implement in the near future?
- Would your government prefer an international / EU solution, for example EU legislation?

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** dinsdag 3 december 2019 11:39
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Interception and OTT
**Bijlagen:** nl-cabinet-encryption-position.pdf

Ha 10.2.e ik kan toch wel melden aan partners dat we een initiatief zijn gestart om in gesprek te gaan met publieke/private partners om toegang te krijgen tot data zonder encryptie structureel te verzwakken? Staat immers ook in de antwoorden op Kamervragen.

Dear 10.2.a

Thank you very much for your response and the contacts you provide. I understand how challenging these times can be, also in The Netherlands things seem to be moving quickly on this file. The questions I sent are part of a larger initiative to enter into a public/private dialogue and explore technological solutions to gaining access to data without structurally weakening encryption. In this way we strive to operate within the limits of the position of the Dutch government on encryption (attached). Given the complexity of the issue I look forward to learning about how other countries are dealing with the common challenges we face. Hopefully we can all benefit from the answers. Off course I understand some elements will be classified in that regard.

Let's stay in touch on further developments on this file and the best of luck in finalizing your view of encryption.

Yours sincerely,

10.2.e
Policy advisor cybercrime

.....
**Ministry of Justice and Security**
**Law Enforcement Department**
**Cybercrime unit**
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands
P.O. Box 20301 | 2500 EH | The Hague | The Netherlands
.....
**M** 10.2.e
10.2.e @minvenj.nl
www.government.nl/venj
.....

**Van:** 10.2.a en 10.2.e
**Verzonden:** dinsdag 3 december 2019 10:56
**Aan:** 10.2.e BD/DRC/CV ; 10.2.a en 10.2.e
**CC:** 10.2.a en 10.2.e ; 10.2.e @minbuza.nl
**Onderwerp:** RE: Interception and OTT

Dear Me 10.2.e

11.1 en 10.2.a

11.1 en 10.2.a

10.2.a en 10.2.e

You can reach them from me.

Best regards,

10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
10.2.a en 10.2.e

10.2.e @minbuza.nl
10.2.a RE: Interception and OTT

Dear 10.2.a en 10.2.e,

Due to our previous contact on interception of OTT I wanted to give you a head's up that we will go to Brussels to talk with Counsellors about access to encrypted data. We asked the Counsellors to contact subject experts in the capitals so these questions might find their way to you.

- Does your government have general views you can share on the issue of encryption related to the interests of security of communications, national security and law enforcement?
- What technical possibilities do you consider possible without weakening encryption in general?
- What are the biggest obstacles to finding a solution in your experience?
- Does your government have specific technical, operational and/or legal solutions in place to tackle encryption in the interest of national security and law enforcement?
- What solutions does your government see as desirable or does your government foresee to implement in the near future?
- Would your government prefer an international / EU solution, for example EU legislation?

Yours sincerely,

10.2.e
Policy advisor cybercrime

**Ministry of Justice and Security**
**Law Enforcement Department**
**Cybercrime unit**
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands
P.O. Box 20301 | 2500 EH | The Hague | The Netherlands

**M** 10.2.e

10.2.e @minvenj.nl
www.government.nl/venj

**Van:** 10.2.a en 10.2.e
**Verzonden:** maandag 28 oktober 2019 14:02
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.a en 10.2.e
10.2.e @minbuza.nl
**Onderwerp:** RE: Interception and OTT

Dear 10.2.e

11.1 en 10.2.a

Best,

10.2.a en 10.2.e

10.2.e BD/DRC/CV
10.2.a en 10.2.e
**Cc:** 10.2.a en 10.2.e ; 10.2.e @minbuza.nl
10.2.a Interception and OTT

Dear 10.2.a en 10.2.e and 10.2.a en 10.2.e

My name is 10.2.e and I am a policy advisor on cybercrime in the Ministry of Justice and Security in The Netherlands. A while ago I talked with 10.2.a en 10.2.e and 10.2.a en 10.2.e and they were so kind to provide me with your contact details if I had any questions regarding OTT.

In The Netherlands OTT services cannot be intercepted since they are not part of the traditional definition of telecommunication providers. 11.1 In The Netherlands there is some discussion on the room for manoeuvre on this topic based on the European Electronic Communications Code.

I am hoping my colleagues in other capitals have experienced similar discussions and wondered whether any conclusions have been reached. Did you have similar discussions in 10.2.a or are there other interesting steps taken on the interception of OTT's?

Thank you in advance for your response.

10.2.a .

Yours sincerely,

10.2.e
Policy advisor cybercrime

.....
**Ministry of Justice and Security**
**Law Enforcement Department**
**Cybercrime unit**
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands
P.O. Box 20301 | 2500 EH | The Hague | The Netherlands
.....
M 10.2.e
10.2.e @minvenj.nl
www.government.nl/venj
.....

---



---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

To the President of the House of Representatives
of the States General
Postbus 20018
2500 EA DEN HAAG

**Ministry of Security and Justice**

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

**Our reference**
708641

Date 4 January 2016
Subject Cabinet's view on encryption

**Cabinet's view on encryption**

Please find below the cabinet's view on encryption. This is in line with promises made during the debate of the standing committee on Economic Affairs on the Telecommunications Council of10 June 2015 (TK 2014-2015, 21501-33, no. 552) and the debate of standing committee on Security and Justice on the JHA Council of 7 October 2015.

**Introduction**

Encryption is increasingly easy to obtain and use and is thus more often part of regular data transactions. Encryption is increasingly applied by the government, companies and citizens to protect the confidentiality and integrity of their communication and stored data. This is important for people's confidence in digital products and services and for the Dutch economy in the light of a fast developing digital society. At the same time, encryption inhibits the acquisition of information required for investigation, intelligence and security services when malicious actors (such as criminals and terrorists) use it. The recent attacks in Paris, where encrypted communication may have been used by the terrorists, lead to the justified question what investigation, intelligence and security services need to have and retain good insight into the planning of attacks.

The ambiguity described in the preceding paragraph was also heard in the public debate of the last few months about the dilemmas of the use of encryption. The topic was also discussed in your House. During the debate of the standing committee on Economic Affairs on the Telecommunications Council the question was asked what the cabinet is planning to do to encourage the use of strong encryption. Additionally, the House of Representatives requested the cabinet to adopt a view on encryption.

The importance of encryption for the system and information security of the government and companies and for the constitutional protection of privacy and the confidentiality of communication is discussed below. The importance of detection of serious crimes and protection of national security are also included. Finally, a conclusion is reached after all interests have been assessed.

The situation in the Netherlands cannot be seen separately from its international context. Strong encryption software is increasingly available worldwide or an integral part of products or services. Considering the wide availability and application of advanced encryption techniques and the cross-border nature of data transaction, room for national action is limited.

**The importance of encryption for the government, companies and citizens**
Cryptography plays a key role in the technical security in the digital domain. Many cybersecurity measures in organisations are strongly based on the application of encryption. The secure storage of passwords, the protection of laptops against loss or theft and the secure storage of backups are more difficult without the use of encryption. The protection of data sent via the internet, for instance in internet banking, is only possible with the use of encryption. Due to the interconnectedness of networks, worldwide branching and the different routes communication can take, the risk of interception, infringement, perusal or modification of information and communication is always present.

The government increasingly communicates digitally with citizens and provides services whereby confidential information is exchanged, such as the use of a digital ID (DigiD) or filing a tax return. As formulated in the Coalition Agreement, citizens and companies must be able to arrange and settle their government affairs fully digitally from 2017 onwards. It is the duty of the government in that respect to make sure that this information is protected against third party examination; encryption is indispensable in that respect. The protection of the internal communication of the government also depends on encryption, for example with regard to the security of diplomatic and military communication.

Encryption is essential for companies to securely store and send company information. Being able to use encryption strengthens the international competitive position of the Netherlands and contributes to an attractive business and innovation climate for, for example, start-ups, data centres and cloud computing. Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digital economy.

Encryption supports the respect of personal privacy and confidential communication of citizens because it offers them a means to protect the confidentiality and integrity of personal data and communication. This is also important for exercising the freedom of expression. It enables citizens, but also professions with an important democratic function such as journalists, to communicate confidentially.

Encryption therefore enables all parties involved to ensure the confidentiality and integrity of communication and to better defend themselves against espionage and cybercrime. Fundamental rights and freedoms, security and economic interests benefit from this.

**Encryption and the investigation, intelligence and security services**
The powers and resources available to the services must be suited for the current and future digital reality. The investigation, intelligence and security services support the security of the digital and physical world with effective, lawful access to information. Where encryption is applied by malicious actors, it hinders the access to that information for the investigation, intelligence and security services.

They experience this for instance when they investigate the distribution and storage of child pornography, support military missions abroad, counter cyberattacks or when they want to gain and retain insight into the preparation of terrorist attacks. Criminals, terrorists and opponents in armed conflict are often aware that they might attract the attention of the services at some point in time and nowadays also have access to advanced encryption methods which are difficult to circumvent or break. The use of such methods requires little technical knowledge, as encryption is often an integral part of the internet services which they can use. That complicates, delays or renders it impossible to (timely) gain insight into the communication for the benefit of protecting national security and investigating criminal offences. Additionally, the investigative hearing at the trial and the case for a conviction can be seriously obstructed.

**The right to respect for personal privacy and privacy of correspondence of citizens**

As noted before, the use of encryption helps citizens secure their personal privacy and the confidentiality of their communication. The aforementioned lawful access to information and communication by the investigation, intelligence and security services however infringes on the confidential communication of citizens.

Privacy of communication relates to the constitutional respect for personal privacy and the right to protection of the privacy of correspondence, telephone and telegraph (hereinafter: 'privacy of correspondence'). These fundamental rights are rooted in Sections 10 and 13 respectively of the Constitution. These fundamental rights have also been laid down in Article 8 ECHR and Articles 7 and 8 of the EU Charter (to the extent it touches on EU Law).

The protection of fundamental rights applies to the digital world. The aforementioned constitutional and international law provisions together are the parameters for preventing illegal infringement. The rights mentioned are not absolute, which means that restrictions are allowed as long as they meet the requirements of the Constitution and the ECHR (and the EU Charter where EU law is concerned). An infringement is allowed if it serves a legitimate purpose, if it is regulated by law and if the restriction is foreseeable and known. The restriction must also be necessary in a democratic society. Finally, the infringement must be proportional, which means that the objective sought by the government must be proportionate to the infringement of the personal privacy and/or the privacy of communication.

These requirements are the parameters within which the balance can be decided between the interests at stake with encryption, such as the right to personal privacy and privacy of correspondence, public and national security and the prevention of criminal offences. To the extent it concerns the special powers of the intelligence and security services, the preceding assessment parameters have also been laid down in the Intelligence and Security Services Act 2002 (Sections 18 and 31). The obligations to cooperate regarding decryption that are included in the Intelligence and Security Services Act 2002 (Articles 24 (3) and 25 (7)) and in the Dutch Criminal Code (Article 126m (6)), may be invoked if associated special powers are exercised after an assessment as previously specified.

**Assessment and conclusion**

Nowadays the possibility to break encryption is decreasing. The possibility to obtain unencrypted information from a service provider is less often available.

Service providers increasingly process information that has already been encrypted through modern applications of encryption when it reaches them. Considering the importance of the investigation and prosecution of criminal offences and the interests involved in national security, these developments require a search for new solutions.

There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that use encryption. For instance, introducing technical access into an encryption product would make it possible for investigation services to inspect encrypted files, digital systems can become vulnerable to, for instance, criminals, terrorists and foreign intelligence services. This would have undesirable consequences for the security of communicated and stored information and the integrity of IT systems, which are increasingly important for the functioning of society.

For the performance of their statutory tasks, the investigation, intelligence and security services partly depend on cooperation with providers of IT products and services. Given this dependency, consultation with providers is needed about effectively providing information when their services are used by malicious actors, while taking into account to everyone's role and responsibilities and the statutory parameters.

Given the preceding assessment, the following conclusion is reached:

It is the responsibility of the cabinet to guarantee the security of the Netherlands and to investigate criminal offences. The cabinet underlines the necessity of lawful access to information and communication in this respect. Additionally, government authorities, companies, and citizens benefit from maximum security of digital systems. The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.

The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands. The Netherlands will disseminate this conclusion and the underlying assessment internationally. As regards the stimulation of strong encryption, the Minister of Economic Affairs will follow up on the purport of the amendment (TK 2015-2016, 34300 XIII, no.10) on the budget of the Ministry of Economic Affairs.

Minister of Security and Justice,

G.A. Van der Steur

Minister of Economic Affairs

H.G.J. Kamp

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 4 december 2019 17:20
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** FW: Minister mbt encryptie

**Van:** 10.2.e
**Verzonden:** woensdag 4 december 2019 16:07
**Aan:** 10.2.e BD/DRC/CV ; 10.2.e BD/DRC/CV
**CC:** 10.2.e 10.2.g ; 10.2.e 10.2.g ; 10.2.e (10.2.g ; 10.2.e ; 10.2.e ; 10.2.e ; 10.2.e )
**Onderwerp:** Minister mbt encryptie

Met vriendelijke groet,

10 2.e
Public Policy Manager

T: +10.2.e
M: 10.2.e

10.2.g

10.2.g

---------- Forwarded message ---------
From: **POLITICO Pro Article**<proarticles@politico.eu>
Date: Wed, Dec 4, 2019 at 10:12 AM
Subject: Dutch minister urges EU action to fight child pornography online
To: POLITICO Pro Subscribers

## Dutch minister urges EU action to fight child pornography online

-- By Laurens Cerulus
12/4/19, 11:11 AM CET | View in your browser

The Dutch minister of justice and security is calling on the European Union to crack down on child exploitation online by granting law enforcement more access to data held by tech companies, including encrypted messaging.

Ferdinand Grapperhaus said that a new EU law on data access would allow police investigators to force social media companies like Facebook and Google to hand over electronic evidence to prosecute child exploitation networks.

"Internet companies have shown they're willing. They have adopted codes of conduct and said they'd take down child pornography as quickly as possible. But using encryption to exchange child pornography should simply be made impossible," he told POLITICO.

Putting legal requirements on internet platforms and services means "you'll have an authority that can pick up this work, that can name and shame too," he added.

Legal obligations to hand over data would mean that smaller platforms would also fall under the same requirements, Grapperhaus said.

"There are parties with bad intentions," he said, referring to smaller platforms that fall outside the scope of many self-regulatory efforts endorsed by internet companies. "You can't force those to respect voluntary commitments."

The EU has a law in place to combat sexual abuse and exploitation of children, including legal provisions to fight child pornography online. Countries have also pushed for safeguards to fight child pornography online in internet governance bills like the proposed e-Privacy Regulation.

But several governments have sought stronger powers to fight the growing problem of online child pornography — notably targeting internet companies for their role in hosting platforms used for exchanging abusive material.

The EU's law enforcement agency Europol told POLITICO recently it sees the growing amount of child exploitation material as a key cybercrime issue. "The amount of indecent images of children available is being fueled substantially by self-generated material [through] increasing access of children to high-quality smartphones taking high-quality images," Steven Wilson, head of Europol's European Cybercrime Centre (EC3), said.

According to Grapperhaus, reports of child exploitation material went from 3,000 in 2012 to 18,000 in 2017 and up to 40,000 this year.

The Dutch minister's statements also fit within growing calls from selected EU capitals to broaden state powers to police the internet — despite concerns of privacy activists that doing so could violate privacy and threaten data security.

In a conversation with POLITICO earlier this week, Sweden's Home Affairs Minister Mikael Damberg called on the new Commission to revamp efforts to create a pan-European data retention regime. While the European Court of Justice has issued repeated rulings striking down such privacy-invading police powers in several EU countries, Damberg said that times had changed.

Grapperhaus was on his way to Washington D.C. to discuss cybersecurity, lawful access to data and other issues this week. Among other meetings he will be sitting down with U.S. Attorney General William Barr, who launched an effort in October to make U.S. tech giants give police forces access to encrypted data.

"I have expressed similar concerns within the EU," said Grapperhaus. "I understand the importance of encryption but I think we should come to an understanding with internet companies about access keys if we have suspicions of serious crimes," he said.

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** dinsdag 10 december 2019 12:46
**Aan:** 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV
**CC:** 10.2.e - BD/DRC/CV
**Onderwerp:** FW: JenV-breed VS-overleg (met name terugkoppeling werkbezoek MJenV aan de VS)
**Bijlagen:** Mijn aantekeningen

Hierbij de aantekeningen van 10.2.e. 11.1

**Van:** 10.2.e - BD/DEIA/IBP
**Verzonden:** dinsdag 10 december 2019 12:39
**Aan:** 10.2.e BD/DRC/CV
**Onderwerp:** RE: JenV-breed VS-overleg (met name terugkoppeling werkbezoek MJenV aan de VS)
Dag 10.2.e
Zie bijgaande aantekeningen opgesteld door 10.2.e van het gesprek met
Ik was zelf niet aanwezig bij dit gesprek, dus als jou iets niet geheel duidelijk is, graag even met 10.2.e bellen; ik ben tot vrijdag met verlof.
Groet,
10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 10 december 2019 12:34
**Aan:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: JenV-breed VS-overleg (met name terugkoppeling werkbezoek MJenV aan de VS)
Hallo 10.2.e
Kun je alvast een inhoudelijke terugkoppeling geven op wat er is gezegd over encryptie? Wij moeten gaan bellen met de Amerikanen en horen graag wie wat heeft gezegd.
Ik kan er helaas de 16e niet bij zijn ik stuur je verzoek door naar 10.2.e en 10.2.e
Groet,
10.2.e

-----Oorspronkelijke afspraak-----
**Van:** 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 10 december 2019 12:16
**Aan:** 10.2.e

**CC:** 10.2.e
**Onderwerp:** JenV-breed VS-overleg (met name terugkoppeling werkbezoek MJenV aan de VS)
**Tijd:** maandag 16 december 2019 09:30-11:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
**Locatie:** N36-10; Noord-Brabantzaal-JenV

Beste collega's,
Graag nodig ik jullie hierbij uit voor het eerstvolgende JenV-brede VS-overleg, dat plaats zal vinden op maandag 16 december a.s., 09.30-11.00 uur in de Noord-Brabantzaal (N36.10) van het Ministerie van JenV.
Op 2 december jl. zond ik al de bijgaande 'Save the date' voor dit overleg.
Zoals daaruit blijkt zal het overleg op 16 december voornamelijk terugblikken op het werkbezoek dat minister Grapperhaus van 3 t/m 6 december jl. heeft gebracht aan de VS.
Een uiterst korte weergave van dat werkbezoek, treffen jullie hieronder aan. Het concept verslag van het werkbezoek volgt later deze week.
Ik stel de volgende concept-agenda voor:

1. Opening en mededelingen
2. Verslag JenV-breed VS-overleg van 4 oktober 2019
3. Terugblik op de ontmoeting tussen de MJenV en 10.2.a (zie bijgaand verslag)
4. Terugblik op het werkbezoek van de MJenV aan Washington DC / presentatie door 10.2.e
5. Vooruitblik op de mogelijke vervolgontmoeting tussen de MJenV en 10.2.a (16/1/20; 12.30-13.00; M08.314):
   met name Buiten reikwijdte ' en mogelijkheden Buiten reikwijdte
6. Rondvraag / sluiting.

Graag tot 16 december a.s.
Eventuele aanmeldingen voor toegang tot het Ministerie graag sturen aan het Secretariaat van DEIA (zie cc).

**Korte terugblik werkbezoek MJenV aan Washington (3-6 december 2019):**
De hoofdthema's van de diverse gesprekken van de MJenV in de VS met zijn Amerikaanse counterparts betroffen:
1. Cybersecurity/economische veiligheid
2. Drugs/ondermijning
3. Aanpak kindermisbruik

Hiertoe heeft de MJenV gesprekken gevoerd met o.a. 10.2.a Ook is onder andere een bezoek gebracht aan het National Center for Missing and Exploited Children.
De MJenV heeft verder ook een goed bezochte lezing gegeven aan het Centre for Strategic and International Studies (CSIS) over de internationale bestrijding van cybercriminaliteit.
Het eerder geplande besprek met de 10.2.a kon geen doorgang vinden vanwege een gelijktijdige bespreking van de heer 10.2.a met President Trump.
De ontmoeting met het 10.2.a krijgt mogelijk in januari al een vervolg. De 10.2.a bezoekt dan Nederland en een afspraak met de MJenV is in gang gezet. Onderwerp van gesprek zal dan onder meer Buiten reikwijdte

Met vriendelijke groet,
10.2.e

10.2.e
Coördinator Internationale Relaties: VS, Canada, Westelijke Balkan, Turkije en EU-uitbreiding

.....
**Ministerie van Justitie en Veiligheid**
**Directie Europese en Internationale Aangelegenheden**
**Internationale Betrekkingen en Projecten**
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**
.....

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** vrijdag 13 december 2019 11:21
**Aan:** 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV
**Onderwerp:** RE: gesprek over versleuteling

Ihkv verbreding is het in dit geval goed om 10.2.e (pag). 10.2.e (OvJ) en 10.2.e van het OM aan te sluiten en 10.2.e .

In hoeverre nemen de nadelige consequenties van encryptie voor interceptie toe? Zijn deze consequenties meer zichtbaar bij bepaalde typen misdrijven? Welke typen interceptie worden het meest hierdoor geraakt? Soorten aanbieders, ip-tap, etc.

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** donderdag 12 dec. 2019 16:03
**Aan:** 10.2.e /DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** FW: gesprek over versleuteling

Deel 2!

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** Grapperhaus, F.B.J. - BD/AL <10.2.e @minjenv.nl>
**Datum:** donderdag 12 dec. 2019 4:27 PM
**Aan:** 10.2.e 10.2.g . Secretariaat - Minister van Justitie en Veiligheid <10.2.e @minjenv.nl>
**Kopie:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, Dam, A. van - BD/DGRR 10.2.e @minjenv.nl>, 10.2.e 10.2.g
**Onderwerp:** RE: gesprek over versleuteling

10.2.e

Dat lijkt mij ok. Dan wordt het wel een breder gesprek dus meer tijd.

Groet
Ferd Grapperhaus

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e 10.2.g
**Datum:** donderdag 12 dec. 2019 13:27

**Aan:** Grapperhaus, F.B.J. - BD/AL <10.2.e @minjenv.nl>, Secretariaat - Minister van Justitie en Veiligheid 10.2.e @minjenv.nl>
**Kopie:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, Dam, A. van - BD/DGRR <10.2.e @minjenv.nl>, 10.2.e 10.2.g
**Onderwerp:** gesprek over versleuteling

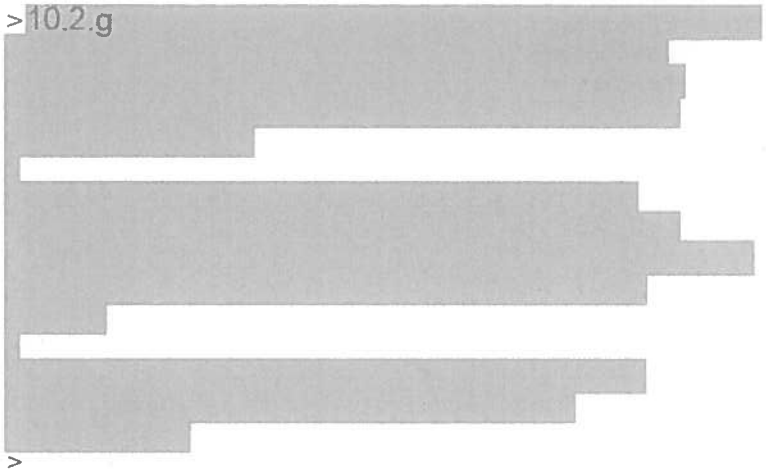
Geachte minister, beste Ferd,

Vriendelijk dank voor de snelle positieve reactie. Een paar punten:

-10.2.g

Met vriendelijke groet,
10.2.e .

On 12-12-2019 11:59, Grapperhaus, F.B.J. - BD/AL wrote:
> Beste 10.2.e
>
> 11.1 Eerlijk gezegd strekt
> mijn voornemen niet zo ver als in sommige mediaberichten is gesuggereerd.
> Ik ben desalniettemin graag bereid om een door jou geleid gesprek aan te
> gaan met cyber-experts over het onderwerp 11.1
>
>
> Groet,
> Ferd
>
> Verzonden met BlackBerry Work
> (www.blackberry.com)
>
>
> *Van: 10.2.e 10.2.g >
> *Datum: *woensdag 11 dec. 2019 09:38
> *Aan: *Secretariaat - Minister van Justitie en Veiligheid
> <mailto 10.2.e@minjenv nl>>
> *Kopie: 10.2.e 10.2.g >
> *Onderwerp: 10.2.e > AFSPRAAK>minister
> Grapperhaus10.2.g 10.2.e 10.2.g
> 10.2.g DGPSenB/10.2.e :10.2.g
10.2.g

>
> Beste 10.2.e
>
> 10.2.g

>
> Ik hoor het graag.
>
> Met vriendelijke groet.
> 10.2.e
>
>
> On 19-02-2019 14:50, Secretariaat - Minister van Justitie en Veiligheid
> wrote:
>> Geachte heer 10.2.e
>>
>>
>>
>> Minister Grapperhaus vroeg mij een afspraak met u te maken. Kunt u op 2
>> april 2019, 11.30 - 12.30 uur? Locatie: Den Haag/Turfmarkt
>> 147/ministerie van Justitie en Veiligheid/M.08.314
>>
>>
>>
>> Graag verneem ik van u.
>>
>>
>>
>> Met vriendelijke groet,
>>
>> *10.2.e
>> Secretaresse van de Minister van Justitie en Veiligheid
>>
>> .....
>> *Ministerie van Justitie en Veiligheid
>> Bureau Secretaris-Generaal*
>> Turfmarkt 147 | 2511 DP | Den Haag | M.08.311
>> Postbus 20301 | 2500 EH | Den Haag
>> .....
>> *T 10.2.e
>> 10.2.e@minvenj.nl <10.2.e @minvenj.nl>
>>
>>
> ----------
>
> Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u
> niet de geadresseerde bent of dit bericht abusievelijk aan u is
> toegezonden, wordt u verzocht dat aan de afzender te melden en het
> bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor
> schade, van welke aard ook, die verband houdt met risico's verbonden aan
> het elektronisch verzenden van berichten.
>

> Ministerie van Justitie en Veiligheid
>
> This message may contain information that is not intended for you. If
> you are not the addressee or if this message was sent to you by mistake,
> you are requested to inform the sender and delete the message. The State
> accepts no liability for damage of any kind resulting from the risks
> inherent in the electronic transmission of messages.
>
> Ministry of Justice and Security
>

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 7 januari 2020 12:46
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV
**Onderwerp:** FW: Verslag encryptie hearing
**Bijlagen:** Verslag hearing the balance of end 2 end encryption.docx

TI, verslag hearing van het Congres. 11.1

**Van:** 10.2.e
**Verzonden:** maandag 6 januari 2020 21:44
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** Verslag encryptie hearing

Dag 10.2.e

Ik ben vergeten het verslag van de hearing over encryptie in de senaat richting jou te sturen.
Bij dezen.

Gr.

10.2.e
Ministry of Justice and Security
Embassy of the Kingdom of the Netherlands
4200 Linnean Avenue NW, Washington DC
M: 202-894-0793

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 7 januari 2020 14:17
**Aan:** 10.2.e - BD/DRC/FO; 10.2.e - BD/DRC/CV; 10.2.e . - BD/DRC/CV
**CC:** 10.2.e - BD/DRC/FO; 10.2.e - BD/DRC/GC
**Onderwerp:** RE: Kaderinstructie strategische richtsnoeren compilatie tot dusver

Inmiddels met 10.2.e gesproken.

Op encryptie wordt ingezet via de richtsnoeren. 11.1

Interceptie en OTT wordt uit de richtsnoeren gehouden om het separate traject te bewandelen.

OK wat mij betreft dus zo.

Groet,

10.2.e

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 7 januari 2020 13:05
**Aan:** 10.2.e - BD/DRC/FO ; 10.2.e BD/DRC/CV ; 10.2.e BD/DRC/CV
**CC:** 10.2.e - BD/DRC/FO ; 10.2.e - BD/DRC/GC
**Onderwerp:** RE: Kaderinstructie strategische richtsnoeren compilatie tot dusver

Ha 10.2.e ,

Ik heb voor het kerstreces voorgesteld om interceptie en OTT uit de richtsnoeren te houden en het separate traject te volgen. Interceptie en OTT is nauw verbonden met encryptie. Onderstaande passage staat nu in het document.

Kun je iets meer duiding geven van de intentie van deze passages en de gevolgen daarvan? Op wiens verzoek zijn deze passages geformuleerd en opgenomen? 11.1

- **Encryptie (verkenning NL)**

Wat zijn de plannen?
11.1

Bereiken (engels)
- 11.1

Vermijden (engels)
A 11.1

Krachtenveld
Wordt momenteel in kaart gebracht.

Welke actie nodig qua beïnvloeding/verbetering info positie:
11.1

- **Interceptie & Data retentie**

Wat zijn de plannen?
11.1

Bereiken (engels)
11.1

11.1

Vermijden (engels)
11.1

Krachtenveld
11.1

Welke actie nodig qua beïnvloeding/verbetering info positie:
11.1

**Van:** 10.2.e BD/DRC/FO 10.2.e @minjenv.nl>
**Verzonden:** maandag 6 januari 2020 12:39
**Aan:** 10.2.e @minjenv.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>; 10.2.e BD/DRC/GC 10.2.e @minjenv.nl>
**Onderwerp:** FW: Kaderinstructie strategische richtsnoeren compilatie tot dusver

Dag allemaal, zie hierbij, mede op basis van onze input, de voorlopige conceptinstructie van DEIA voor de discussie over de strategische richtsnoeren. DEIA wil daar van de week met de betrokken directies verder over praten. We houden jullie op de hoogte. Groeten, 10.2.e

**Van:** 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 24 december 2019 15:12
**Aan:** 10.2.e
**CC:** 10.2.e <v.c.s.sanders@minjenv.nl>; Boom, S.M. - BD/DEIA/EU <s.m.boom@minjenv.nl>; l.j.m.lingketon@minbuza.nl
**Onderwerp:** Kaderinstructie strategische richtsnoeren compilatie tot dusver

Beste collega's,

Hierbij de compilatie van jullie inbreng voor de kaderinstructie (nog zonder selectie/prioritering), met veel dank voor jullie bijdragen. Begin januari plan ik een afspraak in voor de week van 6 januari en kom ik verder terug op het proces.

Fijne Kerst!

Groet,

10.2.e

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 7 januari 2020 16:22
**Aan:** 10.2.e BD/DRC/CV
**Onderwerp:** Dossiernotitie bezoek 10.2.e aan MinJenV 16jan2020
**Bijlagen:** Dossiernotitie bezoek 10.2.e aan MinJenV 16jan2020.doc

Ha 10.2.e

Een enkele suggestie. 11.1

Maar heb het zo gelaten.

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** woensdag 2 oktober 2019 16:20
**Aan:** 10.2.e (Landelijk Parket)'
**CC:** 10.2.e van (PaG Den Haag)
**Onderwerp:** RE: Antw: Terugkoppeling presentatie OTT
**Bijlagen:** Nota interceptie OTT samenvatting.docx; Interceptie en OTT.pptx

Ha 10.2.e

Dit is h'm uiteindelijk geworden.

+ presentatie.

**Van:** 10.2.e (Landelijk Parket) 10.2.e @om.nl]
**Verzonden:** woensdag 2 oktober 2019 16:13
**Aan:** 10.2.e - BD/DRC/CV
**CC:** 10.2.e (PaG Den Haag)
**Onderwerp:** Antw: Terugkoppeling presentatie OTT

11.1 Heel mooi. Ongeacht de uitkomst is dit m.i. een belangrijke exercitie. Heb jij misschien de definitieve versie van de nota die aan de Minister is gezonden. Wij hebben daar destijds met 10.2.e ook aan gewerkt. Groet! 10.2.e

---

**Van:** 10.2.e - BD/DRC/CV
**Datum:** 2 oktober 2019 om 15:34:59 CEST
**Aan:** 10.2.e

**Onderwerp:** Terugkoppeling presentatie OTT

Hallo collega's,

Ik zou jullie nog mailen over de presentatie bij MJenV over de OTT diensten.

11.1 De minister is akkoord met het inventariseren van een Europese oplossing voor het interceptievraagstuk vwb OTT diensten. Dit inventariseren gaat gebeuren met bepaalde EU partners en hij heeft graag dat we dit snel afronden. Hij is zich bewust van de waardenspanning die we in de nota hebben geformuleerd.

BTW excuus voor de vergaderingen spam, als ik een zaal wijzig moet blijkbaar iedereen dat accepteren. Er komt nog een wijziging bij, 10.2.e attendeerde mij erop dat we een afspraak hebben op 5 december waardoor dit voor mensen met kleine kinderen een minder geschikt tijdstip is...

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2.e
10.2.e @minvenj.nl

---

10.2.e DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** vrijdag 11 oktober 2019 11:19
**Aan:** 10.2.e BD/DJOA/JBOZ
**Onderwerp:** RE: Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

Hallo 10.2.e

Ik ga wat dichten.

Groet,

10.2.e

---

**Van:** 10.2.e BD/DJOA/JBOZ
**Verzonden:** donderdag 10 oktober 2019 14:45
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

Beste 10.2.e

Van mijn collega, 10.2.e, heb ik begrepen dat jij input kan leveren voor de beantwoording van bovengenoemde set Kamervragen.
Kun je mij voorzien van input voor de beantwoording van deze vragen?

Met vriendelijke groet,

10.2.e )

T 10.2.e
E 10.2.e @minjenv.nl
**Afwezig op woensdag**
.....
**Ministerie van Justitie en Veiligheid**
Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden
Afdeling Juridische, Bestuurlijke en Operationele Zaken

Turfmarkt 147 | 2511 DP | Den Haag | N19
Postbus 20301 | 2500 EH | Den Haag | 070-3706663
www.rijksoverheid.nl/venj
.....

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** maandag 14 oktober 2019 17:10
**Aan:** 10.2.e - BD/KS; 10.2.e - BD/DBAenV/IenK; 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/PNDV
**Onderwerp:** Donderdag 17 okt

Hallo 10.2.e en 10.2.e

Voor aanstaande donderdag wilde ik voor de 'actualiteit' een spreeklijn op encryptie en FB meegeven:

Achtergrond:
Het lid Verhoeven heeft op 7 okt jl. een Mondelinge vraag gesteld over het bericht: 'Minister bezorgd om versleuteling Facebook', nadat deze Mondelinge vraag niet is goedgekeurd zijn 9 okt. jl. schriftelijke vragen ontvangen.

Kern:
Het lid maakt zich zorgen over effecten die het initiatief van de VS, VK en AUS kan hebben op encryptie. Hij vraagt zich af hoe uw 'begrip' voor dit initiatief zich verhoudt tot het Nederlandse encryptiestandpunt en wat de inzet wordt van het gesprek dat u gaat voeren in Washington.

Spreeklijn:
11.1

Kunnen jullie hier op- of aanmerkingen op geven?

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

.....
**Ministerie van Veiligheid en Justitie**
**Directie Rechtshandhaving en Criminaliteitsbestrijding**
**Cybercrime unit**
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**
.....

Buiten reikwijdte

Buiten reikwijdte

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 16 oktober 2019 18:09
**Aan:** 10.2.e - BD/DRC/CV; Dam, A. van - BD/DRC
**CC:** 10.2.e BD/DRC/CV; 10.2.e - BD/DBAenV/IenK; 10.2.e - BD/PNDV
**Onderwerp:** Gesprek minister met 10.2.g
**Bijlagen:** 211.1 FB en 11.1 .docx; 211.1 10.2.g .docx; 2a 11.1 Nota MJ&V 11.1 .docx; 2b 11.1 11.1 MJ&V 11.1 .docx; 3 11.1 factsheet en QenA.docx; Oplegnota.docx

Hallo Annemieke en 10.2.e
Vanmiddag hebben we bijgevoegde voorbereiding bij de minister afgeleverd vanuit DGRR. Dit is samengevoegd met de voorbereiding van de NCTV.
Morgen is er maar 15 minuten tijd volgens de PA, dus er zal niet veel besproken worden.
Onverwacht werd ik bij het afleveren van de dossiers de kamer ingeroepen en heb per onderwerp in ieder geval het hoofdpunt toegelicht.
11.1
Buiten reikwijdte
Ter info:
Vanuit de NCTV is de minister voorbereid op 11.1
Hierover zou ook binnen twee weken (voor het AO cybersecurity van 30 oktober) een brief voor naar de Kamer moeten. Op dit moment lijkt dit geen raakvlakken te hebben voor DRC.
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minveni.nl

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** dinsdag 22 oktober 2019 12:45
**Aan:** 10.2.e
**CC:** 10.2.e BD/DRC/CV
**Onderwerp:** RE: KV versleuteling Facebook

Hallo 10.2.e

Dankjewel voor de reactie. Ik ben dichterbij de agreed text van het encryptiestandpunt gaan zitten. Ik mail de versie zo rond. 11.1

Groet,

10.2.e

**Van:** 10.2.e
**Verzonden:** vrijdag 18 oktober 2019 10:10
**Aan:** 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: KV versleuteling Facebook

Ha 10.2.e hierbij onze wijzigingsvoorstellen (att). Met deze wijzigingen kunnen we akkoord gaan met de antwoorden.

Belangrijkste punt zit wat ons betreft 11.1

Groet, 10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 15 oktober 2019 11:38
**Aan:** 10.2.e
@minjenv.nl>; 10.2.e @minjenv.nl>
**Onderwerp:** KV versleuteling Facebook

Beste collega's,

Er is een set Kamervragen gesteld naar aanleiding van de voornemen van Facebook om meer berichtgeving end-to-end te versleutelen en het initiatief tot overleg van de VS, VK en Australië.

Ik heb bijgevoegde conceptantwoorden opgesteld op basis van het encryptiestandpunt. Zouden jullie hier deze week naar willen kijken? Mochten jullie concrete suggestie hebben, dan lees ik deze graag

via 'track changes' de tekst. 'Comments' in de zijlijn worden niet overgenomen. Wanneer het niet lukt hier deze week op te reageren geef dan svp een seintje anders gaat het proces richting akkoord van de minister door.

Alvast bedankt.

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

.....
**Ministerie van Veiligheid en Justitie**
**Directie Rechtshandhaving en Criminaliteitsbestrijding**
**Cybercrime unit**
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**
.....

---

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** woensdag 23 oktober 2019 13:50
**Aan:** 10.2.e - BD/DBAenV/IenK; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Tekst openbrief Facebook

Ha 10.2.e

Ik zou bij ad 1, ook aangeven dat 11.1 Conform huidige staand beleid. Kleed je het iets meer in.

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Datum:** woensdag 23 okt. 2019 1:06 PM
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: Tekst openbrief Facebook

Bijgaand versie 4 en de memo voor DGSTAF. Ingekort en opgeschoond. 11.1
Dank voor de input. 10.2.e reageert nog even later vandaag. Groet!

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** woensdag 23 oktober 2019 10:44
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e BD/DBAenV/IenK; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Tekst openbrief Facebook
Hi allen,
Ik begreep dat DCOM alleen meekijkt en niet meeschrijft, klopt dat? Hierdoor werd ik getriggerd om weer naar de tekst te kijken die 10.2.e had aangepast.
In de bijlage versie 3. Ik twijfel erg over de laatste twee alinea's. Wellicht kan jij die scherper maken 10.2.e Zowel inhoudelijk als tekstueel.
Mvg,
10.2.e

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 23 oktober 2019 9:21
**Aan:** 10.2.e BD/DBAenV/IenK; 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV
**Onderwerp:** RE: Tekst openbrief Facebook
Ha 10.2.e,
Sorry voor de vertraging. Ik reageer vandaag!

**Van:** 10.2.e BD/DBAenV/IenK
**Verzonden:** dinsdag 22 oktober 2019 15:37
**Aan:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e BD/DRC/CV
**Onderwerp:** FW: Tekst openbrief Facebook
Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e - BD/DCOM/P&B 10.2.e @minjenv.nl>
**Datum:** dinsdag 22 okt. 2019 2:48 PM
**Aan:** 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>, 10.2.e - BD/DCOM/P&B 10.2.e @minjenv.nl>
**Onderwerp:** RE: Tekst openbrief Facebook

Dag 10.2.e
Zie mijn trackies. Het lijkt me best een interessant thema.
Ik twijfel over de aanloop.
Moeten we niet sneller ter zake komen?
Ons punt maken en dan uitleggen waarom?
Daarbij vbb uit de praktijk halen van interventies die nog wel konden en straks niet meer kunnen.
En filosoferen over toekomstige problemen.
Als dit doorgaat dan....
Sorry, verder kom ik nu niet, ik ben heel druk.
GR!

**Van:** 10.2.e - BD/DBAenV/IenK
**Verzonden:** dinsdag 22 oktober 2019 11:32
**Aan:** 10.2.e - BD/DCOM/P&B; 10.2.e - BD/DCOM/P&B
**Onderwerp:** Tekst openbrief Facebook

Ha [redacted] en 10.2.e
Bijgaand een voorstel voor een openbrief van minister JenV over Facebook, versleuteling (encryptie) en KP. Ik wil een platte tekst graag in het Stafoverleg DGRR van aanstaande maandag met hem bespreken. Een oplegmemo volgt nog.
Zouden jullie even willen kijken of dit wat is en of er een betere tekst van te maken valt? Ik sleutel er ook nog verder even aan...
Dank en groet,
10.2.e
Programmamanager
10.2.e

10.2.e /DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 18:54
**Aan:** 10.2.e - BD/DCOM/P&B; 10.2.e - BD/DBAenV/IenK
**CC:** 10.2.e - BD/DRC/CV; 10.2.e BD/DBO; 10.2.e BD/DCOM/P&B; Dam, A. van - BD/DRC
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Bijlagen:** Input interview Nieuwsuur.docx

Hallo 10.2.e

Hierbij de input van Nieuwsuur die 10.2.e en ik hebben opgesteld.

Groeten,

10.2.e

**Van:** 10.2.e - BD/DCOM/P&B
**Verzonden:** maandag 28 oktober 2019 16:59
**Aan:** 10.2.e BD/DBAenV/IenK ; 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DBO ; 10.2.e - BD/DCOM/P&B
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hi all,

Ik heb nog even gebeld met Nieuwsuur. Zie hieronder.

Heb de punten van de vorige keer ook weer gebruikt. Graag nog evt jullie aanvulling/11.1 Dan bundel ik alles en stuur het naar de minister. Afhankelijk van tijdstip schorsing, wordt het dus tussen 12-14 opgenomen morgen.

Nog niet bekend wanneer de uitzending is.

10.2.e

**Insteek uitzending**

- uitleg wat E2E is
- Wat Barr e.a. willen
- Gesprek met Verhoeven nav de Kamervragen
- Gesprek met Grapperhaus
- 11.1

**Vragen aan Ferd:**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?
  - 11.1

- Is dit een nieuw probleem of al bekend?
  - 11.1 [redacted]
- Wat zijn deze zorgen precies?
- Waarom precies kinderporno?
  - 11.1 [redacted]
- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?
  - 11.1 [redacted]

**Openbrief – platte tekst**

11.1 [redacted]

11.1 [redacted]

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** dinsdag 29 oktober 2019 09:12
**Aan:** 10.2.e - BD/DCOM/P&B
**Onderwerp:** FW: voorbereiding nieuwsuur
**Bijlagen:** Input interview Nieuwsuur.docx

Kleine wijziging ten behoeve van de printjes, zoals gisteren gesmst.

**Van:** 10.2.e - BD/DCOM/P&B
**Verzonden:** dinsdag 29 oktober 2019 09:09
**Aan:** Grapperhaus, F.B.J. - BD/AL
**CC:** 10.2.e - BD/DBO ; 10.2.e - BD/DBAenV/IenK ; 10.2.e - BD/DRC/CV ; 10.2.e BD/DRC/CV ; 10.2.e - BD/DCOM/P&B
**Onderwerp:** voorbereiding nieuwsuur

Dag Ferd,

Zoals besproken gister sta je vanmiddag tijdens de lunchschorsing Nieuwsuur te woord over E2E. Hieronder de opzet van de uitzending en de vragen die ze jou gaan stellen incl korte QenA. In bijlage vind je de uitgebreide voorbereiding van 10.2.e en 10.2.e Met daarin zoals besproken de kaders waarbinnen je moet blijven.

Ik zorg ook voor printjes.

10.2.e

**Insteek uitzending**

- uitleg wat E2E is
- Wat Barr e.a. willen
- Gesprek met Verhoeven nav de Kamervragen
- Gesprek met Grapperhaus
- 11.1

**NB**

- 11.1

**Vragen aan Grapperhaus**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?
  - 11.1
- Is dit een nieuw probleem of al bekend?
  - 11.1

- 11.1 [redacted]

- Wat zijn deze zorgen precies?
- Waarom precies kinderporno?
  - 11.1 [redacted]
- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?
  - 11.1 [redacted]

Met vriendelijke groet,

10.2.e [redacted]
Woordvoerder

.....
**Ministerie van Justitie en Veiligheid**
**Directie Communicatie**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
**M** 10.2.e [redacted]
10.2.e [redacted] @minjenv.nl
www.rijksoverheid.nl/jenv
.....
**Voor een rechtvaardige en veilige samenleving**
.....

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 31 oktober 2019 10:19
**Aan:** 10.2.e (PaG Den Haag)'
**CC:** 10.2.e @om.nl; 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV
**Onderwerp:** RE: Non paper interception OTT

Ha 10.2.e

Dankjewel! Het proces met de 10.2.a moeten we zeker verder uitlopen. Bij navraag gebruiken de 10.2.a de term elektronische communicatiedienst ipv de interpersoonlijke communicatiedienst. Daarnaast zijn ook de 10.2.a nationaal bezig. Waar de 10.2.a het encryptieprobleem erkennen, erkennen de 10.2.a de problematiek rond de handhaving.

11.1 Ik neem de richting waar de non-paper naartoe moet gaan over.

Wat we op de achtergrond moeten bedenken is dat 11.1

Mijn inschatting is, 11.1

Maar dat is inderdaad iets voor (veel later) in het proces. Het volgende concept zal alleen op hoofdlijnen zien. Ik ben er wel voorstander van om 11.1

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e (PaG Den Haag)
**Verzonden:** woensdag 30 oktober 2019 19:03
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Non paper interception OTT

Ha 10.2.e

Onlangs spraken wij elkaar al even telefonisch over het non-paper. Mijn eerste reactie was dat ik 11.1 Ik heb het stuk gisteren

tijdens ons interne interceptieoverleg besproken met 10.2.e en 10.2.e Daaruit wil ik je graag het volgende teruggeven:

- Inmiddels is het non-paper enigszins ingehaald door het bericht uit 10.2.a alwaar men voornemens is [redacted] Wij denken dat we gezien deze ontwikkeling 11.1 [redacted]
- Hierbij is van belang dat 11.1 [redacted]
- We vragen ons af of 11.1 [redacted] Kort gezegd denken wij 11.1 [redacted]
- Als we voor het non-paper nog enige richting mogen meegeven, dan zou dit de navolgende zijn. Wij zouden de onderwerpen 11.1 [redacted]
- We zouden daarom meer focus willen leggen op 11.1 [redacted] Een argument om dit te willen regelen 11.1 [redacted]
- In verband met het encryptiestandpunt zou een oplossingsrichting kunnen zijn dat 11.1 [redacted]

Ik hoop dat je hiermee verder kunt. Laat het vooral weten indien iets niet duidelijk is en tot slot: 11.1 [redacted] 11.1

Dank en hartelijke groet,
10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl]
**Verzonden:** maandag 21 oktober 2019 22:49
**Aan:** 10.2.e (PaG Den Haag); 10.2.e (Landelijk Parket); 10.2.e @politie.nl; 10.2.e - BD/PIDS; 10.2.e - BD/KS
**CC:** 10.2.e (Parket-Generaal); 10.2.e (Landelijk Parket Rotterdam)
**Onderwerp:** Non paper interception OTT

Hallo allemaal,

Zoals jullie weten heeft de minister het akkoord gegeven om bij enkele lidstaten te inventariseren of zij interesse hebben in Europese regelgeving rond het kunnen aftappen van OTT's.

In overleg met de internationale directie heb ik een non-paper gemaakt. Dit paper stelt haar in staat om te inventariseren bij een beperkte groep LS om te bezien of zij ook oren hebben naar een Europese regeling om OTT's af te tappen.

Een non-paper zou de probleemstelling, context en oplossingsrichting duidelijk moeten maken.

Ik heb dit geprobeerd in bijgevoegde non-paper, zouden jullie er eens naar willen kijken? Brengt dit paper de noodzaak duidelijk genoeg naar voren? Ik verspreid het paper bewust nog even onder de JenV organisaties, dus verspreid h'm svp niet.

Groeten,

10.2.e

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2 e
10.2.e @minvenj.nl

---

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** donderdag 31 oktober 2019 16:13
**Aan:** 10.2.e BD/DJOA/JBOZ
**CC:** 10.2.e - BD/DJOA/JBOZ
**Onderwerp:** RE: KV 'Minister bezorgd om versleuteling Facebook'

Halo 10.2.e

Ja, zondag is er een uitzending van nieuwsuur waar de minister op dit onderwerp ingaat. Dit wil ze afwachten. Daarnaast heeft ze gevraagd om 11.1 ... Ik ga hiermee aan de slag. Ik zag dat het uitstelverzoek was verzonden.

**Van:** 10.2.e - BD/DJOA/JBOZ
**Verzonden:** donderdag 31 oktober 2019 15:48
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: KV 'Minister bezorgd om versleuteling Facebook'

Hoi 10.2.e

Ik was dinsdag en woensdag afwezig. Heb je Annemieke kunnen spreken?

Groet,

10.2.e

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 29 oktober 2019 13:36
**Aan:** Dam, A. van - BD/DRC
**CC:** 10.2.e - BD/DJOA/JBOZ; 10.2.e - BD/DJOA/JBOZ; 10.2.e - BD/DBAenV/IenK
**Onderwerp:** KV 'Minister bezorgd om versleuteling Facebook'

Hallo Annemieke,

Je hebt aangegeven dat je over deze KV graag even wilt overleggen. Volgens het secretariaat lukt dat niet meer voor je verlof.

Zijn je vragen van dien aard dat ik ze per mail kan beantwoorden of zal ik even een momentje plannen voor na je verlof.

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

.....
**Ministerie van Veiligheid en Justitie**
**Directie Rechtshandhaving en Criminaliteitsbestrijding**
**Cybercrime unit**
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**

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** maandag 4 november 2019 09:53
**Aan:** 10.2.e - BD/DGRR/STAF; 10.2.e BD/DRC/CV; Dam, A. van - BD/DRC; Balleqooij, mr. dr. G.A.C.M. van - BD/DJOA
**CC:** 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e 10.2.e - BD/DRC/CV; 10.2.e - BD/DBAenV/IenK
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo Gerard, hierbij een appreciatie ism met 10.2.e

Appreciatie:

11.1

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e BD/DGRR/STAF 10.2.e @minjenv.nl>
**Datum:** maandag 04 nov. 2019 8:38 AM
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DGRR/STAF 10.2.e @minjenv.nl>, Dam, A. van - BD/DRC 10.2.e @minjenv.nl>, Ballegooij, mr. dr. G.A.C.M. van - BD/DJOA 10.2.e @minjenv.nl>
**Kopie:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Gisteren in nieuwsuur nietwaar? Gerard van ballegooij zit in de ministerstaf straks. Wil je hem rechtstreeks informeren? Dank!

---

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** zondag 03 nov. 2019 6:28 PM
**Aan:** 10.2.e - BD/DGRR/STAF 10.2.e @minjenv.nl>, Dam, A. van - BD/DRC 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo 10.2.e

Tbv degene die maandag bij de ministerstaf zit voor dgRR:

Minister Grapperhaus wil toegang tot chat- en berichtendiensten
https://nos.nl/l/2308847

Er kan worden vastgesteld dat in het bericht zowel door de politiek (Verhoeven, D66) als enkele 'cyber specialisten' kritisch op het wetsvoorstel tot een ontsleutelrecht wordt gereageerd. 11.1

Ambtelijke achtergrond: de voorbereiding voor dit interview is toentertijd gedeeld met de NCTV.

Het item moet nog op nieuwsuur worden getoond, zo nodig volgt er een aanvulling van deze mail

Groet,

10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** maandag 28 okt. 2019 6:57 PM
**Aan:** 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo 10.2.e
Zoals gezegd heeft de minister morgen een interview met Nieuwsuur, hierbij onze input. Wanneer je echt prangende punten naar voren wilt brengen kun je het ZSM laten weten? De minister staat Nieuwsuur te woord in de schorsing van de APB in de EK.
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 18:54
**Aan:** 10.2.e BD/DCOM/P&B ; 10.2.e BD/DBAenV/IenK
**CC:** 10.2.e mr. C. - BD/DRC/CV ; 10.2.e - BD/DBO ; 10.2.e - BD/DCOM/P&B ; Dam, A. van - BD/DRC
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
Hallo 10.2.e
Hierbij de input van Nieuwsuur die 10.2.e en ik hebben opgesteld.
Groeten,
10.2.e

**Van:** 10.2.e - BD/DCOM/P&B 10.2.e @minjenv.nl>
**Verzonden:** maandag 28 oktober 2019 16:59
**Aan:** 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DBO 10.2.e @minjenv.nl>; 10.2.e - BD/DCOM/P&B 10.2.e @minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hi all,

Ik heb nog even gebeld met Nieuwsuur. Zie hieronder.

Heb de punten van de vorige keer ook weer gebruikt. Graag nog evt jullie aanvulling/11.1 Dan bundel ik alles en stuur het naar de minister. Afhankelijk van tijdstip schorsing, wordt het dus tussen 12-14 opgenomen morgen.

Nog niet bekend wanneer de uitzending is.

10.2.e

**Insteek uitzending**

- uitleg wat E2E is
- Wat Barr e.a. willen
- Gesprek met Verhoeven nav de Kamervragen
- Gesprek met Grapperhaus
- 11.1

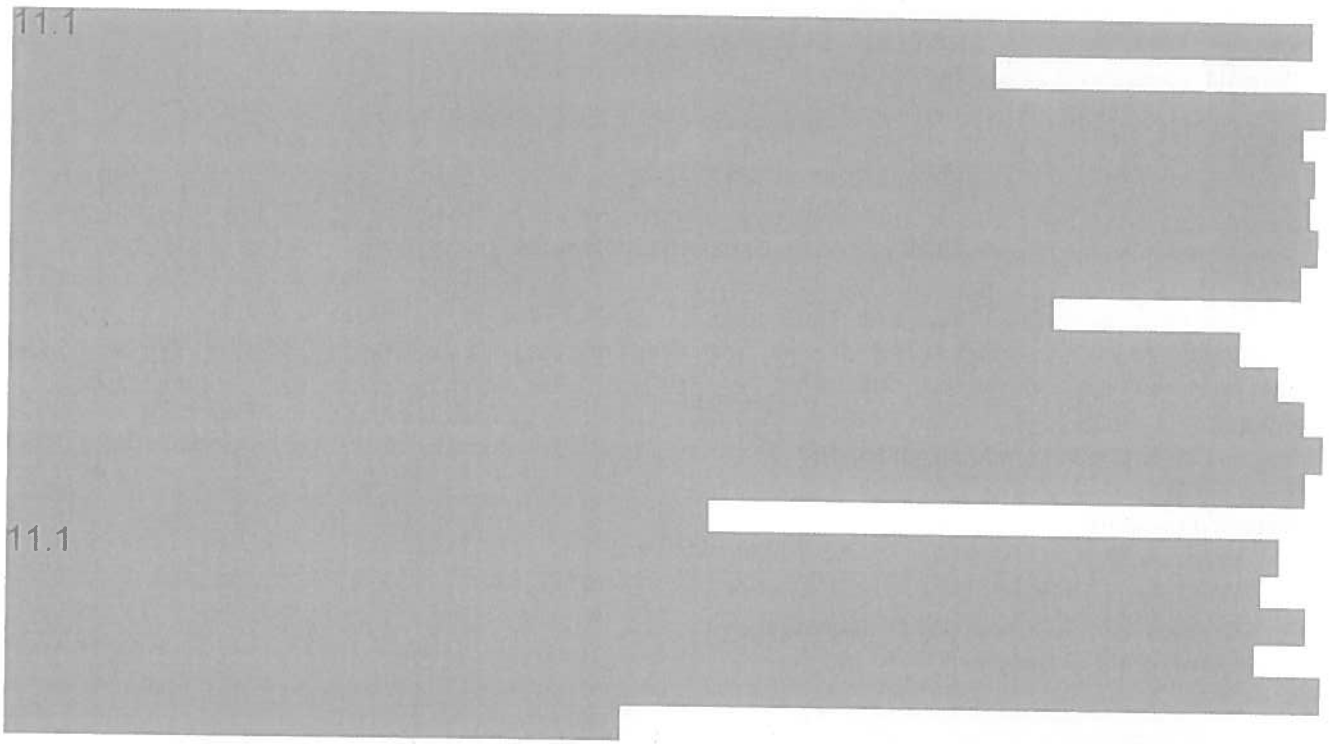
**Vragen aan Ferd:**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?
  - o 11.1
- Is dit een nieuw probleem of al bekend?
  - o 11.1
- Wat zijn deze zorgen precies?
- Waarom precies kinderporno?
  - o 11.1
- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?
  - 11.1

**Openbrief – platte tekst**

11.1

11.1



11.1

10.2.e **BD/DRC/CV**

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** 10.2.e - BD/DGRR; 10.2.e - BD/KS; 10.2.e 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DWJZ/SSR; 10.2.e mr. S.W. - BD/DWJZ/JZW
**CC:** 10.2.e BD/DRC/CV; 10.2.e - BD/DBAenV/IenK
**Onderwerp:** Gespreksnota encryptie
**Bijlagen:** Gespreksnota.docx

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om 11.1

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst 11.1 Uiteraard houd ik jullie hoe dan ook aangesloten.
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?
Groet,
10.2.e

**10.2.e - BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 5 november 2019 16:29
**Aan:** 10.2.e - BD/KS; 10.2.e - BD/DGRR; 10.2.e 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DWJZ/JZW
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Ha 10.2.e

Kun je iets meer duiding geven bij de toevoeging die je in gedachten hebt? Ik wil deze nota toespitsen op de uitwerking en contouren van een ontsleutelplicht, het is een startschot tot het aangaan van een inventarisatie hoe we vorm kunnen geven aan een ontsleutelplicht. De minister wil geen structurele verzwakking van encryptie. In de diverse voorbereidingen, spreeklijnen en nota's hebben we hem nadrukkelijk geïnformeerd over waarvoor encryptie noodzakelijk is. Dit wordt nu ook in deze nota benoemd. Toch?

Ik kan een leidinggevende van je opnemen in de lijn in DJ.

Groet,

10.2.e

**Van:** 10.2.e - BD/KS
**Verzonden:** dinsdag 5 november 2019 16:16
**Aan:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DGRR ; 10.2.e BD/DWJZ/SSR 10.2.e - BD/DWJZ/SSR ; 10.2.e - BD/DWJZ/JZW
**CC:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Hoi 10.2.e ja we willen de minister 11.1
en ik moet eea ook met mijn lijn afstemmen. Dit lukt me niet voor morgenochtend.
Gr 10.2.e

10.2.e
NCTV
+316 10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 3:31 PM
**Aan:** 10.2.e - BD/DGRR 10.2.e @minjenv.nl>, 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>, 10.2.e - BD/DWJZ/SSR 10.2.e @minjenv.nl>, 10.2.e BD/DWJZ/SSR 10.2.e @minjenv.nl>, 10.2.e - BD/DWJZ/JZW 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e minjenv.nl>, 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,

Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.

De minister wordt geadviseerd om 11.1 [redacted]

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst 11.1 [redacted] Uiteraard houd ik jullie hoe dan ook aangesloten.

Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?

Groet,

10.2 e

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DRC/CV
**Verzonden:** woensdag 6 november 2019 12:19
**Aan:** 10.2.e - BD/KS; 10.2.e - BD/DWJZ/SSR; 10.2.e BD/DGRR; 10.2.e - BD/DWJZ/SSR; 10.2.e DWJZ/JZW
**CC:** 10.2.e BD/DRC/CV; 10.2.e BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie
**Bijlagen:** Gespreksnota.docx

Hallo 10.2.e

Dankjewel. Ik heb de nota aangepast. 11.1

Wat ik niet heb overgenomen is 11.1 De nota leidt tot een gesprek en als er zodanige problemen zijn met deze term kunnen deze daar naar voren worden gebracht.

Is het nodig dat we even bellen?

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e - BD/KS
**Verzonden:** woensdag 6 november 2019 10:15
**Aan:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DWJZ/SSR ; 10.2.e BD/DGRR ; 10.2.e 10.2.e - BD/DWJZ/SSR ; 10.2.e - BD/DWJZ/JZW
**CC:** 10.2.e BD/DRC/CV ; 10.2.e BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Hoi 10.2.e en collega's,

Bijgaand onze aanpassingen op de nota. De uitspraken van de minister zijn gisteren uitgebreid besproken bij ons intern en daaruit kwamen een paar noties die we van belang vinden om in deze fase aan minister mee te geven 11.1 Wat mij betreft een logisch moment, aangezien de eerdere besprekingen met de minister gericht waren op inventarisatie van oplossingen, en niet op een ontsleutelplicht (alleen). Wat ons betreft is het dan ook van belang om 11.1

Ook vinden we als concipient destijds van het kabinetsstandpunt dat 11.1 NCSC heeft al kenbaar gemaakt dat ze bereid zijn om ook aan te schuiven. Maar 11.1 .

Ik kan me verder ook aansluiten bij 10.2.e opmerkingen, dus ook wat dat betreft, is het 11.1

Graag ontvang ik een definitieve versie om ook met mijn MT verder af te stemmen.

Gr. 10.2.e

10.2.e
NCTV
10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 5:42 PM
**Aan:** 10.2.e - BD/DWJZ/SSR 10.2.e @minjenv.nl>, 10.2.e - BD/DGRR 10.2.e @minjenv.nl>, 10.2.e BD/KS 10.2.e @nctv.minjenv.nl>, 10.2.e 10.2.e BD/DWJZ/SSR 10.2.e @minjenv.nl>, 10.2.e - BD/DWJZ/JZW 10.2.e @minjenv.nl>
**Kopie:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e /DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Hallo 10.2.e

Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies. Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat 11.1

We houden je op de hoogte!

Groet,

10.2.e

**Van:** 10.2.e BD/DWJZ/SSR 10.2.e minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DGRR 10.2.e @minjenv.nl>; 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DWJZ/SSR 10.2.e @minjenv.nl>; 10.2.e - BD/DWJZ/JZW 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Ha 10.2.e

Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. 11.1
- Verder moet je je afvragen of 11.1
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare

telecommunicatienetwerken en -diensten). 11.1

Groet,

10.2.e

---

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** 10.2.e - BD/DGRR <10.2.e @minjenv.nl>; 10.2.e LLM, N.W.F. - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DWJZ/SSR 10.2.e - 10.2.e @minjenv.nl>; 10.2.e BD/DWJZ/SSR 10.2.e @minjenv.nl>; 10.2.e . - BD/DWJZ/JZW 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,

Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.

De minister wordt geadviseerd om 11.1

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst 11.1 Uiteraard houd ik jullie hoe dan ook aangesloten.

Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?

Groet,

10.2.e

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 14:21
**Aan:** 10.2.e - BD/PNDV
**CC:** 10.2.e - BD/KS
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

Ha 10.2.e

Ja kan nog worden toegevoegd.

**Van:** 10.2.e - BD/PNDV
**Verzonden:** donderdag 7 november 2019 10:04
**Aan:** 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/KS
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

Hallo 10.2.e

10.2.e stuurde onderstaande emailwisseling ter info door. Ik weet niet of het nog mogelijk is, maar vanuit ons toch nog een suggestie om ook nog een bullet te wijden aan 11.1

Dit laatste is immers ook onderdeel van zijn portefeuille. Als hij het niet benoemd wordt hij er misschien op gewezen door andere aanwezigen, wat me wat ongemakkelijk lijkt.

Terzijde: weet jij of minister Dekker al ergens hierover op de lijn is gekomen hierover? Vanuit het oogpunt privacybescherming, komt hij ook vrij snel in aanraking met encryptie.

Groet,
10.2.e

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** woensdag 06 nov. 2019 5:49 PM
**Aan:** 10.2.e - BD/KS <10.2.e @nctv.minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

Ha 10.2.e

Prima, in beginsel streven om binnen de kaders te blijven. Anders overleg.

**Van:** 10.2.e BD/KS 10.2.e @nctv.minjenv.nl>
**Verzonden:** woensdag 6 november 2019 17:47
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>; 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

10.2.e

Ik durf niet te stellen dat 11.1 . de zorgen zelf misschien wel, maar het was niet voor niks dat in 2016 ook niet tot wettelijke beperkende maatregelen kon worden gekomen tav het gebruik van encryptie. Dus het lijkt me 11.1 Bovendien zullen we andere dept wel degelijk ook bij de oplossing moeten gaan betrekken. Mijn voorstel heb ik hieronder Aangepast.

Gr 10.2.e

10.2.e
NCTV
10.2.e

---

**Van:** 10.2.e en@minjenv.nl>
**Datum:** woensdag 06 nov. 2019 5:40 PM
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>, 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** Encryptie OTT mogelijk tbv MR

Hallo allen,

10.2.e heeft gevraagd om een spreeklijn voor onze minister in het geval het onderwerp opkomt in de MR.

Effectieve toegang tot versleutelde gegevens.

- 11.1

11.1

11.1

11.1 [redacted]

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 14:19
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DWJZ/SSR; 10.2.e - BD/DRC/CV; 10.2.e - BD/DBAenV/IenK
**CC:** 10.2.e - BD/DEIA/EU; 10.2.e BD/DEIA/EU; 10.2.e minbuza.nl
**Onderwerp:** bilateraal overleg MJenV met 10.2.a en [redacted] bij aankomende JBZ van

Hallo collega's,

Op twee dossiers worden we (weer) actief in het Brusselse: Buiten reikwijdte en interceptie OTT (decryptie).

Is het een goed idee om en marge van de aankomende JBZ (9 december). Bilateralen te plannen met 10.2.a en [redacted] (of een ontbijt met z'n vieren oid).

Inzet zou kunnen zijn:

Buiten reikwijdte [redacted]

<u>Interceptie OTT</u>
11.1 [redacted]

Groeten,

10.2.e

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 14:58
**Aan:** Dam, A. van - BD/DRC
**CC:** 10.2.e - BD/DRC/CV 10.2.e - BD/DRC/CV; 10.2.e 10.2.e BD/DBAenV/IenK; 10.2.e - BD/PNDV
**Onderwerp:** FW: Encryptie OTT mogelijk tbv MR

Hallo Annemieke,

10.2.e van DBO kwam op de lijn voor een spreeklijn tbv de Ministerraad. Mogelijk kan de minister daar tijden de raad of en marge op worden aangesproken. Onderstaande lijn is afgestemd met de NCTV.

- 11.1

11.1

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 19:37
**Aan:** 10.2.e BD/DBO/ADVIES; 10.2.e BD/DRC/CV
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

Sorry, moest onverwacht naar directeur.

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e - BD/DBO/ADVIES 10.2.e@minjenv.nl>
**Datum:** donderdag 07 nov. 2019 6:22 PM
**Aan:** 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>
**Onderwerp:** RE: Encryptie OTT mogelijk tbv MR

Vind, het is helaas te laat. Stukken zijn al de deur uit. ☹

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 18:03
**Aan:** 10.2.e BD/DBO/ADVIES
**Onderwerp:** FW: Encryptie OTT mogelijk tbv MR
Ha 10.2.e
Ik zou je nog een spreeklijntje sturen.
Hierbij:
NB de ministers met de AIVD en MIVD in hun portefeuille hebben voor deze verantwoordelijkheid een gedeeld belang als de opsporing.

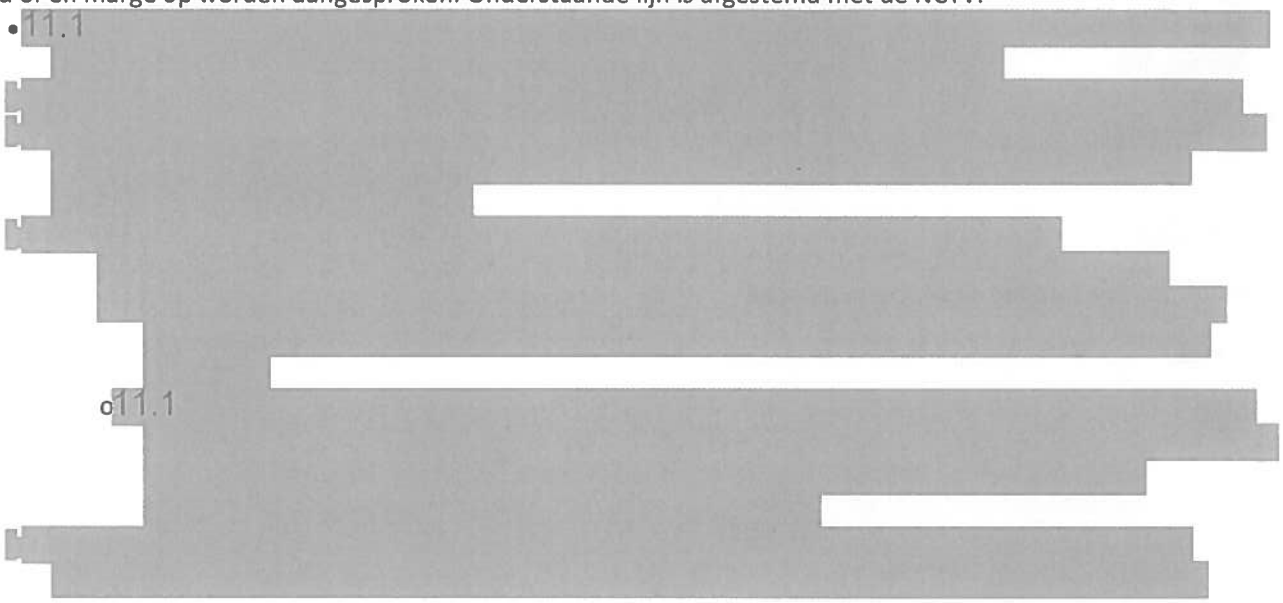
- 11.1
  - 11.1

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** donderdag 7 november 2019 14:58
**Aan:** Dam, A. van - BD/DRC 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/PNDV 10.2.e @nctv.minjenv.nl>
**Onderwerp:** FW: Encryptie OTT mogelijk tbv MR

Hallo Annemieke,

10.2.e van DBO kwam op de lijn voor een spreeklijn tbv de Ministerraad. Mogelijk kan de minister daar tijden de raad of en marge op worden aangesproken. Onderstaande lijn is afgestemd met de NCTV.

- 11.1
  - 11.1



10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** maandag 11 november 2019 12:02
**Aan:** 10.2.e - BD/KS
**Onderwerp:** RE: Facebook encryption

Ha 10.2.e

Dank je. We hebben inmiddels contact!

Groet,

10.2.e

**Van:** 10.2.e - BD/KS
**Verzonden:** maandag 11 november 2019 11:37
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** FW: Facebook encryption

10.2.e mag ik deze dame (10.2.a in Den Haag) aan jou koppelen?
Gr 10.2.e

**Van:** 10.2.a en 10.2.e
**Datum:** vrijdag 01 nov. 2019 2:53 PM
**Aan:** 10.2.e - BD/KS <10.2.e @nctv.minjenv.nl>, 10.2.e - BD/PSD 10.2.e @nctv.minjenv.nl>
**Kopie:** 10.2.a en 10.2.e
**Onderwerp:** Facebook encryption

10.2.e

10.2.a

,

10.2.a en 10.2.e

10.2.a

10.2.e /DRC/CV

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** dinsdag 12 november 2019 09:15
**Aan:** 10.2.e - BD/DBAenV/IenK
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e 10.2.e - BD/KS
**Onderwerp:** RE: Kamerbrief KP

Ha 10.2.e

Ik vind het over het geheel een 11.1 Zo'n beknopt overzicht van de stavaza van een beleidsonderwerp is wat mij betreft 11.1 . Tekent de MJenV niet met Ferdi pv F.B.J (en er moet wat tekst op de pagina van de ondertekening staan ;))

De passage over encryptie is idd grotendeels uit de beantwoording van de KV, ik heb alleen twee opmerkingen.
11.1

**Encryptie**
11.1

**Van:** 10.2.e - BD/DBAenV/IenK
**Verzonden:** donderdag 7 november 2019 17:35
**Aan:** 10.2.e BD/DRC/CV
**Onderwerp:** Kamerbrief KP

Ha 10.2.e
Nav onderstaande mail, heb ik bijgaande brief opgesteld. Het is nog een ruwe eerste versie, maar zou jij op de alinea over encryptie commentaar willen geven? Aanvullingen het liefst met tekstsuggesties.
Dank en groet, 10.2.e

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** woensdag 13 november 2019 08:13
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e (PaG Den Haag)'; 10.2.e (Landelijk Parket)
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: OTT aftappen

Dankjewel 10.2.e

Zeker nuttig. Gaan de 10.2.a iets vertellen over de 10.2.a wet, 10.2.a

10.2.a en 10.2.a dus bezig regulerend kader te scheppen, maar hebben geen antwoord op encryptie? Heb je de contact details van deze personen? Mijn initiële contact met hen was goed, maar toen ik vroeg wat hun ideeën waren bij decryptie werd het stil over de mail. 10.2.e en ik gaan binnenkort naar Brussel om face to face met wat lidstaten te praten. 10.2.a en 10.2.a zijn dan goede partners.

10.2.a10.2.a

Succes daar!

10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e riks@politie.nl>
**Datum:** woensdag 13 nov. 2019 12:03 AM
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e (PaG Den Haag)' 10.2.e @om.nl>, 10.2.e @om.nl>, 10.2.e om.nl>
**Kopie:** 10.2.e minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: OTT aftappen

De 10.2.a zijn van mening dat 10.2.a De OTT's vinden dat 10.2.a en 10.2.a Ze vragen wel aandacht voor 10.2.a Verder is hun Homerouting standpunt gebaseerd op geldende wetgeving die als volgt wordt uitgelegd. 10.2.a

Verder werd er uitgebreid gesproken over de cloudact waar de 10.2.a en de 10.2.a inmiddels overeenstemming over hebben. Deze wet houdt in dat de 10.2.a direct kan gaan tappen/gegevens bevragen in de 10.2.a en vv. De Europese Cie is blijkbaar met de 10.2.a hierover aan het praten in relaties tot e-evidence.

10.2.a

10.2.a volgt maar wat ik tot nog toe heb begrepen is dat 10.2.a

Groet 10.2.e

---

**Van:** 10.2.e
**Datum:** 12 november 2019 om 11:16:45 GMT+13
**Aan:** 10.2.e - BD/DRC/CV , 10.2.e (PaG Den Haag)' , 10.2.e , 10.2.e (Landelijk Parket)
**CC:** 10.2.e - BD/DRC/CV , 10.2.e - BD/DRC/CV
**Onderwerp:** RE: OTT aftappen

10.2.a

Groet 10.2.e

---

**Van:** 10.2.e - BD/DRC/CV
**Datum:** 9 november 2019 om 03:49:03 GMT+13
**Aan:** 10.2.e (PaG Den Haag)' , 10.2.e (Landelijk Parket) , 10.2.e
**CC:** 10.2.e - BD/DRC/CV , 10.2.e BD/DRC/CV
**Onderwerp:** RE: OTT aftappen

Ha 10.2.e
Dank je! Ik wil de 11.1 Ik begrijp en deel dus de zorgen die je hebt, ik ben alleen op zoek naar 11.1 Zo te lezen is het beter om even in een gesprek de standpunten en doelen te overleggen.
Ik probeer voor volgende week een moment te plannen, inclusief politie.
Over dat traditionele telefoniediensten ook onder 'interpersoonlijke communciatie dienst horen, is dit het onderscheid tussen de in de in de definitie van elektronische communicatiedienst gehanteerde 'geheel of hoofdzakelijk bestaat in het overbrengen van signalen' en het openbaar telecommunicatienetwerk gebruikte 'geheel of gedeeltelijk'. Of ligt dit in het onderscheid tussen telecomunicatienetwerk en – dienst.
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e (PaG Den Haag)
**Verzonden:** vrijdag 8 november 2019 10:53
**Aan:** 10.2.e BD/DRC/CV ; 10.2.e (Landelijk Parket Rotterdam) ; 10.2.e (Landelijk Parket) 10.2.e @politie.nl
**CC:** 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: OTT aftappen

Dag 10.2.e en overige collega's,

Volgens mij is het standpunt van OM en politie dat 11.1 Dat vraagstuk moeten we m.i. 11.1 @10.2.e jouw alternatieve voorstel 11.1 De 'interpersoonlijke communicatiedienst' omvat namelijk zowel klassieke telefoniediensten als OTT-diensten. Je zou dus een ander voorbehoud moeten maken dat enkel op OTT-diensten ziet. Daarin schuilt een kans om de gehanteerde terminologie in H13 gelijk te trekken met de rest van de Tw.

Groeten,

10.2.e
Senior Adviseur
Openbaar Ministerie
Parket-Generaal, Afdeling Beleid & Strategie
Cluster georganiseerde en ondermijnende criminaliteit, opsporing en politie
10.2.e
10.2.e @om.nl
www.om.nl

**Van:** 10.2.e - BD/DRC/CV [mailto:10.2.e @minjenv.nl]
**Verzonden:** donderdag 7 november 2019 17:42
**Aan:** 10.2.e (Landelijk Parket Rotterdam); 10.2.e (PaG Den Haag); 10.2.e (Landelijk Parket); 10.2.e @politie.nl
**CC:** 10.2.e - BD/DRC/CV; 10.2.e DRC/CV
**Onderwerp:** OTT aftappen

Hallo allemaal,

11.1

Moeten we even bellen met z'n allen over nut en noodzaak? Er gaat nu veel gebeuren op decryptie nav Nieuwsuur.

11.1

11.1 [redacted]

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

---



---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

---------- Disclaimer ----------
De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen.
Kennisneming door anderen is niet toegestaan.
De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen.
Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen.
---

**/o=Exchange/ou=DBOB/cn=Recipients/cn**10.2.e

**Van:** 10.2.a en 10.2.e
**Verzonden:** woensdag 18 december 2019 09:05
**Aan:** 10.2.e BD/DRC/CV; 10.2.a en 10.2.e
**CC:** 10.2.e ; WAS-JenV; 10.2.e - BD/DEIA/IBP; 10.2.e BD/DEIA/IBP; 10.2.e BD/DEIA/IBP; 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e @minbuza 10.2.e BD/DEIA/EU
**Onderwerp:** 10.2.a
**Bijlagen:** 2019.08.26-Lawful_Access_Trifold_SHARE_Version.pdf; 2019.09.11-LA_Booklet-AG.FBI.DIR-ICCS_Fordham.pdf

10.2.e

10.2.a

10.2.a

10.2.a en 10.2.e

---

**From:** 10.2.a en 10.2.e
**Sent:** Monday, December 16, 2019 4:04:35 PM
**To:** 10.2.e - BD/DRC/CV
**Cc:** 10.2.e ; WAS-JenV ; 10.2.e BD/DEIA/IBP ; 10.2.e - BD/DEIA/IBP ; 10.2.e , 10.2.e - BD/DEIA/IBP ; 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e @minbuza.nl ; 10.2.e - BD/DEIA/EU

**Subject:** 10.2.a [redacted]

10.2.a en 10.2.e [redacted]

---

**From:** 10.2.e - BD/DRC/CV
**Sent:** Monday, December 16, 2019 3:08 PM
**To:** 10.2.a en 10.2.e
**Cc:** 10.2.e ; WAS-JenV ; 10.2.e - BD/DEIA/IBP ; 10.2.e BD/DEIA/IBP ; 10.2.e , 10.2.e - BD/DEIA/IBP ; 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e @minbuza.nl ; 10.2.e - BD/DEIA/EU
**Subject:** 10.2.a [redacted]

Dear 10.2.a en 10.2.e ,

10.2.e and I just discussed the email below. We would be very interested to discuss your views on end-to-end encryption and lawful access, especially the different policy and technical options. I am available tomorrow morning or in the afternoon after 4 pm. Later in the week is also possible.

Kind regards,

10.2.e
Ministry of Justice and Security
Law Enforcement Directorate
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
M 10.2.e
10.2.e @minjenv.nl

**Van:** 10.2.e - BD/DEIA/IBP
**Verzonden:** maandag 16 december 2019 14:20
**Aan:** 10.2.a en 10.2.e ; 10.2.e @minbuza.nl; 10.2.e - BD/DEIA/EU ; 10.2.e - BD/DRC/CV ; 10.2.e BD/DRC/CV ; 10.2.e - BD/DRC/CV ; 10.2.e - BD/DRC/CV
**CC:** 10.2.e ; WAS-JenV ; 10.2.e - BD/DEIA/IBP ; 10.2.e - BD/DEIA/IBP
**Onderwerp:** 10.2.a [redacted] .

Dear 10.2.a en 10.2.e ,

Many thanks for your message.

10.2.e and I have indeed discussed the possible follow up.

I have also discussed the same issue last Friday-afternoon, directly after our telephone call with my deputy director, 10.2.e .

10.2.e – who was also present during the meeting of Minister Grapperhaus with 10.2.a - is in charge of the EU-coordination Department of this Ministry.

He will come back on the possible scenarios for having a discussion – with the possible involvement of the FBI – at the EU-level on the negative aspects for law enforcement of the end-to-end encryption by Facebook Messenger.
After 10.2.e feedback, we will have a better idea how to proceed.
The expert within this Ministry on that subject (Mr 10.2.e ) is on leave until January 7, 2020.
Therefore, I have copied in his direct colleagues, 10.2.e as well as 10.2.e and 10.2.e to this message; 10.2.e : are you / is one of you available for a discussion with 10.2.a en 10.2.e (The Hague) – "today or tomorrow" - on this subject and the help which the FBI could provide in this area? ("other initiatives to best support your efforts ")
10.2.a

Kind regards,
10.2.e
10.2.e
Coordinator International Relations: US, Canada, Western Balkan's, Turkey and EU-accession.
M.:+3 10.2.e

**Van:** 10.2.a en 10.2.e
**Verzonden:** maandag 16 december 2019 13:18
**Aan:** 10.2.e @minbuza.nl
**CC:** 10.2.e @politie.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; WAS-JenV 10.2.e @minbuza.nl>
**Onderwerp:** 10.2.a

10.2.a en 10.2.e

---

**From:** 10.2.e minbuza.nl>
**Sent:** Saturday, December 14, 2019 12:33 PM
**To:** 10.2.a en 10.2.e
**Cc:** 10.2.e @politie.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; WAS-JenV 10.2.e @minbuza.nl>
**Subject:** 10.2.a
Hi
Thanks for reaching out. 10.2.a

10.2.a . I know that 10.2.e and 10.2.e are in touch with you, trying to work out a time slot for the Minister and 10.2.a to meet again in The Netherlands. I hope this works out.
I'm actually in The Netherlands right now. On Monday morning, I have a meeting with 10.2.e en several other policy advisors from my ministry. I will discuss this matter, and give you a call afterwards.
Looking forward to talking to you again.
Enjoy your weekend!

10.2.e
10.2.e
Counselor for Justice and Security
Embassy of the Kingdom of The Netherlands
4200 Linnean Avenue N.W.
20008 Washington D.C.
Mob: 10.2.e
10.2.e
NLintheUSA.com

**From:** 10.2.a en 10.2.e
**Sent:** vrijdag 13 december 2019 02:53
**To:** 10.2.e @minbuza.nl>
**Cc:** 10.2.e @politie.nl>
**Subject:** 10.2.a
10.2.a

10.2.a en 10.2.e

---

**From:** 10.2.a en 10.2.e
**Sent:** Tuesday, December 10, 2019 11:03 AM
**To:** 10.2.e @minjenv.nl>
**Cc:** Secretariaat - Minister van Justitie en Veiligheid 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; 10.2.a en 10.2.e 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>; 10.2.e @politie.nl>
**Subject:** 10.2.a

10.2.a

10.2.a en
10.2.e

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

---

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic

transmission of messages.

Ministry of Justice and Security

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DCOM/P&B
**Verzonden:** donderdag 5 december 2019 05:06
**Aan:** 10.2.e BD/DRC/CV
**CC:** 10.2.e BD/DRC/CV; 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Fwd: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that

Vanmiddag bij Barr geweest. Uitgebreider verslag volgt via DEIA denk ik. 11.1

10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Datum:** woensdag 04 dec. 2019 2:20 PM
**Aan:** 10.2.e - BD/DCOM/P&B <10.2.e @minjenv.nl>
**Kopie:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: Fwd: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that

Ja zag het, dank je. Hoe gaat het daar? Al bij Barr geweest?

"Using encryption to exchange child pornography should simply be made impossible,"

11.1

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e - BD/DCOM/P&B 10.2.e @minjenv.nl>
**Datum:** woensdag 04 dec. 2019 6:44 PM
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** FW: Fwd: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that

Verhoeven heeft weer kamervragen gesteld

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e BD/DCOM/P&B <10.2.e @minjenv.nl>
**Datum:** woensdag 04 dec. 2019 12:31 PM
**Aan:** 10.2.e @minjenv.nl>, 10.2.e - BD/DBO
10.2.e @minjenv.nl>, Zorko MPA, P.M. - BD/NCTV 10.2.e @nctv.minjenv.nl>
**Onderwerp:** FW: Fwd: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that

**CYBER DIPLOMACY**

**DUTCH TRIP TO WASHINGTON:** The Netherlands' Justice and Security Minister Ferdinand ("Ferd") Grapperhaus landed in Washington for half a week of discussionswith his American counterparts including U.S. Attorney General William Barr. The Dutch minister wants to strengthen ties on cybersecurity, he told Cyber Insights over the phone while schlepping to the U.S.

"The Netherlands is a small country, but we approached [Dutch security services] early on to work on cybersecurity," he said. The Dutch government already reaped the benefit, conducting pioneering operations that brought down dark web market places like Hansa. (According to the Volkskrant paper the Dutch government also assisted U.S. intelligence services in their investigations into Russian hacking groups, and the Dutch together with the U.K. security services stopped a Russian hacking attempt on an international organization.)

**Friends:** "We cooperate very well in exchanging information, and in exchanging methods to counter threats on the dark web," Grapperhaus said. "Now, we're looking at how to take this to the next level." He said the U.S. can help foster support to beef up cybersecurity systems in other parts of Europe, too.

**Foes:** The Dutch government in its latest annual threat report flagged state actors as the main threat and called out China, Iran and Russia for having "offensive cyber programs" that targeted the country. Grapperhaus said "it's becoming more clear to the wider public, to the media, that these threats exist" and that "the offensive behavior of other countries is becoming clearer."

**On encryption:** The minister launched a call on his fellow European ministers and the EU Commission to come up with legislation that would outlaw encrypting child pornography — or something to that extent. "Using encryption to exchange child pornography should simply be made impossible," he said.

He added platforms have shown willingness to tackle to growing problem of child exploitation material online, but that legal requirements lack and encryption should be part of a legislative solution. We have that story here.

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** 10.2.e @politico.eu>
**Datum:** woensdag 04 dec. 2019 12:28 PM
**Aan:** 10.2.e @minjenv.nl>
**Onderwerp:** Fwd: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that

Hier een stuk (nieuwsbrief vandaag)

10.2.e
Reporter, POLITICO Europe
10.2.e
10.2.e@politico.eu
Twitter: @10.2.e

Private email:
10.2.e

— Sent from my iPhone

Begin doorgestuurd bericht:

**Van:** POLITICO Cyber Insights <cyberinsights@politico.eu>
**Datum:** 4 december 2019 om 15:46:10 CET
**Aan:** POLITICO Europe Subscribers 10.2.e @politico.eu>
**Onderwerp: POLITICO Pro Cyber Insights: 5G face-off — Dutch-American connection — Pseudonymize that**
**Antwoord aan:** POLITICO Cyber Insights <cyberinsights@politico.eu>

POLITICO Cyber Insights

By Laurens Cerulus | @laurenscerulus | lcerulus@politico.eu | Contact us on Signal, WhatsApp | View in your browser

*With thanks to Matthew Brown, David Herszenhorn, Tim Starks and Nicholas Vinocur.*

**TODAY'S TOP LINE — NATO NOISES:** Leaders at the NATO summit talk 5G security and launch a cybersecurity exercise. That and more below.

**WELCOME to Cyber Insights,** POLITICO's cybersecurity and data protection newsletter, giving you the daily lowdown on hacks, leaks and cyber policy chatter in Europe.

**5G SECURITY**

**NATO LEADERS AGREE ON 'SECURE AND RESILIENT' 5G:** Leaders at the NATO summit in London discussed telecom security today, the defense alliance's Secretary General Jens Stoltenberg told reporters, and "agreed to rely only on secure and resilient systems."

Meanwhile, Japan joined NATO's cybersecurity exercise called the Cyber Coalition exercise, which lasts until Friday and challenges government officials to respond to scenarios like massive cyberattacks with technical, political and diplomatic tools. Nikkei Asian Review has more.

**US PUTS MONEY WHERE MOUTH IS:** Bloomberg reported the U.S. is planning to open up a $60 billion budget in an agency called the International Development Finance Corporation to support foreign governments or even take minority states in companies that decide to procure 5G equipment from competitors of Huawei and ZTE — notably the Swedish Ericsson and Finnish Nokia.

"The U.S. could bankroll Huawei alternatives through loans or loan guarantees to developing nations and companies, or even acquiring minority stakes in emerging makers of competing gear," Bloomberg wrote.

"Ericsson shares jumped as much as 4.2 percent, while Nokia gained as much as 3.2 percent following the story."

**CHINESE REBUTTAL:** China's representative to the European Union today rebutted U.S. warnings that Chinese telecom equipment makers should be kept out of European 5G networks.

Recent warnings by U.S. State Secretary Mike Pompeo "are a far cry from the truth," Zhang Ming, the head of the Chinese Mission to the EU, wrote in a letter to the editor published on POLITICO today. "Despite the witch hunt and media hype, not a single country or individual has come up with solid evidence to prove that Huawei poses a security threat," he said.

## CYBER DIPLOMACY

**DUTCH TRIP TO WASHINGTON:** The Netherlands' Justice and Security Minister Ferdinand ("Ferd") Grapperhaus landed in Washington for half a week of discussions with his American counterparts including U.S. Attorney General William Barr. The Dutch minister wants to strengthen ties on cybersecurity, he told Cyber Insights over the phone while schlepping to the U.S.

"The Netherlands is a small country, but we approached [Dutch security services] early on to work on cybersecurity," he said. The Dutch government already reaped the benefit, conducting pioneering operations that brought down dark web market places like Hansa. (According to the Volkskrant paper the Dutch government also assisted U.S. intelligence services in their investigations into Russian hacking groups, and the Dutch together with the U.K. security services stopped a Russian hacking attempt on an international organization.)

**Friends:** "We cooperate very well in exchanging information, and in exchanging methods to counter threats on the dark web," Grapperhaus said. "Now, we're looking at how to take this to the next level." He said the U.S. can help foster support to beef up cybersecurity systems in other parts of Europe, too.

**Foes:** The Dutch government in its latest annual threat report flagged state actors as the main threat and called out China, Iran and Russia for having "offensive cyber programs" that targeted the country. Grapperhaus said "it's becoming more clear to the wider public, to the media, that these threats exist" and that "the offensive behavior of other countries is becoming clearer."

**On encryption:** The minister launched a call on his fellow European ministers and the EU Commission to come up with legislation that would outlaw encrypting child pornography — or something to that extent. "Using encryption to exchange child pornography should simply be made impossible," he said.

He added platforms have shown willingness to tackle to growing problem of child exploitation material online, but that legal requirements lack and encryption should be part of a legislative solution. We have that story here.

## DATA PROTECTION

**PSEUDONYMIZATION = HARD.** To comply with the EU's General Data Protection Regulation law's higher standards for privacy, cyber experts and technologists are exploring techniques to protect user info. They explored one strategy, pseudonymization, in a report published on Tuesday by the EU's Agency on Cybersecurity. Though approaches vary, pseudonymization replaces a person's identifiable info with aliases. And it's harder that it seems. Essentially, the report concluded that implementation will be difficult no matter what sort of pseudonymization is adopted, presenting a lot more work for the cyber experts and technologists.

## THREAT REPORT

**STATE OF SECURITY:** Cybersecurity company Akamai today released its yearly State of the Internet/Security report. The key takeaway, really, is that it's gotten bad and is expected to get worse: "We're moving away from an era when the security advisors in a company were viewed as alarmists, to one where even we [security advisors] are sometimes caught off guard by the severity and impact of attacks," the company writes.

**FRIENDS OF SHAMOON:** Iran is likely behind new destructive malware that IBM discovered, the company's X-Force IRIS team revealed today. The wiper, dubbed ZeroCleare, "was used to execute a destructive attack that affected organizations in the energy and industrial sectors in the Middle East," IBM wrote in a blog post. The malware resembles Shamoon, the infamous destructive wiper used in the landmark Saudi Aramco attack, IBM determined.

## MOVERS & SHAKERS

**BELGIAN TELCO REGULATOR:** Mieke de Regt, digital and telecom expert at the Belgian permanent representation, is joining the national telecom regulator BIPT. She'll assist the Chairman Michel Van Bellinghen in preparing for the presidency of BEREC, the European group of telecom regulators, in 2021.

**UK CONSULTING:** Joshua Burch has joined FTI Consulting in London as a senior managing director and head of cybersecurity for the Europe, Middle East and Africa region, the organization announced Monday. He most recently worked on cyber and national security for U.K. government.

## FOOTAGE DU JOUR

Mark Zuckerberg attempts to pull off the absolutely-normal-everyday-family-man look in a CBS News interview at the kitchen table.

## ELSEWHERE ON THE WEB

— The European Data Protection Supervisor released a report providing "an overview of the activities carried out by the EDPS from 2015-2019." EDPS

— Report on "Industrial cyber attacks: a humanitarian crisis in the making." Humanitarian Law & Policy

— Huawei bolsters public-relations blitz with legal action. Wall Street Journal

— The Dutch government has landed on tougher requirements for 5G security. NOS

— Deutsche Telekom 5G deals on hold pending Huawei ban decision. Reuters

— Why I opt out of facial recognition, by Robert Hackett. Fortune

Here's a recap of today's news, along with Pro articles and alerts from overnight.

**Thierry Breton: The high-speed commissioner**
France's man in Brussels wants to move fast — at the risk of ruffling feathers.
By Laura Kayali | 12/4/19, 2:29 PM CET

**Dutch minister urges EU action to fight child pornography online**
Ferd Grapperhaus backed US calls to break encryption for investigatory purposes.
By Laurens Cerulus | 12/4/19, 11:11 AM CET

**Cristian-Silviu Buşoi confirmed to lead Parliament's industry and energy committee**
By Laura Greenhalgh, Laura Kayali | 12/4/19, 9:43 AM CET

**Google co-founders hand over reins of parent company Alphabet**
The leadership transition comes at a precarious moment for the company.
By Steven Overly | 12/4/19, 12:40 AM CET

**Report linking Labour leak to Russia reveals weakness of UK electoral system**
New analysis points out similarities between leak to Jeremy Corbyn's party and Russian disinformation operation.
By Mark Scott, Eleni Courea | 12/3/19, 8:30 PM CET

**E-privacy rapporteur warns against withdrawal of the proposal**
By Laura Kayali | 12/3/19, 5:49 PM CET

10.2.e **BD/DRC/CV**

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** maandag 2 december 2019 15:48
**Aan:** 10.2.e BD/DRC/CV
**CC:** 10.2.e BD/DRC/CV; 10.2.e @minbuza.nl
**Onderwerp:** RE: Mail EU-lidstaten en VS over encryptie

Hoi 10.2.e
Hierbij zoals besproken een paar kleine suggesties. Ik hoor graag of je akkoord gaat.
Vriendelijke groet,
10.2.e

Dear madam/sir,

The Dutch Ministry of Justice and Safety would like to invite you for a lunch meeting on 11 December 2019 at the Permanent Representation of the Netherlands to the EU (Avenue de Cortenbergh 4-10) to discuss the subject of encryption. As there is a Working Party on Cooperation in Criminal Matters that day, the exact timing will depend on the lunch break provided by the Finnish Presidency.

In 2016, the position of the Dutch cabinet on the use of encryption was published. The cabinet position elaborates on the importance of encryption for communications and the importance of access to unencrypted data for law enforcement and national security purposes.

Earlier this year, Facebook confirmed plans to use end-to-end-encryption for Facebook Messenger. On 4 October 2019, the United Kingdom Secretary of State for the Home Department of the United Kingdom, the United States Attorney General and the Secretary of Homeland Security, and the Australian Minister for Home Affairs sent an open letter to the Chief Executive Officer of Facebook in which they voiced their concerns over this announcement. On 3 November 2019 the Netherlands Minister of Justice and Security publicly stated the need for a possibility for law enforcement to decrypt data in specific cases, under appropriate conditions and safeguards. On 15 November the Minister answered parliamentary questions on this topic. In his answers he underlined both the importance of encryption for safe communications ~~of~~ between individuals, organizations and government, and the importance of access to unencrypted data for national security and law enforcement purposes.

The developments in the use of encryption stress the importance of solutions in the interest of national security and law enforcement. Therefore, we would be interested in discussing possible future solutions, especially those that do not generally weaken encryption, both its use, methods and development. More specifically, we would like to discuss the following questions:

- Does your government have general views you can share on the issue of encryption related to the interests of security of communications, national security and law enforcement?
- What technical possibilities do you consider possible without weakening encryption in general?
- What are the biggest obstacles to finding a solution in your experience?
- Does your government have specific technical, operational and/or legal solutions in place to tackle encryption in the interest of national security and law enforcement?
- What solutions does your government see as desirable or does your government foresee to implement in the near future?
- Would your government prefer an international / EU solution, for example EU legislation?

We would be grateful if you could forward this email to your competent national authorities and if you could indicate which representative(s) wishes to attend the lunch meeting. Should you have any questions or require more information, please don't hesitate to contact us.

Kind regards,

---



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

10.2.e BD/DRC/CV

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** maandag 28 oktober 2019 20:03
**Aan:** 10.2.e . - BD/DRC/CV
**CC:** 10.2.e BD/DRC/CV; 10.2.e - BD/DEIA/IBP; WAS-JenV
**Onderwerp:** RE: Terugkoppeling DGRR-staf

Prima. Bedankt!
10.2.e
Counselor for Justice and Security
Embassy of the Kingdom of The Netherlands
4200 Linnean Avenue N.W.
20008 Washington D.C.
10.2.e
NLintheUSA.com

**From:** 10.2.e - BD/DRC/CV
**Sent:** maandag 28 oktober 2019 15:02
**To:** 10.2.e
**Cc:** 10.2.e - BD/DBAenV/IenK ; 10.2.e - BD/DEIA/IBP ; WAS-JenV
**Subject:** RE: Terugkoppeling DGRR-staf
De oproep aan ICT bedrijven om naast de ontwikkeling van encryptie ook effectieve toegang tot deze gegevens mogelijk te maken. Hiervoor zijn technische oplossingen nodig. Hij nodigt de bedrijven uit deze te ontwikkelingen. De overheid is hierbij graag bereid om samen te werken.

**Van:** 10.2.e minbuza.nl>
**Verzonden:** maandag 28 oktober 2019 19:59
**Aan:** 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**CC:** 10.2.e - BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; WAS-JenV 10.2.e @minbuza.nl>
**Onderwerp:** RE: Terugkoppeling DGRR-staf
Hoi 10.2.e
Nog een nabrander:
Ongetwijfeld zal de journalist vragen: En, minister, wat gaat u hier aan doen?
Welke actie kondigt hij dan aan?
Bedankt,
10.2.e
10.2.e
Counselor for Justice and Security
Embassy of the Kingdom of The Netherlands
4200 Linnean Avenue N.W.
20008 Washington D.C.
10.2.e
NLintheUSA.com

**From:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Sent:** maandag 28 oktober 2019 14:47
**To:** 10.2.e @minbuza.nl>
**Cc:** 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e BD/DEIA/IBP 10.2.e @minjenv.nl>; WAS-JenV 10.2.e @minbuza.nl>
**Subject:** RE: Terugkoppeling DGRR-staf

Ha 10.2.e
Ja dat klopt. NB op locatie, niet in de studio.
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** maandag 28 oktober 2019 19:46
**Aan** - BD/DRC/CV 10.2.e @minjenv.nl>
**CC:** 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>; WAS-JenV 10.2.e @minbuza.nl>
**Onderwerp:** RE: Terugkoppeling DGRR-staf

Hoi 10.2.e
Bedankt voor de terugkoppeling. Begrijp ik goed dat hij zijn interview morgen bij Nieuwsuur over dit onderwerp gaat?
Hgr,

10.2.e
10.2.e
Counselor for Justice and Security
Embassy of the Kingdom of The Netherlands
4200 Linnean Avenue N.W.
20008 Washington D.C.
10.2.e
NLintheUSA.com

**From:** 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>
**Sent:** maandag 28 oktober 2019 14:05
**To:** 10.2.e @minbuza.nl>
**Cc:** 10.2.e BD/DBAenV/IenK 10.2.e @minjenv.nl>; 10.2.e - BD/DEIA/IBP 10.2.e @minjenv.nl>
**Subject:** Terugkoppeling DGRR-staf

Hallo 10.2.e,
We hebben uiteindelijk even kort gebeld met de minister. De minister wordt morgen geïnterviewd door Nieuwsuur. De minister wilt het gesprek over oplossingen stimuleren, noodzaak voor effectieve toegang tot gegevens voor opsporing, maar is op dit moment geen voorstander 11.1 .
Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime
M 10.2.e
10.2.e @minvenj.nl



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message

was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

---

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

10.2.e /DRC/CV

**Van:** 10.2.e BD/DBAenV/IenK
**Verzonden:** maandag 28 oktober 2019 18:18
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** Facts KP en encryptie.docx
**Bijlagen:** Facts KP en encryptie.docx

Dit is mijn A4

## End-to-end encryptie: Wat zijn de gevolgen voor de bestrijding van kinderporno?

De politie ziet gebruik op grote schaal van de verschillende chat- en messenger applicaties voor het delen van strafbaar materiaal. De gevolgen van encryptie voor de bestrijding van kinderporno:

- Een flinke afname van het aantal meldingen over kinderpornografische content (Facebook meldt nu als één van de besten. Een halvering van het aantal meldingen is denkbaar).
- Een verslechtering van de informatiepositie van politierechercheurs. Bijvoorbeeld slechtere vroeg-signalering van verdachten.
- Vertraging bij het in kaart brengen van slachtoffers.
- Het bemoeilijkt het vinden van daders.

Dit geldt voor de bestrijding van kinderporno, maar ook voor bijvoorbeeld wapenhandel.

## Ontwikkeling van meldingen bij politie/OM

In de laatste jaren nam het totaal aantal meldingen van online seksueel misbruik en kinderpornografie bij politie/OM explosief toe:

- Van ruim 5000 in 2015
- Naar ruim 30.000 in 2018

Ten opzichte van 2017 is de instroom van het aantal meldingen bij politie/OM gestegen met 69%.

Een belangrijke oorzaak van de stijging van het werkaanbod is volgens politie/OM onder meer de digitalisering van het leven mondiaal en het feit dat iedereen 27/7 online is en er dus steeds meer communicatie op het internet is.

In 2018 hebben de politieteams die kinderporno bestrijden 636 interventies uitgevoerd en 185 misbruikte kinderen geïdentificeerd.

## Oneliners (uit platte tekst openbrief)

- 11.1 [redacted]

10.2.e - BD/DRC/CV

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** zondag 27 oktober 2019 02:34
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV
**CC:** WAS-JenV; 10.2.e - Nationaal Rapporteur
**Onderwerp:** Gesprek met Minister maandag

Ha 10.2.e en 10.2.e,

Naar aanleiding van onze gesprekken heb ik het kabinetsstandpunt encryptie van 4 januari 2016 vergeleken met:

- de Conclusions van de Council of the EU d.d. 27 september 2019;
- het Statement van NCMEC, d.d. 3 oktober 2019;
- de brief van AG Barr, Secretary of DHS en de ministers van het VK en Australië, d.d. 4 oktober 2019.

Mijn conclusie is dat 11.1 Ik heb enkele citaten op een rij gezet (de onderstrepingen zijn van mij):

In de laatste twee alinea's van de Kamerbrief Kabinetsstandpunt encryptie staat o.a.:
"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."
"Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet (...)"
Conclusie: "Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen (...)"

Tot het nemen van "beperkende wettelijke maatregelen" wordt in geen van de drie documenten opgeroepen. Bovendien zegt het kabinet in deze brief: "op dit moment". Dus

In alle drie documenten wordt het belang van sterke encryptie onderschreven. Zij doen enkel een oproep om deze sterke encryptie in de virtuele wereld zodanig te ontwikkelen, dat vele duizenden kwetsbare kinderen in de fysieke wereld daar niet het slachtoffer van worden:

1. Concusions Council of EU:

Onder punt 13:
"The Council urges the industry to ensure lawful access for law enforcement and other competent authorities to digital evidence, including when encrypted or hosted on IT servers located abroad, without prohibiting or weakening encryption and in full respect of privacy (...). Dit standpunt komt grotendeels overeen met het standpunt van AG Barr c.s.

1. Statement van NCMEC:

Laatste alinea:
"If end-to-end encryption is implemented without a solution in place to safeguard children, NCMEC estimates that more than half of its CyberTipline reports will vanish." Met andere woorden: NCMEC is niet tegen end-to-end encryptie, mits een oplossing wordt gevonden ter bescherming van kinderen.

1. Brief van AG Barr c.s.:

Derde alinea:
"We support strong encryption, which is used by billions of people every day for services such as banking, commerce, and communications. We also respect promises made by technology companies to protect users' data."
Een-na-laatste alinea, vierde bullit van de oproep aan Facebook:
"- Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational."

Zoals we vrijdag bespraken, 11.1

Daarnaast zou het goed zijn als 11.1

- 11.1

Ik hoop dat jullie hier iets aan hebben.
Veel succes maandag!
Ik hoor graag na afloop hoe het geweest is.
Hgr,
10.2.e

10.2.e - BD/DRC/CV

**Van:** 10.2.e @minbuza.nl>
**Verzonden:** donderdag 24 oktober 2019 15:12
**Aan:** 10.2.e BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e - Nationaal Rapporteur
**CC:** WAS-JenV; 10.2.e
**Onderwerp:** FW: Visit of Dutch Minister of Justice and Security to NCMEC
**Bijlagen:** End-to-End Encryption Media Kit (1).pdf

Hoi,
Hierbij alvast het statement over encryptie van NCMEC, dat zij 2 dagen voor het verschijnen van de brief van AG Barr aan Facebook naar buiten hebben gebracht, alsmede een link www.missingkids.org/e2ee naar het deel van hun site dat ingaat op de encryptieproblematiek.
Vanmiddag gaan 10.2.e en ik naar DOJ.
Hgr,
10.2.e

10.2.e
Counselor for Justice and Security

Embassy of the Kingdom of The Netherlands
4200 Linnean Avenue N.W.
20008 Washington D.C.
Mob: 10.2.e
NLintheUSA.com

10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DBAenV/IenK
**Verzonden:** woensdag 23 oktober 2019 09:54
**Aan:** 10.2.e BD/DRC/CV
**Onderwerp:** Brief Facebook
**Bijlagen:** FB ver2.docx

Ik mail je even de reactie van twee tegenlezers.
Deze is van 10.2.e .

## 10.2.e - BD/DRC/CV

**Van:** 10.2.e BD/DBAenV/IenK
**Verzonden:** woensdag 16 oktober 2019 10:31
**Aan:** 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DGPenV/PPBT/PBO
**Onderwerp:** FB en werkbezoek Groningen

Ha 10.2.e
De digijuststroom van de nota nazending werkbezoek Groningen is terug van minister. Hij schrijft: *Graag spoedig overleg hierover ook met dcom er bij.* 11.1

Goed om even kort te sluiten. Groet, 10.2.e

10.2.e
Programmamanager
10.2.e

10.2.e - BD/DRC/CV

**Van:** 10.2.e - BD/DBAenV/IenK
**Verzonden:** vrijdag 11 oktober 2019 11:21
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV
**Onderwerp:** Draft Joint declaration
**Bijlagen:** Joint Declaration of the European Police Chiefs v1.1.pdf

Ha 10.2.e
Zie bijgaande brief: het betreft een mogelijke gezamenlijke reactie van Europese korpschefs tav encryptie met als insteek KP. Politie NL overweegt 11.1
Conform nadrukkelijk telefonisch verzoek bijgaande brief bij ons houden: niet verder verspreiden.
Groet, 10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** 10.2.e @politie.nl>
**Datum:** vrijdag 11 okt. 2019 10:57 AM
**Aan:** 10.2.e @minjenv.nl>
**Onderwerp:** Fwd: Draft Joint declaration

Fyi. Niet ter verspreiding.

Gr.

10.2.e

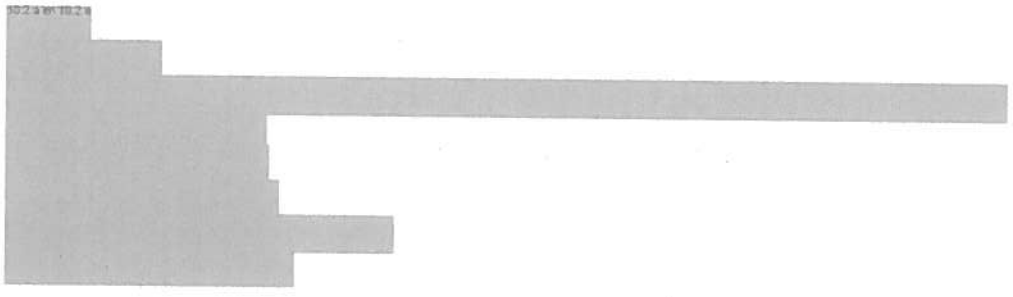
---

**Van:** 10.2.a en 10.2.e
**Verzonden op:** donderdag 10 oktober 2019 17:24
**Aan:** 10.2.e
**CC:** 10.2.a en 10.2.e "
**Onderwerp:** Draft Joint declaration

OFFICIAL

10.2.e

As foreshadowed, attached draft joint declaration, which will be going to Member States as well as relevant third countries and INTERPOL shortly - providing an opportunity to comment.
Regards



10.2.a [redacted]

10.2.a [redacted]

10.2.a [redacted]

10.2.e **BD/DRC/CV**

**Van:** 10.2.e - BD/DCOM/P&B
**Verzonden:** vrijdag 4 oktober 2019 14:01
**Aan:** Grapperhaus, F.B.J. - BD/AL
**CC:** 10.2.e - BD/DCOM/P&B; 10.2.e - BD/DRC/CV; 10.2.e BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e 10.2.e BD/DRC/CV; 10.2.e - BD/DBO; 10.2.e 10.2.e - BD/KS
**Onderwerp:** NOS over encryptie
**Bijlagen:** Verspreiding KP via platforms nav werkbezoek Groningen.docx

Beste Ferd,
De NOS wil je idd bij de uitloop ministerraad nog een paar vragen stellen nav het artikel dat je appte: https://nos.nl/artikel/2304627-vs-wil-uitstel-encryptieplannen-facebook.html

Bij deze opzet in afstemming met 10.2.e. Zij begeleidt je zo bij de uitloop ministerraad.

- Aangeven dat je de open brief nog wilt lezen, maar dat je wel in je eerste reactie kunt zeggen dat:
- Je het dilemma ziet tussen het verder versleutelen – encryptie – van chatdiensten en de aanpak van georganiseerde criminaliteit, terrorisme en kinderporno
- Het is verstandig dat vooraf goed wordt nagedacht wat de maatschappelijke risico's zijn als chatdiensten verder worden versleuteld

- Op dit moment circuleert een enorme hoeveelheid kinderporno op internet. Dit afschuwelijke materiaal wordt ook verspreid en verhandeld via Facebook en Instagram.
- Privacy en cybersecurity zijn van groot belang, maar mag geen schild vormen voor criminelen om zich achter te verschuilen
- En zeker niet voor mensen die kinderporno verspreiden of nog erger - kinderen seksueel misbruiken en beeldmateriaal daarvan verhandelen via internetdiensten

*Gaat u dan verdere encryptie aanpakken?*
- Zoals ik heb gezegd, ga ik de brief eerst lezen.
- Het gaat om de balans tussen legitieme opsporingsbelangen en de privacy en veiligheid

Groeten,
10.2.e

10.2.e
Persvoorlichter

**Ministerie van Justitie en Veiligheid**
**Directie Communicatie**

Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

**M** 10.2.e
10.2.e @minjenv.nl
www.rijksoverheid.nl/jenv

**Voor een veilige en rechtvaardige samenleving**

Ministerie van Justitie en Veiligheid

minister van JenV

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
CV - Programma KP

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverhe d.nl/jenv

**Contactpersoon**
10.2.e

T 070 10.2.e

**Datum**
1 oktober 2019

**Projectnaam**
Aanpak Online seksueel kindermisbruik

**Ons kenmerk**
2880718

**Bijlagen**
1

# memo

Verspreiding kinderporno via social media platformen

## Aanleiding

Woensdag 25 september bezocht u TBKK-Groningen. In de reservetijd gaf digitaal rechercheur 10.2.e aan dat ook via Instagram en Facebook kinderpornografisch beeldmateriaal verspreid wordt. In deze memo krijgt u, conform verzoek, nadere informatie over deze werkwijze. Daarnaast is in deze memo is aanvullende informatie toegevoegd.

- -Ten eerste is over de rol van social media platformen is ook ruggespraak gehouden met de Landelijke Eenheid TBKK-Zoetermeer, om zo een breder beeld te krijgen naast het Groningse voorbeeld.
- -Ten tweede is vanwege actualiteit een alinea toegevoegd over de voorgenomen end-to-end encryptie door Facebook.

De uitleg van de handelswijze uit het Groningse voorbeeld gaat uit van de huidige situatie.

## Wat is de werkwijze in het Groningse voorbeeld?

Een aanbieder van kinderpornografisch beeldmateriaal maakt (meerdere) profielen (sites) aan. Deze profielen maakt hij openbaar: voor eenieder toegankelijk. De profielen zien er gewoon uit maar zijn nep, de getoonde openbare foto's zijn normaal, teksten echter soms wat seksueel. Achter een meisjesprofiel zit bijvoorbeeld een jongen of man. 10.2.c

## Wat gebeurt er?

Wat er plaatsvindt is het leggen van onderling contact, het handelen en leveren van beeldmateriaal via de chatfunctie (of berichtenfunctie), 1 op 1 tussen een aanbieder en een afnemer. Binnen zo'n chat kan ook een upload en download van het beeldmateriaal plaatsvinden. Deze chatfunctie is afgeschermd[1], niet openbaar zichtbaar. 10.2.c

## Waar gebeurt het?

10.2.c

[1] Bij Facebook is deze functie Messenger op dit moment niet end-to-end encrypt.
[2] WhatsApp gebruikt op dit moment wel end-to-end encryptie.

Directoraat-Generaal
Rechtspleging en
Rechtshandhaving
Directie Rechtshandhaving en
Criminaliteitsbestrijding
CV - Programma KP

Datum
1 oktober 2019

Ons kenmerk
2880718

**Waarom op deze platforms?**
Omdat ze door heel veel mensen gebruikt worden, gebruiksvriendelijk en snel zijn. De combinatie van een openbaar profiel en een afgeschermde chatfunctie[3] werkt 'succesvol'.

**Hoe verloopt de handel?** 10.2.c

**Wat weten we over de aanbieder?**
10.2.c

**Wat kunnen we zeggen over de afnemer?**
10.2.c

**Welke risico's lopen aanbieder en afnemer?**
10.2.c

**Hoe weten aanbieder en afnemer elkaar te vinden?**
10.2.c

**Landelijke Eenheid TBKK-Zoetermeer**
Om naast de Groningse zaak een landelijk beeld te verkrijgen is de Landelijke Eenheid TBKK in Zoetermeer (verder: LE) om een reactie gevraagd:
- 10.2.c

[3] Afgeschermd als in niet-openbaar. Het Platform kan er nu nog wel bij en de chat afleveren wanneer dit wordt gevorderd. Dit verandert na introductie end-to-end encryptie.

**Directoraat-Generaal Rechtspleging en Rechtshandhaving**
Directie Rechtshandhaving en Criminaliteitsbestrijding
CV - Programma KP

**Datum**
1 oktober 2019

**Ons kenmerk**
2880718

10.2.c

- 10.2.c

**Handelingsperspectief**
Facebook heeft onder andere filters in hun berichtenverkeer draaien om kinderporno te detecteren. Dit is één van de redenen waardoor Facebook zo veel meldingen kan doen: er is veel én ze vinden veel. In Groningen ging het echter om nieuw materiaal, dat niet met bestaande hashcodes kan worden herkend. Opsporen door OM en politie blijft dus essentieel. 11.1

**End-to-end encryptie door Facebook**
Facebook is voornemens end-to-end encryptie in te voeren voor het berichtenverkeer op hun social media platforms. De overheden van VS, VK en Australië hebben in een brief hun zorgen daarover geuit, mede omdat het detecteren van kinderporno door filters van Facebook dan niet meer mogelijk lijkt. De meldingen door Facebook nemen dan drastisch af, terwijl de uitwisseling van kinderporno op hun platform kan blijven plaatsvinden. 11.1

11.1

**/o=Exchange/ou=DBOB/cn=Recipients/cn=10.2.e**

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** vrijdag 27 september 2019 17:48
**Aan:** 10.2.e - BD/DRC/CV
**Onderwerp:** RE: Nota interceptie OTT samenvatting

Hoi 10.2.e mooie eenvoudige sheets, daar ben ik een fan van. Eén suggestie, niet voor toevoeging, maar wellicht om mondeling mee te nemen: 11.1

**Van:** 10.2.e . - BD/DRC/CV
**Verzonden:** vrijdag 27 september 2019 17:23
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/FO; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/PNDV; 10.2.e LLM, 10.2.e BD/KS; 10.2.e - BD/PNDV; 10.2.e - BD/PNDV; 10.2.e - BD/DBO/ADVIES; 10.2.e n@minbuza.nl'; Dam, A. van - BD/DRC
**Onderwerp:** RE: Nota interceptie OTT samenvatting

Hallo allemaal,

Ter info, bijgevoegd de concept-presentatie.

Met vriendelijke groet,

10.2.e
Beleidsadviseur cybercrime

M 10.2.e
10.2.e @minvenj.nl

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** vrijdag 27 september 2019 15:44
**Aan:** Directiesecretariaat - DRC
**CC:** 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/FO; 10.2.e . - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/PNDV; 10.2.e - BD/KS; 10.2.e 10.2.e - BD/PNDV; 10.2.e - BD/PNDV; 10.2.e - BD/DBO/ADVIES; 10.2.e @minbuza.nl; Dam, A. van - BD/DRC
**Onderwerp:** Nota interceptie OTT samenvatting

Hallo 10.2.e ,

Zou je bijgevoegde nota in IBABS willen zetten voor dinsdag 13:15-14:00 voor minister Grapperhaus? Het overleg vindt plaats op zijn kamer 10.2.e

Zou je naast de personen in CC ook 10.2.e kunnen toevoegen?

Alvast veel dank.

Groet en fijn weekend,

10.2.a

**/o=Exchange/ou=DBOB/cn=Recipients/cn 10.2.e**

**Van:** 10.2.e - BD/PNDV
**Verzonden:** vrijdag 27 september 2019 12:30
**Aan:** 10.2.e - BD/DRC/CV; 10.2.e - BD/KS; 10.2.e - BD/DRC/CV
**CC:** 10.2.e - BD/PNDV; 10.2.e - BD/PNDV
**Onderwerp:** RE: SPOED: OTT: minister wil presentatie ook met NCTV
**Bijlagen:** Interceptie OTT

**Urgentie:** Hoog

Goedemiddag allen,

Dinsdag a.s. vindt een overleg plaats met de minister over de nota interceptie van OTT-diensten.
Mij is gevraagd om daar vanuit de NCTV bij aan te sluiten.
Ik ben benieuwd of er inmiddels meer achtergrond en context bekend waarom is de minister de NCTV erbij wil hebben.
10.2.e heeft eerder aangegeven dat de minister behoefte heeft aan nadere 11.1

In de nota staat onder het kopje "cybersecurity":
11.1

**Uit Kamerbrief encryptie (januari 2016):**

*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.*

**uit Kamerbrief over de voortgang Roadmap Digitaal Veilige Hardware en Software (juni 2019):**
*Het kabinet stimuleert open source encryptie met extra middelen in het kader van de NCSRA III. Het Ministerie van JenV heeft hiervoor een bedrag van € 410.000 ter beschikking gesteld.*

Hartelijke groet, | Kind regards,

10.2.e
Coördinerend senior beleidsmedewerker | Coordinating Senior Policy Officer

.....
**Ministry of Justice and Security**
**National Coordinator for Security and Counterterrorism**
**Coordinator Cyber Security Policy**
.....
M 10.2.e
10.2.e @nctv.minjenv.nl
www.nctv.nl

---

**Van:** 10.2.e - BD/DRC/CV
**Verzonden:** vrijdag 6 september 2019 11:23
**Aan:** 10.2.e - BD/KS; 10.2.e - BD/PNDV; 10.2.e - BD/PNDV; 10.2.e n - BD/PNDV
**Onderwerp:** RE: SPOED: OTT: minister wil presentatie ook met NCTV

Ben ik weer..

De nieuwe datum is **donderdag 3 oktober 13.30-14.15.** Graag hoor ik nog steeds spoedig wie er aanwezig zijn vanuit jullie.

Met vriendelijke groet,

10.2.e **, MSc.**
*Directie Rechtshandhaving en Criminaliteitsbestrijding*
*Afdeling Criminaliteit & Veiligheid*

T: 10.2.e
E: 10.2.e @minveni.nl

.....
*Ministerie van Justitie en Veiligheid*
*DG Rechtspleging en Rechtshandhaving*
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....

.....

---

**Van:** 10.2.e - BD/KS
**Verzonden:** vrijdag 6 september 2019 10:42
**Aan:** 10.2.e - BD/PNDV; 10.2.e BD/PNDV; 10.2.e - BD/PNDV
**CC:** 10.2.e - BD/DRC/CV
**Onderwerp:** SPOED: OTT: minister wil presentatie ook met NCTV
**Urgentie:** Hoog

Hoi 10.2.e en 10.2.e

Bijgaande nota is door DGRR iam ons (10.2.e en mij) naar minister gegaan. strekking 11.1
Maar er zitten ook andere reguleringsvraagstukken aan.
Minister wil door DGRR samen met NCTV worden bijgepraat as. dinsdag.
Wie kan daarbij zijn? Ik ben zelf niet beschikbaar en 10.2.e ook niet.
Svp per ommegaande reactie richting DGRR.

Gr 10.2.e

---

**From:** 10.2.e - BD/DRC/CV
**Sent:** vrijdag 6 september 2019 10:38
**To:** 10.2.e . - BD/KS; 10.2.e - BD/PNDV; 10.2.e BD/DRC/FO; 10.2.e . 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/FO
**Cc:** 10.2.e - BD/DRC/GC
**Subject:** RE: OTT: minister wil presentatie ook met NCTV
**Importance:** High

Beste collega's,

De presentatie over OTT-diensten staat voor nu ingepland op dinsdag **10 september 13.45 – 14.30.** Wel onder voorbehoud van het vragenuurtje, maar op vrij korte termijn dus.

Wie moeten er aanwezig zijn? Dan kan ik dat doorgeven aan 10.2.e, **graag deze ochtend nog reactie.**

Met vriendelijke groet,

10.2.e , **MSc.**
*Directie Rechtshandhaving en Criminaliteitsbestrijding*
*Afdeling Criminaliteit & Veiligheid*

T: 10.2.e
E: 10.2.e @minvenj.nl

.....
*Ministerie van Justitie en Veiligheid*
*DG Rechtspleging en Rechtshandhaving*
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....

.....

---

**Van:** 10.2.e - BD/KS
**Verzonden:** vrijdag 6 september 2019 9:54
**Aan:** 10.2.e - BD/PNDV
**CC:** 10.2.e - BD/DRC/CV
**Onderwerp:** FW: OTT: minister wil presentatie ook met NCTV

ha 10.2.e

minister wil over nota van dgrr over OTTs bijgepraat worden. Strekking vd nota is 11.1
Mhoo cybersecurity regulering lijkt me een 11.1
Kan jij aansluiten bij (nog in te plannen) overleg?

Gr 10.2.e

10.2.e
NCTV
10.2.e

**Van:** 10.2.e @minjenv.nl>
**Datum:** donderdag 05 sep. 2019 4:49 PM
**Aan:** 10.2.e - BD/KS 10.2.e @nctv.minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
**Onderwerp:** RE: OTT: minister wil presentatie ook met NCTV

Dag 10.2.e en 10.2.e

DBO kan geen nadere uitleg geven, ik vermoed dat 11.1 Zou jij kunnen nagaan wie ik kan laten uitnodigen voor de presentatie? Zou je de naam aan mijn collega 10.2.e kunnen doorgeven. Zij zal het OTT dossier samen met 10.2.e een half jaar waarnemen omdat ik bij de NVWA gedetacheerd ben.

@ 10.2.e omdat ik morgen al weg ben, zou jij het op je willen nemen om de presentatie (drie kwartier) met de minister in te laten plannen, dan voorkomen we dat de secretaresse met mij mailt en een out-of-office krijgt? Dat kan via 10.2.e @minjenv.nl). Je kan dan verwijzen naar bijgesloten minuut. Als die is ingepland is het goed om even te kijken wie er bij moeten zijn vanuit ons. Iig 10.2.e ik en eimand van de NCTV en dan even vragen of 10.2.e of 10.2.e er bij willen zijn of dat ze t aan ons laten.

Veel dank alvast.

Groet,

10.2.e

**Van:** 10.2.e - BD/KS
**Verzonden:** woensdag 4 september 2019 17:53
**Aan:** - BD/DRC/FO
**Onderwerp:** RE: OTT: minister wil presentatie ook met NCTV

Hoi 10.2.e weet je waarom hij nctv erbij vroeg? We kunnen morgen even bellen maar ik zit wel op een heidag. Anders vrijdag?

10.2.e
NCTV
10.2.e

**Van:** 10.2.e @minjenv.nl>

**Datum:** woensdag 04 sep. 2019 2:08 PM

**Aan:** BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>, 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>, 10.2.e 10.2.e @nctv.minjenv.nl>

**Onderwerp:** OTT: minister wil presentatie ook met NCTV

Dag allen,

Vers van de pers, de minsiter heeft de OTT nota gelezen en wil graag een presentatie en discussie van drie kwartier waarbij ook de NCTV aansluit. Deze week nog maar even bespreken wat handig is.

Groet

10.2.e
Coördinerend beleidsadviseur Gegevens & Ordening
.....
**Ministerie van Veiligheid en Justitie**
**DGRR-DRC-Afdeling Fraude en Ordening**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

.....

T 10.2.e

10.2.e @minjenv.nl

Secretariaat - 10.2.e

@ 10.2.e @minjenv.nl

T 10.2.e

(Vrijdag afwezig)

# Deel B: stukken NCSC

10(2)(e)

**Van:** [redacted]
**Aan:** [redacted]@lists.ncsc.nl
**Onderwerp:** [redacted] Monday 04-11-2019 07:30 [redacted]
**Datum:** maandag 4 november 2019 14:40:19

---

[redacted]

Buiten scope [redacted]

[redacted]

[redacted]

[redacted]

-= Uitspraken Minister over Encryptie =-
In samenwerking met de Kerneenheid Analyse wordt er een mindmap gemaakt om de verschillende aspecten van encryptie in relatie tot diensten als Whatsapp te belichten.

[redacted]

[redacted]

[redacted]

Buiten scope [redacted]

[redacted]

[redacted]

10(2)(e) [redacted] buiten scope

10(2)(e) [redacted]

11(1) + buiten scope [redacted]

10(2)(e) [redacted]

**Van:** Cert (NCSC-NL) <[redacted]@ncsc.nl>
**Verzonden:** maandag 4 november 2019 11:34
**Aan:** NCSC Bestuurlijke Ondersteuning [redacted]
**Onderwerp:** Encryptie + Grapperhaus

Hoi BO,

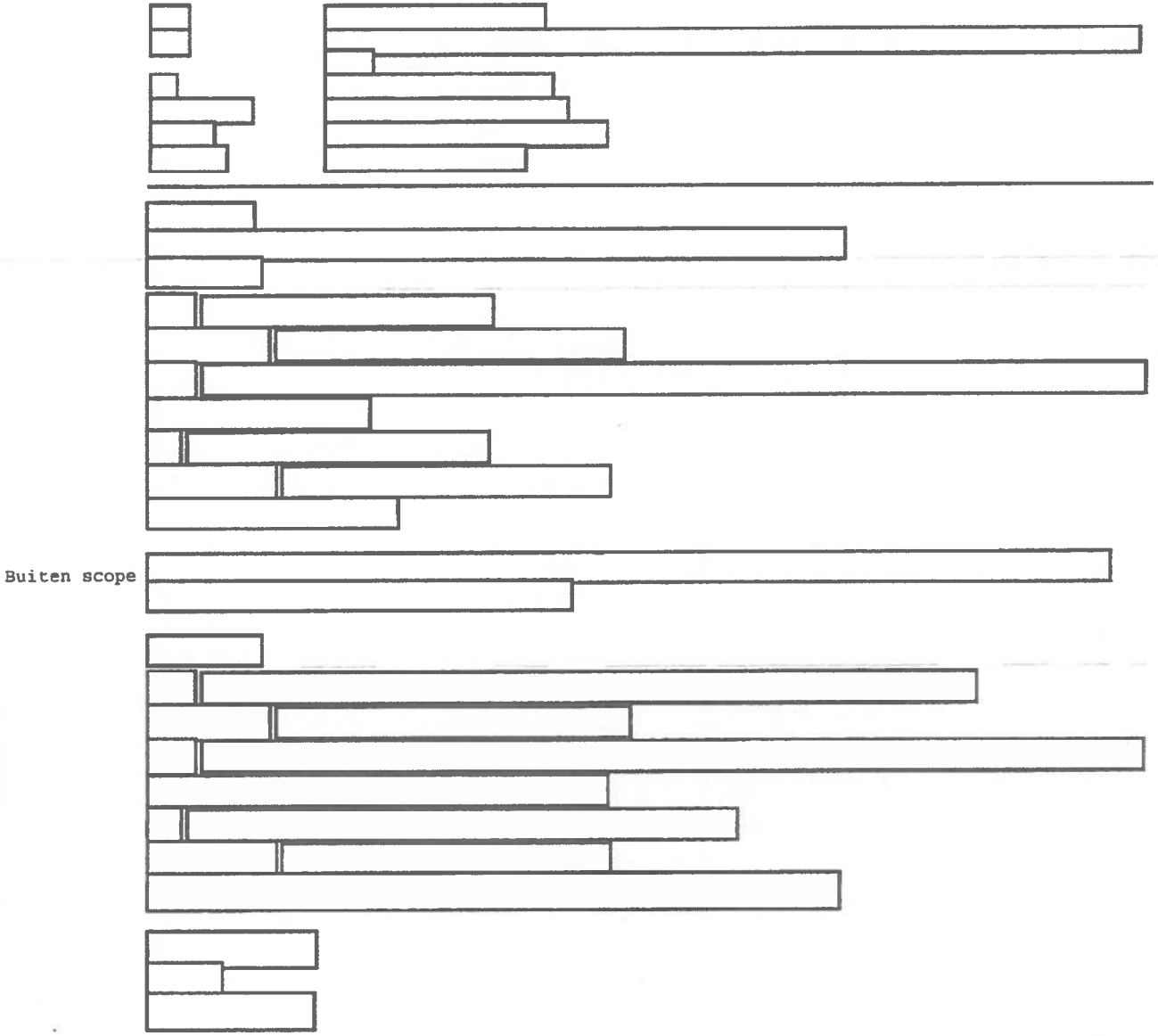
Afgelopen weekend heeft Grapperhaus iets gezegd over encryptie. [redacted] 10(2)(e)
[redacted] en BoF heeft vandaag dit artikel gepubliceerd:
https://www.bitsoffreedom.nl/2019/11/04/grapperhaus-irriteert-niet-gebrek-aan-kennis-over-eigen-beleid/

11(1) + 10(2)(g) [redacted] Volgens het [redacted] van vanochtend wordt er in samenwerking met de Kerneenheid Analyse een mindmap gemaakt om de verschillende aspecten van encryptie in relatie tot diensten als Whatsapp te belichten.

[redacted]

10(2)(e) [redacted]

Buiten scope [redacted]


Buiten scope

# Deel C: stukken NCTV

**Van:** [redacted] BD/DAS/AS
**Aan:** [redacted] BD/PDCT/PBI
**Cc:** [redacted] BD/DRC/FQ; [redacted] - BD/DCS/ACSB; [redacted] - BD/DCS/ACSB; [redacted] BD/PDCT/PBI; [redacted] - BD/DAS/AS; [redacted] BD/DRC/CV
**Onderwerp:** FW: Bezoek Google [redacted]
**Datum:** maandag 22 januari 2018 11:37:30
**Bijlagen:** Factsheet Encryptie.docx

10.2.e

---

Ha [redacted]
2 opties: je kunt het encryptie factsheet bijvoegen maar dat is volgens mij veel te uitgebreid. Hooguit voor Dick (gezien detailniveau). Of je voegt onderstaande tekst nog onderaan in je notitie. 10.2e
Final version gaat nog wel via Dick toch? Gr [redacted]

**Encryptie**:

- Het Nederlandse kabinetsstandpunt inzake encryptie is op 4 januari 2016 geformuleerd: 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. Het kabinet heeft daarnaast tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen en onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Het kabinet is 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.
- Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptieproducten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren.
- Dit draagt NL ook in de EU uit.
- In de EU zijn/ worden de mogelijkheden bezien inzake encryptie: technisch (bijv. tools), operationeel (bijv. training) en wettelijk. Er vindt een dialoog met aanbieders plaats in het EU internet forum, en er wordt wetgeving voorgesteld voor e-evidence en e-privacy. Het voorstel voor de E-privacy verordening richt zich op het gelijkstellen van internet services aan telecomproviders, waaronder de verplichting tot medewerking in strafzaken voorzover mogelijk. Het Europees Parlement heeft zich in juni 2017 expliciet uitgesproken n.a.v. de verordening (amendement 116) voor de verplichting tot end-to-end-encryptie en een verbod op backdoors. Dit is in de Raad nog niet behandeld.
- Enkele Lidstaten hebben (of overwegen) nationale juridische verplichtingen voor alle aanbieders van internet- of elektronische communicatie om mee te werken aan het rechtsproces, inclusief het aanbieden van ontsloten (gedecrypteerde) informatie of het toegankelijk maken van "legal access." Het toegankelijk maken van content voor autoriteiten is niet mogelijk in geval van end-to-end-encryptie.

---

**From:** [redacted] BD/PDCT/PBI
**Sent:** maandag 22 januari 2018 11:10
**To:** [redacted] BD/DAS/AS; [redacted] BD/DAS/AS
**Cc:** [redacted] - BD/PDCT/PBI
**Subject:** RE: Bezoek Google [redacted]

10.2.e

Hey,
[redacted] Ja, fijn. Ok, dat helpt me idd.
[redacted] eens, ga ik aanpassen. Deze indeling hadden we afgesproken, maar is niet logisch.
Gezien? https://www.buzzfeed.com/alexkantrowitz/youtube-intelligence-desk-will-spot-inappropriate-content?utm_term=.fqLZZY0vK#.fe6KKboeB
Dit bericht ga ik ook nog even verwerken.
Groeten,
[redacted]

---

**Van:** [redacted] BD/DAS/AS
**Verzonden:** vrijdag 19 januari 2018 10:15
**Aan:** [redacted] BD/PDCT/PBI
**CC:** [redacted] BD/DAS/AS
**Onderwerp:** FW: Bezoek Google [redacted]
Verkeerde adresbalk, zie onder [redacted]
Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** [redacted] - BD/DAS/AS <[redacted]@nctv.minvenj.nl>
**Datum:** vrijdag 19 jan. 2018 10:14 AM
**Aan:** [redacted] - BD/DAS/AS <[redacted]@nctv.minvenj.nl> 10.2.e
**Onderwerp:** RE: Bezoek Google [redacted]
Hoi [redacted] op Cyber krijg je nog wat van ons. OTT info (van [redacted] is ter info voor jou als dossierhouder niet voor dit gesprek.

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** [redacted] BD/DAS/AS <[redacted]@nctv.minvenj.nl>
**Datum:** donderdag 18 jan. 2018 3:46 PM
**Aan:** [redacted] - BD/PDCT/TR <[redacted]@nctv.minvenj.nl>, [redacted]. - BD/PDCT/PBI <[redacted]@nctv.minvenj.nl>, [redacted] - BD/PDCT/PBI [redacted]@nctv.minvenj.nl>, [redacted] - BD/DW/AGV [redacted]@nctv.minvenj.nl>, [redacted] - BD/DRC/CV <[redacted]@minvenj.nl>, [redacted] - BD/DRC/FO [redacted]@minvenj.nl>, [redacted] BD/DCS/ACSB <[redacted]@nctv.minvenj.nl>, [redacted]. - BD/DBAenV/IenK <[redacted]@minvenj.nl>, [redacted]. - BD/DAS/AS <[redacted]@nctv.minvenj.nl>, [redacted]. - BD/PDCT/TR [redacted]@nctv.minvenj.nl> 10.2.e
**Kopie:** [redacted] - BD/DCS/ACSB [redacted]@nctv.minvenj.nl>, [redacted] - BD/PDCT/VS <[redacted]@nctv.minvenj.nl>
**Onderwerp:** RE: Bezoek Google [redacted]
Hoi [redacted]

[redacted] L

Groet,
[redacted]

**Van:** [redacted]. - BD/PDCT/TR
**Verzonden:** donderdag 18 januari 2018 14:31
**Aan:** [redacted] - BD/PDCT/PBI; [redacted] - BD/DAS/AS; [redacted] - BD/PDCT/PBI; [redacted] BD/DW/AGV; [redacted]. - BD/DRC/CV; [redacted] - BD/DRC/FO; [redacted] - BD/DCS/ACSB; [redacted] - BD/DBAenV/IenK; [redacted] - BD/DAS/AS; [redacted] - BD/PDCT/TR
**CC:** [redacted] - BD/DCS/ACSB; [redacted]. - BD/PDCT/VS
**Onderwerp:** RE: Bezoek Google [redacted]

[redacted] L

Groet,
[redacted]

---

**Van:** [redacted] - BD/PDCT/PBI
**Verzonden:** donderdag 18 januari 2018 13:55
**Aan:** [redacted] - BD/DAS/AS; [redacted] - BD/PDCT/PBI; [redacted] BD/DW/AGV; [redacted] - BD/DRC/CV; [redacted] - BD/DRC/FO; Berg, [redacted] - BD/DCS/ACSB; [redacted] - BD/DBAenV/IenK; [redacted] - BD/DAS/AS; [redacted] - BD/PDCT/TR; [redacted] - BD/PDCT/TR
**CC:** [redacted] - BD/DCS/ACSB; [redacted]. - BD/PDCT/VS
**Onderwerp:** RE: Bezoek Google [redacted]
Beste collega's,
Dank voor jullie aanwezigheid afgelopen maandag.
Zoals afgesproken stuur ik jullie hierbij een opzetje voor onze gezamenlijke annotatie.
Ook suggesties voor een bijv. een andere indeling of iets dergelijks zijn welkom.

Graag ontvang ik jullie afgestemde bijdragen in het Engels voor maandag 22 januari 12:00.
[redacted] dank voor je snelle input en afstemming met BZK.
[redacted] dank voor je email, maar ik vond het lastig om te beoordelen of ik de stukken die je meestuurde over OTT diensten integraal over kon nemen.
[redacted]
Dank en groeten,
[redacted]
<< Bestand: Bezoek Google nav EU Internet forum.doc >>
-----Oorspronkelijke afspraak-----
**Van:** [redacted] BD/PDCT/PBI
**Verzonden:** maandag 15 januari 2018 17:54
**Aan:** [redacted] - BD/PDCT/PBI; [redacted] - BD/DAS/AS; [redacted] - BD/PDCT/PBI; [redacted] - BD/DW/AGV; [redacted] - BD/DRC/CV; [redacted] BD/DRC/FO; [redacted] BD/DCS/ACSB; [redacted] - BD/DCS/ACSB
**CC:** [redacted] - BD/PDCT/TR; [redacted] BD/PDCT/TR; [redacted] - BD/DAS/AS; [redacted] - BD/DBAenV/TenK
**Onderwerp:** Bezoek Google [redacted]
**Tijd:** dinsdag 16 januari 2018 11:30-12:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
**Locatie:** [redacted] (melden bij NCTV receptie)
Heren,
Op 25 januari komt [redacted] (Google [redacted] op bezoek bij onze Minister.
Onze Minister heeft aangegeven te willen spreken over:
[redacted]
Graag wil ik kort van jullie horen of er vanuit jullie werk elementen zijn die jullie graag zouden willen agenderen.
Hopelijk tot morgen!
[redacted]
Ps. excuses voor dit later vergaderverzoek.

DEPARTEMENTAAL VERTROUWELIJK

**Factsheet Encryptie**

| | |
|---|---|
| Dossierhouder | [redacted] |
| Bereikbaarheid | [redacted]nctv.minvenj.nl |
| Datum factsheet | 22-01-2018 |

10.2.e

**Prioriteiten inzake encryptie**

- Internationaal: volgen van EU discussie, Commissie streeft geen wetgeving na maar beleidsmatige maatregelen zoals training, dialogen met Internet service providers (ISP's) en kennis-uitwisseling. Wel worden Over the top leveranciers (OTT's) straks meer gereguleerd (e-privacy verordening) en ontstaan daarmee verplichtingen tot medewerking. Het formeel toegankelijk maken van content voor autoriteiten is niet mogelijk in geval van end-to-end-encryptie.
- UK, Frankrijk en Duitsland hebben opgeroepen tot meer (al dan niet nationale) wetgeving t.a.v. het breken van encryptie door ISP's/OTT's.
- Nationaal: CVIN heeft PIDS (beleidsgroep) opdracht gegeven om binnen de marges van het kabinetsstandpunt te bezien welke (technische en beleidsmatige) oplossingen mogelijk zijn t.b.v. doorbreken/omzeilen van encryptie voor rechtmatige doeleinden.

**NL kabinetsstandpunt**

- Het kabinetsstandpunt is op 4 januari 2016 geformuleerd door de volgende partners: V&J NCTV, DGRR, NCSC/ BZK CZW (grondrechten) en AIVD/ BZ/ DEF MIVD/ EZ.
- Vaak wordt de discussie over encryptie voorgesteld als een keus tussen veiligheid en privacy. Dat is echter een onjuiste vereenvoudiging van feiten. Cybersecurity (veiligheid in het digitale domein) is bijvoorbeeld gebaat bij encryptie; terwijl tegelijkertijd het zicht op communicatie van kwaadwillenden onder gebruik van encryptie te lijden heeft. Ook economische belangen spelen overigens een rol (MinEZ).
- 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.
- Het kabinet heeft daarnaast tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen en onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie.
- Het kabinet is 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.
- Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptieproducten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren.
- Het kabinet vindt van belang dat bevoegde autoriteiten op rechtmatige wijze bij versleutelde informatie kunnen. Daarom vindt binnen de afzonderlijke diensten, maar ook in interdisciplinair overleg onderling, onderzoek plaats naar de mogelijkheden voor overheidsdiensten om in dat verband bij versleutelde informatie te kunnen komen om georganiseerde criminaliteit het hoofd te bieden en de nationale veiligheid te waarborgen. Het doel is om de beleidsmatige en operationele mogelijkheden te bezien, en mogelijkheden te benutten van kruisbestuiving, bijvoorbeeld in relatie tot contact met digitale dienstverleners. Uiteraard blijven de verschillende diensten verantwoordelijk voor de uitoefening van hun eigen taken en bevoegdheden, zoals die hun in wetgeving zijn toegekend.

**EU**

- NL heeft in juni 2016 tijdens het Nederlandse voorzitterschap in de JBZ ingestemd met een tweetal Raadsconclusies ter verbetering van de bestrijding van criminele activiteiten in cyberspace (brief van 27 juni 2016, TK, Vergaderjaar 2015-2016

Kamerstuk 32317 nr. GP). De aanpak bestaat uit drie elementen: Versterken samenwerking met internet service providers; Stroomlijnen rechtshulpprocedures; Herziening regels handhavingsjurisdictie ("enforcement jurisdiction") in cyberspace.

- Tijdens dezelfde JBZ is ook besloten om de technische en legale mogelijkheden te bezien inzake encryptie. Een werkgroep van de CIE heeft in de loop van 2017 de opties uitgewerkt en JBZ heeft deze aanpak in december 2018 geakkordeerd (11e voortgangsrapportage).
- Momenteel wordt vanuit Europa een dialoog gevoerd met OTTs waarin wordt gestreefd naar een oplossing. [redacted] L
- Tegelijk heeft Commissaris Jourová aangekondigd maatregelen, incl. wetgeving, te maken voor betere toegang van Law Enforcement tot internet messages (incl. Whatsapp) met name om deze gemakkelijker buiten Europese jurisdictie op te vragen. Dit spreekt zich nog niet expliciet uit over encryptie.
- Het voorstel voor de E-privacy verordening richt zich op het gelijkstellen van internet services aan telecomproviders, waaronder de verplichting tot medewerking in strafzaken voorzover mogelijk. Naast de aard van de dienst, is er nog een belangrijk verschil tussen het verkeer van OTT-providers (wereldwijd over internet en dus een groter risico op onderschepping onderweg) en dat van telecomproviders (waar hun verkeer in de meeste gevallen binnen lands- regionale grenzen blijft).
- EP heeft zich in juni 2017 uitgesproken n.a.v. de verordening (amendement 116) voor de verplichting tot end-to-end-encryptie en een verbod op backdoors.[1]

**Andere landen**

- Encryptie is onderwerp van brede internationale discussie. In veel Europese landen is deze discussie nog niet tot een conclusie gekomen; [redacted] 10.2a
- **Frankrijk en Duitsland** roepen in de Joint Letter van november 2016 de Commissie onder meer op een wetgevend voorstel te overwegen rondom de verplichtingen voor alle aanbieders van internet- of elektronische communicatie om mee te werken aan het rechtsproces. Ze willen dezelfde voorwaarden als voor telecomproviders. [redacted] 11.1
- **Duitsland** heeft in juni 2017 een wetsvoorstel gelanceerd om het recht tot decryptie en het lezen van encrypted messages te regelen, en De Maizière noemde daarbij expliciet Whatsapp en Signal. [redacted] In dec 2018 heeft DUi echter aangegeven dat zij producenten willen gaan verplichten legal access mogelijk te maken tot private producten/hardware/IoT e.d. 11.1
- **VK** sluit zich hierbij aan en Amber Rudd sprak zich in maart uit voor gedwongen overlevering van data door expliciet whatsapp. De UK investigatory powers act biedt ook het vooruitzicht om ISPs en telecomproviders te verplichten om toegang te geven tot decrypted content 'wherever possible' waarbij men ook kijkt naar het verplichtstellen van technical capabilities bij nieuwe producten [redacted]. 11.1
- De **VS** hebben een soortgelijk standpunt als VK, DUI. Het Encryption working group van het parlement (dec. 2016) heeft zich overigens uitgesproken tegen generieke

[redacted]

verzwakking van encrytie, maar wil wel bekijken wat mogelijk is *legal hacking* en *exploitation of vulnerabilities* mogelijk te maken voor opsporing (via Vulnerabilities Equities Process) of om tot een decryptie-bevel te komen.

**Medewerking OTT's en ISP's**

- [redacted] 10.2a

20180309

**Van:** [redacted] - BD/DAS/AS
**Aan:** [redacted] - BD/DAS/AS; [redacted] - BD/DAS/AS
**Onderwerp:** anno dick voor reis naar [redacted]
**Datum:** vrijdag 9 maart 2018 16:50:07
**Bijlagen:** CONCEPT dossiernotitie cybersecurity NCTV [redacted] maart 2018 [redacted].docx

10.2.e
10.2.a

Dick neemt cyber mee in zn dossier voor [redacted] Ter lering ende vermaack zie anno
ook stuk over ncsa
Gr [redacted],

10.2.a
10.2.e

20180309-1

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
*Ministerie van Justitie en Veiligheid*

NCTV

**Directie Cybersecurity**
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
**Contactpersoon**
[redacted]

**Datum** 10.2.e
14 maart 2018
**Ons kenmerk**
-

# nota

Cybersecurity

[redacted]

L

[redacted]

L

**Spreektekst**

[redacted]

10.1.d
10.2a

[redacted]

10.2.a

[redacted]

**Directie Analyse en Strategie**

**Datum**
15 november 20178

**Ons kenmerk-**

L

Encryption

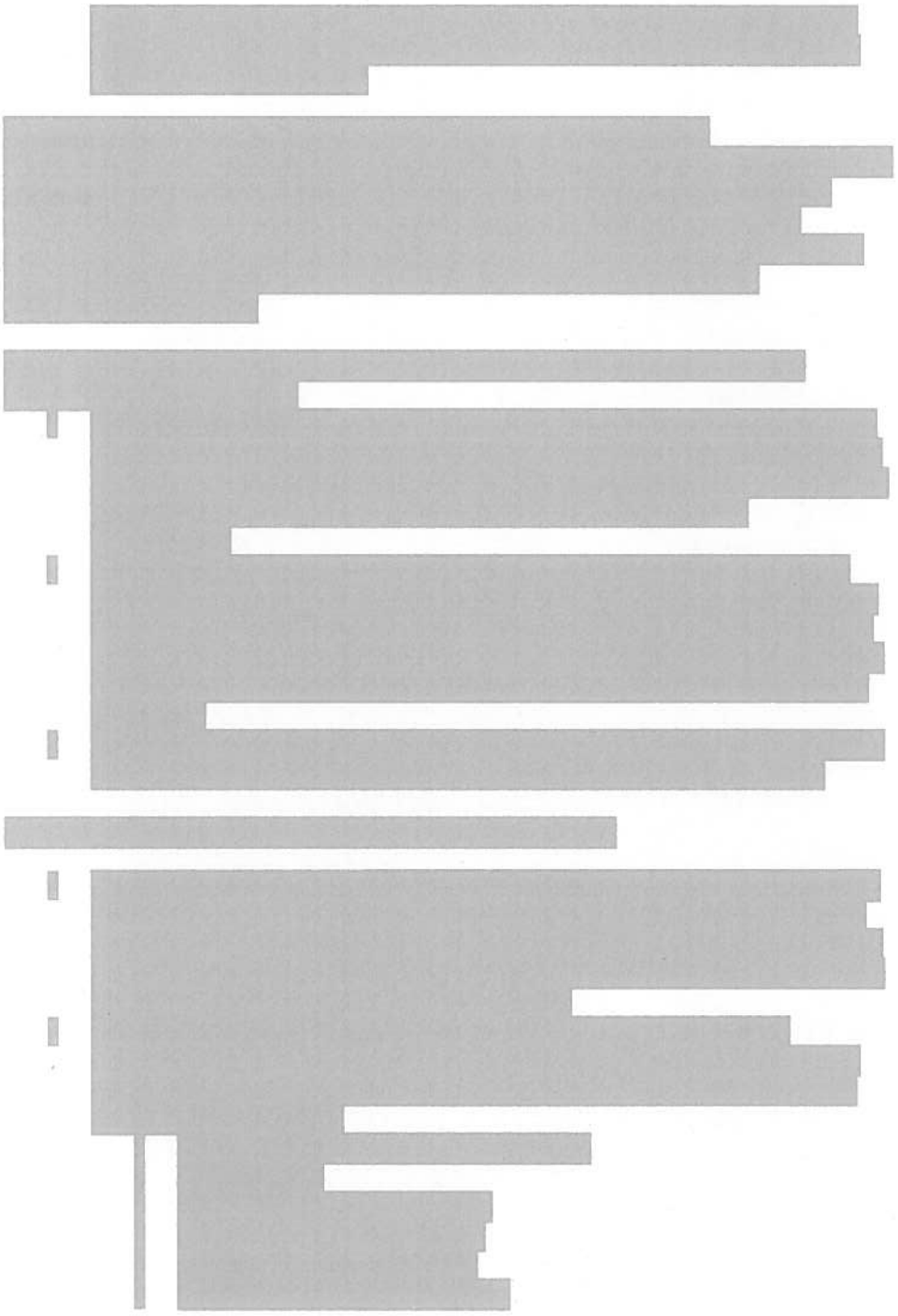
- NL stresses that increased use of encryption is a positive development, necessary for protecting human rights, privacy, confidentiality of communication, to stimulate economic growth and innovation, and cybersecurity;
- At the same time, NL acknowledges that there is a need for competent authorities to be able to access encrypted information.
- Dealing with this challenge while maintaining secure communications is a discussion for the coming years.
- Interesting to hear [redacted] view on the application of legislation to Internet Service Providers and Over the Top providers (OTT's: such as WhatsApp/ telegram/signal etc.)? And specifically, compliance with requests for (decrypted) information? 10.2.a
- NL finds that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption. NL wants to strengthen the cooperation on a voluntary basis with internet service providers to counter crime and radicalization via internet. What's is [redacted] position? 10.2.a

[redacted]

10.2.a
L

10.2.a
L

L
10.1.b

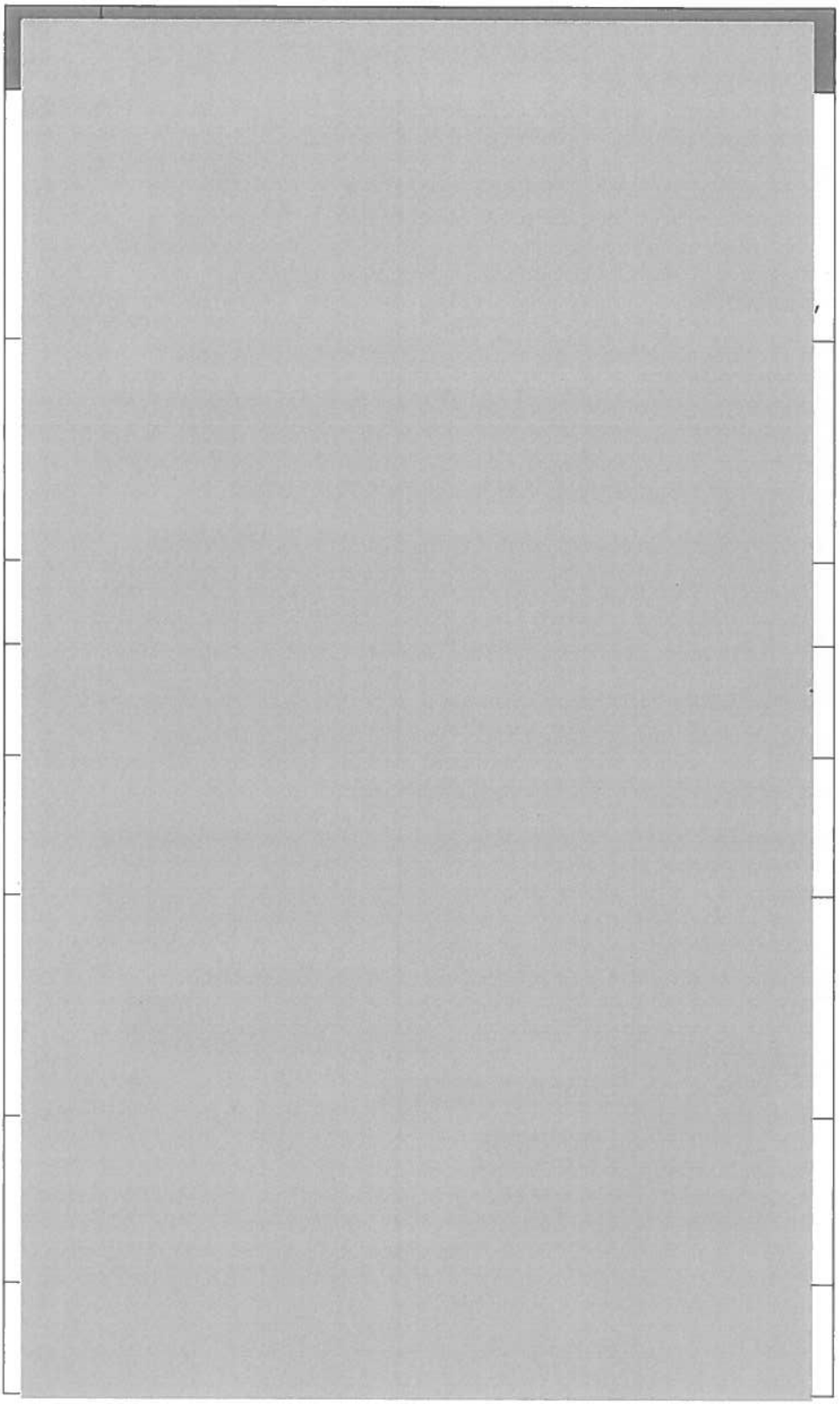


**Directie Analyse en Strategie**

**Datum**
15 november 20178

**Ons**

L; 10.1.b



**Directie Analyse en Strategie**

**Datum**
15 november 20178

**Ons kenmerk-**

L

[redacted]

L

Encryptie
NL draagt het kabinetsstandpunt van 4 januari 2016 actief uit. NL en EU (en andere landen) ervaren grote uitdagingen bij rechtshandhaving (en inlichtingenvergaring) vanwege sterke en alom aanwezige encryptie.

11.1
10.1.b

[redacted]

L
10.1.b

**Van:** [redacted] BD/DAS/AS
**Aan:** BD/DCS/NCSC/AMP
**Cc:** [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/ACSB; [redacted] BD/DCS/ACSB; BD/DCS/ACSB; BD/DCS/ACSB; [redacted] BD/DCS/NCSC/ANDN; BD/DCS/NCSC/ANDN; BD/DCS/NCSC/AMP; [redacted] BD/DCS/NCSC/AEA; BD/DCS/NCSC/AMR; [redacted] IND/BV/IVB/K&N; BD/DCS/NCSC/AEA; [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/NCSC/AEA
**Onderwerp:** RE: Gesprek RSA met [redacted]
**Datum:** vrijdag 6 april 2018 16:50:13
**Bijlagen:** tk-kwetsbaarheden-in-hardware_en-software (1).pdf
Lijnconcept NCSA 2018_20180406.docx
Dossier RSA_input DAS [redacted].docx

10.2.e

---

Ha [redacted]
hierbij anno retour met aanvullingen.

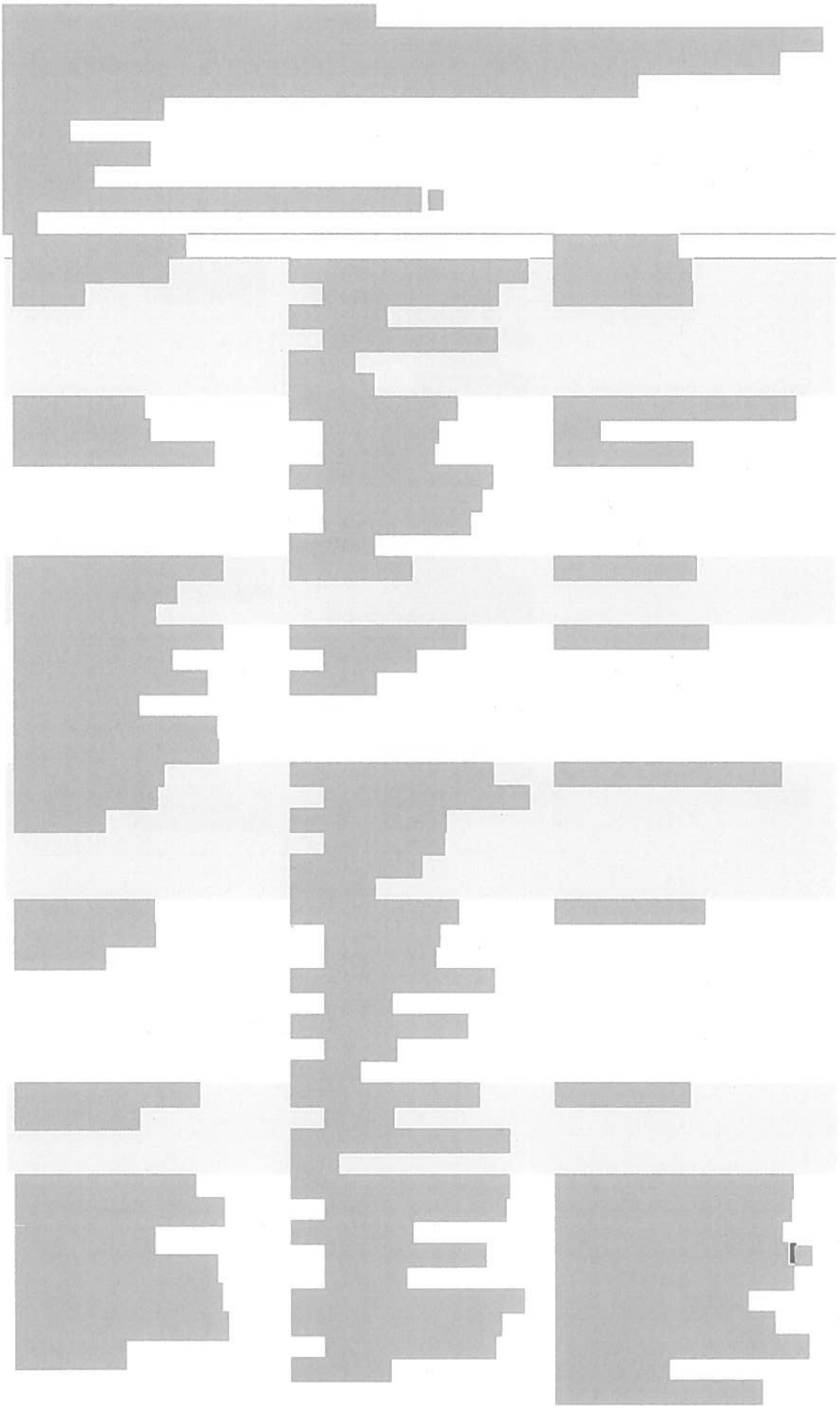
[redacted] 11.1

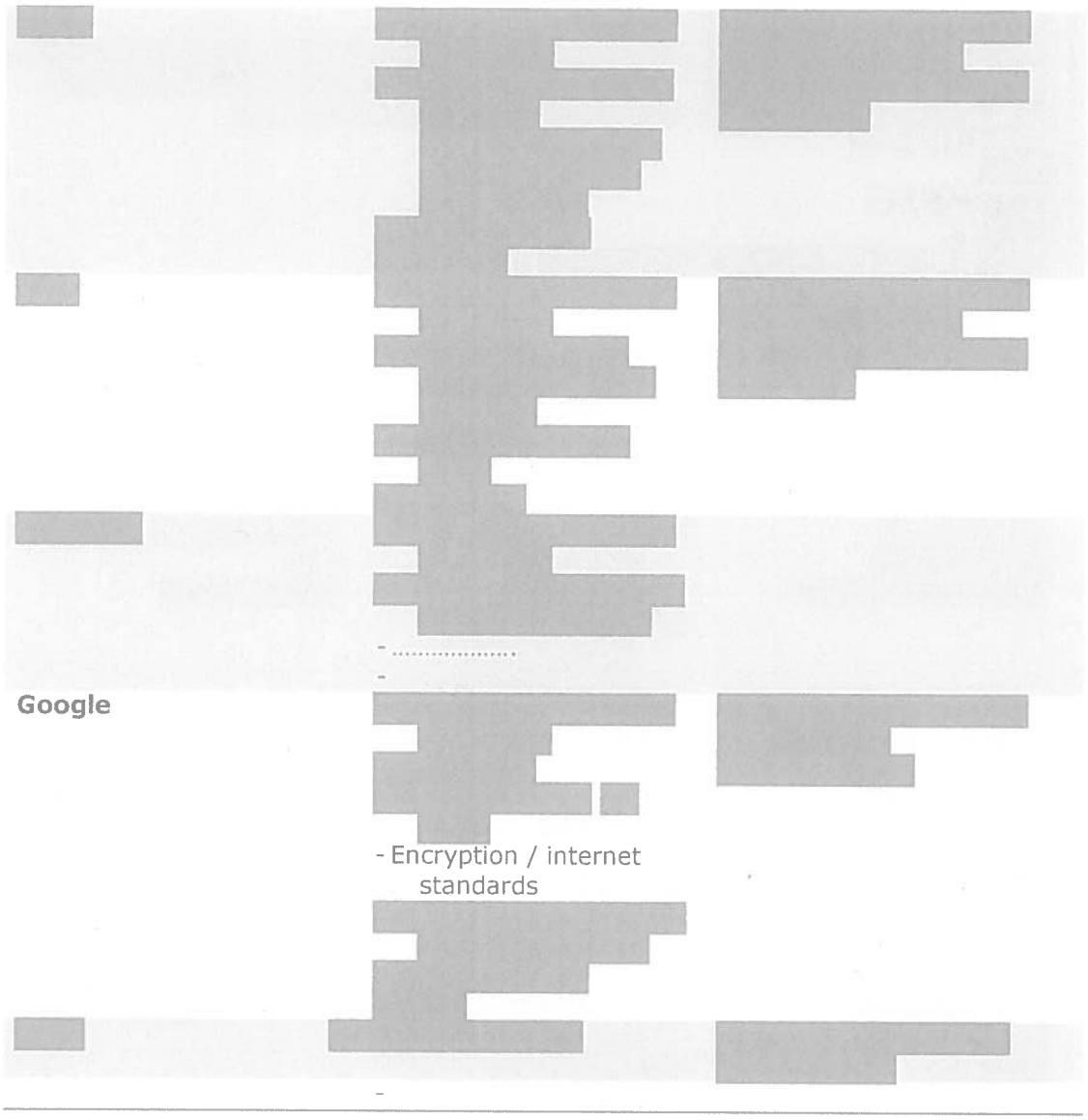
**From:** [redacted] BD/DCS/NCSC/AMP
**Sent:** vrijdag 6 april 2018 13:48
**To:** [redacted] BD/DAS/AS

[redacted] L

**From:** [redacted] BD/DCS/NCSC/AMP
**Sent:** vrijdag 30 maart 2018 15:17
**To:** [redacted] BD/DCS/NCSC/ANDN; [redacted] BD/DCS/ACSB; [redacted] BD/DCS/NCSC/ANDN; [redacted] BD/DCS/NCSC/AMP; [redacted] BD/DCS/ACSB; [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/NCSC/AMR; [redacted] BD/DCS/NCSC/AMR; [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/NCSC/AEA; [redacted] - BD/DAS/AS
**Cc:** [redacted] BD/DCS/ACSB; [redacted] BD/DCS/NCSC/AEA; [redacted] BD/DCS/ACSB
**Subject:** Verzoek om aanvulligen dossier HdV RSA + bilats

[redacted] L




Google
- Encryption / internet standards

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

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.

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

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

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

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:** [redacted] - BD/DAS/AS
**Aan:** [redacted] - BD/PDCT/TR; [redacted] - BD/DCS/ACSB
**Cc:** [redacted] - BD/PDCT/PBI; [redacted] - BD/DCS/ACSB; [redacted] BD/DAS/AS; [redacted] - BD/DAS/AS
**Onderwerp:** FW: Russische rechter beveelt blokkade van chat-app Telegram
**Datum:** vrijdag 13 april 2018 15:05:29

10.2.e

---

Hi crypto's,
Ter info onderstaand berichtje.
Meteen even beleidsupdate-tje:

- Met dgrr ([redacted]) bijgepraat: [redacted] heeft encrypti[redacted] 10.2.e
  dossier van [redacted] overgenomen.
- [redacted] 11.1
  L
  )
- [redacted] 10.2.e
  11.1
- Overige trajecten mondeling: loop maar keertje langs.

Gr [redacted]

---

**From:** [redacted] - BD/DAS/ANTMD
**Sent:** vrijdag 13 april 2018 14:15
**To:** [redacted] - BD/DW/AGV; [redacted] - BD/DCS/NCSC/ANDN; [redacted] - BD/DAS/ANTMD; [redacted] - BD/DAS/ANTMD; [redacted] - BD/DAS/ANTMD; [redacted] . - BD/DW/AGV
**Cc:** [redacted] - BD/DAS/ANTMD; [redacted] - BD/DCS/ACSB; [redacted] - BD/DAS/ANTMD; [redacted] BD/DW/AGV; [redacted] - BD/DAS/AS; [redacted] . - BD/DAS/AS
**Subject:** Russische rechter beveelt blokkade van chat-app Telegram

[redacted] 11.1

## Russische rechter beveelt blokkade van chat-app Telegram

vrijdag 13 april 2018, 11:06 door **Redactie**, 2 **reacties**

Een Russische rechter heeft bevolen dat de versleutelde chat-app Telegram per direct in Rusland moet worden geblokkeerd omdat het inlichtingendiensten in het land geen toegang tot de inhoud van versleutelde chatberichten geeft, zo meldt het Russische persbureau **TASS**.
Eind maart kreeg Telegram van de Russische mediatoezichthouder Rospotrebnadzor **het bevel** om binnen 15 dagen informatie aan de Russische opsporingsdiensten te verstrekken. Standaard maakt Telegram gebruik van versleuteling, maar dit is geen end-to-end-encryptie. Deze vorm van versleuteling wordt alleen in de "secret chats" functie aangeboden. Voor de normale chats, zowel privé als in een groep, maakt Telegram gebruik van server-client-encryptie.
Telegram-oprichter Pavel Durov liet na de uitspraak van de toezichthouder in maart weten dat de chatdienst zich niet zou laten bedreigen. Een aantal dagen later maakte Telegram bekend dat het de **200 miljoen gebruikers** was gepasseerd. **Begin april** kondigde de toezichthouder aan dat

het Telegram door de rechter wilde laten blokkeren. De rechter heeft dit verzoek nu ingewilligd. De blokkade blijft net zolang in stand totdat Telegram voldoet aan de eisen van de Russische geheime dienst FSB.
https://www.security.nl/posting/558098/Russische+rechter+beveelt+blokkade+van+chat-app+Telegram

**Van:** [redacted]
**Aan:** [redacted] BD/DAS/AS; [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP - instructie 17 juli
**Datum:** maandag 16 juli 2018 17:25:00

10.2.

Ik ben al bezig met een voorzet. Over 15-30 minuten kan ik iets sturen denk ik.

**From:** [redacted] BD/DAS/AS
**Sent:** vrijdag 13 juli 2018 13:43
**To:** [redacted] BD/DCS/ACSB ; [redacted] BD/DRC/CV
**Cc:** [redacted] BD/DRC/CV ; [redacted] BD/DRC/CV
**Subject:** RE: HWP - instructie 17 juli

10.2.e
11.1

[redacted]

1. NL hecht eraan het NL kabinetsstandpunt t.a.v. encryptie nogmaals te benadrukken:

   - 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.

   - Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptieproducten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren.

2. NL acht wenselijk om de lijnen zoals in Raadsconclusies december 2017 geformuleerd (4 uitgewerkte ontwikkellijnen, evenals conclusies dat wettelijke maatregelen niet opportuun waren) verder uit te werken; wel binnen huidige wettelijke kaders.
3. Daarnaast heeft NL CC3 aangenomen die strenge waarborgen stelt t.a.v. de inzet van bijzondere bevoegdheden voor opsporingsdiensten, zoals bevoegdheid tot binnendringen in een geautomatiseerd werk. Het is van belang dat betrokkenheid van EU/ Europol bij inzet van dergelijke bijzondere bevoegdheden aansluit.

[redacted]

11.1
10.2.a

**From:** [redacted] BD/DCS/ACSB
**Sent:** donderdag 12 juli 2018 18:56
**To:** [redacted] BD/DRC/CV
**Cc:** [redacted] BD/DAS/AS; [redacted] BD/DRC/CV; [redacted] BD/DRC/CV
**Subject:** RE: HWP - instructie 17 juli

10.2e

[redacted]

11.1

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minvenj.nl>
**Datum:** donderdag 12 jul. 2018 6:05 PM
**Aan:** [redacted] BD/DCS/ACSB <[redacted]@nctv.minvenj.nl>
**Kopie:** [redacted] BD/DAS/AS <[redacted]@nctv.minvenj.nl>,

[redacted] BD/DRC/CV
<[redacted]@minvenj.nl>, [redacted] BD/DRC/CV <[redacted]@minvenj.nl>
**Onderwerp:** RE: HWP - instructie 17 juli
[redacted] 10.2.a

**Van:** [redacted] BD/DCS/ACSB
**Verzonden:** donderdag 12 juli 2018 17:07
**Aan:** [redacted] BD/DCS/ACSB; [redacted] BD/DCS/NCSC/AMP; [redacted]@minbzk.nl'; [redacted] BD/DAS/AS; [redacted] BD/DRC/CV; [redacted]@mindef.nl'; [redacted] - BD/DRC/CV; [redacted]@minez.nl'; [redacted] - BD/DRC/CV 10.2.e
**CC:** [redacted]@minbuza.nl; [redacted] - BD/DAS/AS
**Onderwerp:** HWP - instructie 17 juli

Allen,

Bijgevoegde de instructie voor de HWP van komende dinsdag. Al met al een groot aantal onderwerpen. Instructie per thema staat beneden aangegeven. Graag ontvang ik jullie in put voor **aanstaande maandag 12.00 uur.**

Agendapunt 2: NCTV, EZK, BZ
Agendapunt 3: NCTV
Agendapunt 4: NCTV
Agendapunt 5 ([redacted]): EZK
Agendapunt 6 ([redacted]): EZK, DGRR, NCTV/NCSC
Agendapunt 7 (encryptie): DGRR, NCTV ([redacted]) L 10.2.a
Agendapunt 8 (post-quantum encryptie): DGRR, NCTV ([redacted])

[redacted]

[redacted] 10.2.e

[redacted]

.....

**Ministerie van Justitie en Veiligheid | Ministry of Justice and Security**
**Directie Cyber Security | Department of Cyber Security**
**Afdeling Cyber security beleid | Cyber Security Policy Division**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | P.O. Box 20301 | 2500 EA | Den Haag | The Netherlands
.....
[redacted]
[redacted] nctv.minvenj.nl 10.2.e
www.nctv.nl
.....

**Van:** [redacted]
**Aan:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB; [redacted] BD/DRC/CV
**Cc:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow"s TOP Encryption
**Datum:** maandag 16 juli 2018 16:31:25
**Bijlagen:** image001.jpg

10.2.e

---

[redacted]

[redacted]

11.1
10.2.a

**From:** [redacted] BD/DAS/AS
**Sent:** maandag 16 juli 2018 16:20
**To:** [redacted] BD/DCS/ACSB ; [redacted] BD/DRC/CV
**Cc:** [redacted] BD/DAS/AS ; [redacted] BD/DCS/ACSB
**Subject:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

10.2.e

[redacted]

11.1
10.2.a

**From:** [redacted] BD/DCS/ACSB
**Sent:** maandag 16 juli 2018 16:02
**To:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DAS/AS
**Subject:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption
**Importance:** High

10.2.e

Ter info: net gecirculeerd nadere toelichting op wat men met encryptie wil doen. Als dit aanleiding is voor jullie om instructie uit te breiden/aan te scherpen: dit graag zsm doorgeven, ook aan [redacted] (in de cc) die bij de HWP aanwezig is.
Groet,

[redacted]

**Van:** [redacted] BD/DAS/AS
**Verzonden:** maandag 16 juli 2018 15:09
**Aan:** [redacted] @minbuza.nl; [redacted] @minbuza.nl; Berk MSc MA, T. van den - BD/DCS/ACSB; [redacted] BD/DCS/ACSB
**CC:** [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted] 11.1 10.2.a

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** [redacted] @minbuza.nl>
**Datum:** maandag 16 jul. 2018 12:25 PM
**Aan:** [redacted] @minbuza.nl <[redacted] @minbuza.nl>, [redacted] BD/DAS/AS <[redacted] @nctv.minvenj.nl>, [redacted] BD/DCS/ACSB <[redacted] @nctv.minvenj.nl>, [redacted] BD/DCS/ACSB <[redacted] @nctv.minvenj.nl>
**Kopie:** [redacted] @minbuza.nl>, [redacted] BD/DRC/CV <[redacted] @minvenj.nl>
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption
Ha [redacted]
Dank voor je bericht. Ik deel je advies, wat mij betreft zouden we dit aan de instructie kunnen toevoegen.
Groet,
[redacted]

---

**From:** [redacted]
**Sent:** maandag 16 juli 2018 11:26
**To:** [redacted] @minbuza.nl>; [redacted] - BD/DAS/AS <[redacted] @nctv.minvenj.nl>; [redacted] @nctv.minvenj.nl; [redacted] BD/NCTV/DCS/ACSB ([redacted] @nctv.minvenj.nl)' <[redacted] @nctv.minvenj.nl>
**Cc:** [redacted] @minbuza.nl>
**Subject:** FW: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted] 11.1 10.2.a

[redacted]

**From:** [redacted]

**Sent:** maandag 16 juli 2018 11:17

**To:** [redacted]

**Cc:** [redacted]

**Subject:** HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

10.2.a

**Von:** [redacted]

**Gesendet:** Freitag, 13. Juli 2018 11:47

**An:** [redacted]

10.2.a; 10.2.e

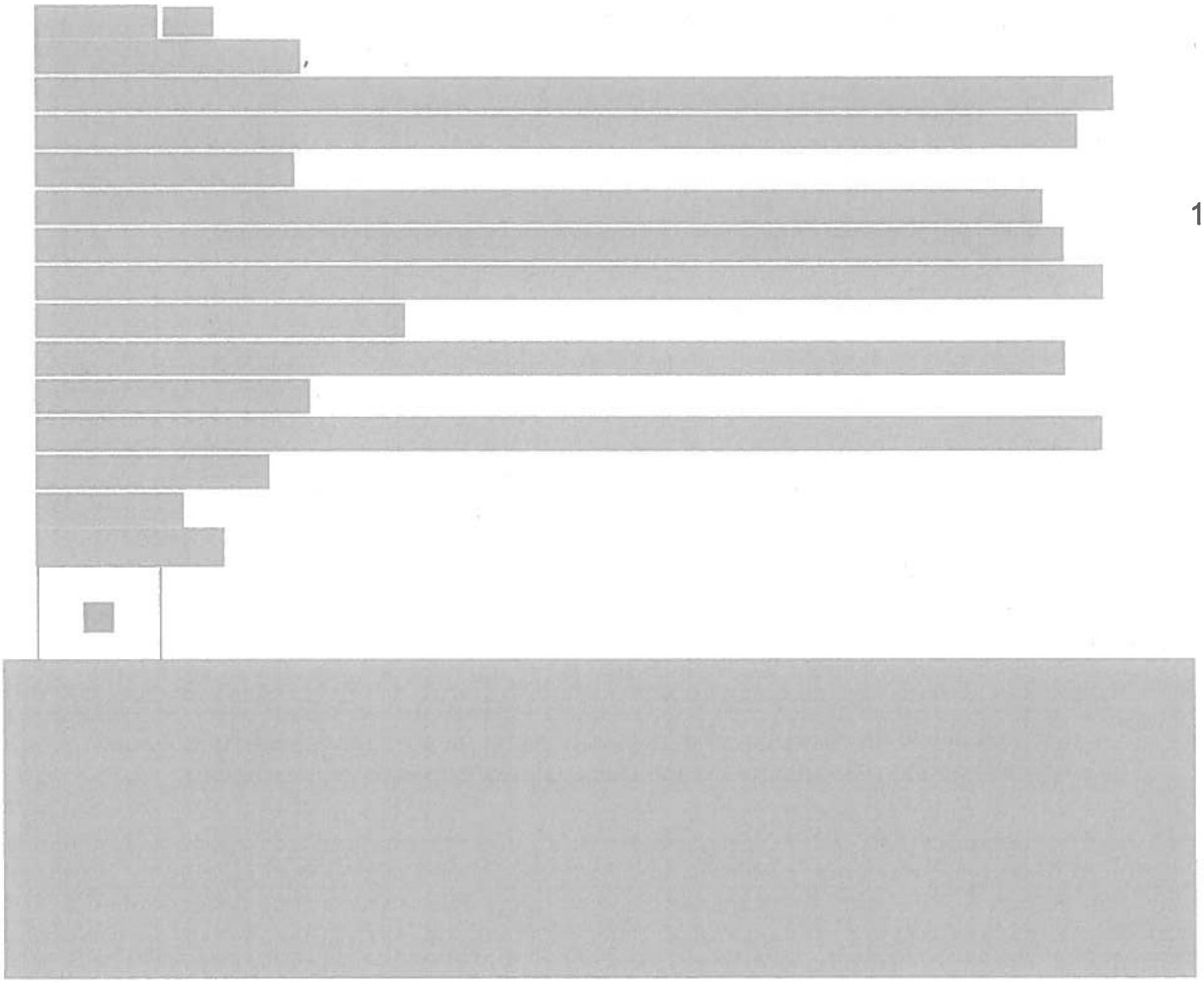
[redacted]

**Cc:** [redacted]

**Betreff:** HWP on Cyber Issues on 17 July 2018: Encryption and [redacted]

[redacted]

10.2.a



Help save paper! Do you really need to print this email?



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

[redacted]

[redacted]

[redacted]
en.
Passief kan worden opgenomen, als de nut en noodzaak in twijfel wordt getrokken.

## 7. The role of encryption in criminal investigations

[redacted] 10.2.a

Instructie: DGRR, NCTV
*Spreekpunten Algemeen*

- In general, NL considers that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the EU.
- There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that use encryption.
- NL wants to focus on advancing discussions on the issue of encryption on the basis of the conclusions of the JHA Council of December 2017, within the current legal framework.
- Recently, new legislation on combating cybercrime has been adopted in NL. This legislation sets strong safeguards for the use of intrusive investigative measures such as accessing automated networks. On the basis of this new legislation, NL will be able to use certain tools that address end-to-end encryption by the end of this year. However, as mentioned, only under very strict conditions.
- Even though NL acknowledges the importance of using information from lawful intercept in criminal investigations, NL is very reluctant as regards providing the mentioned tool to Europol. There are significant differences between the legal systems of the Member States as regards the use of such tools.
- Furthermore, NL is not in favour of encouraging the market ~~to use~~ of so-called 'zero days' which are often used by certain tools. (gebruik van dergelijke tools die wellicht van zero days gebruik maken kan wel, maar onder zeer strikte voorwaarden. Tools waarvan we zeker weten dat ze geen zero days gebruiken, zijn minder politiek gevoelig, maar de fabrikant van de tool zal doorgaans niet willen zeggen of de tool van zero days gebruik maakt. )
- This issue was the most pressing element in the parliamentary debate on the recently adopted NL legislation. As a result of the political process, NL does not only have very strict conditions for the use, but also for the acquisition of tools that may use zero day exploits.
- NL would be open to further discussing this matter, but considers that more information and background is needed as regards providing a decryption capability to Europol. [redacted] 11.1

- [redacted] 10.2.a
- Lastly, NL supports [redacted] that further discussions should be scheduled in COSI. Similar to [redacted] NL is *not in favour of scheduling a discussion on encryption at the JHA Council of October.*

**8. Post-quantum cryptography**

- Presentation by [redacted] on the H2020 project PQCRYPTO
- Exchange of views

10.2.a

Instructie: aanhoren

**9. AOB**

Instructie: aanhoren

**Van:** [redacted] BD/DCS/ACSB
**Aan:** [redacted] BD/DAS/AS
**Cc:** [redacted] BD/DAS/AS
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow"s TOP Encryption
**Datum:** dinsdag 17 juli 2018 08:21:05
**Bijlagen:** image001.jpg

10.2.e

[redacted]

11.1

**Van:** [redacted]
**Verzonden:** maandag 16 juli 2018 19:54
**Aan:** [redacted] BD/DRC/CV; [redacted] BD/DCS/ACSB; [redacted] BD/DAS/ [redacted] Planken, drs. E.J.H. - BD/DRC/CV; [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

11.1

[redacted]

**From:** [redacted] BD/DRC/CV
**Sent:** maandag 16 juli 2018 18:56:18
**To:** [redacted] BD/DCS/ACSB; [redacted] BD/DAS/AS; [redacted] BD/DAS/AS
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DRC/CV
**Subject:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

11.1

**Van:** [redacted]
**Verzonden:** maandag 16 juli 2018 18:11
**Aan:** [redacted] BD/DCS/ACSB; [redacted] BD/DRC/CV; [redacted] BD/DAS/AS; [redacted] BD/DAS/AS
**CC:** [redacted] BD/DRC/CV; [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

[redacted]

11.1

JHA Council of October.

**From:** [redacted] BD/DCS/ACSB
**Sent:** maandag 16 juli 2018 17:16
**To:** [redacted] BD/DRC/CV ; [redacted] BD/DAS/AS ; [redacted] BD/DAS/AS
**Cc:** [redacted] BD/DRC/CV ; [redacted] BD/DRC/CV
**Subject:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption
**Importance:** High

[redacted]

11.1
10.2.a

[redacted]

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 16 juli 2018 16:53
**Aan:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB; [redacted] BD/DAS/AS
**CC:** [redacted] BD/DRC/CV; [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

11.1

**Van:** [redacted] /DAS/AS
**Verzonden:** maandag 16 juli 2018 16:20
**Aan:** [redacted] BD/DCS/ACSB; [redacted] BD/DRC/CV
**CC:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

[redacted]

**From:** [redacted] BD/DCS/ACSB
**Sent:** maandag 16 juli 2018 16:02
**To:** [redacted] BD/DAS/AS; [redacted] BD/DCS/ACSB
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DAS/AS
**Subject:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption
**Importance:** High

Ter info: net gecirculeerd nadere toelichting op wat men met encryptie wil doen. Ale dit aanleiding is voor jullie om instructie uit te breiden/aan te scherpen: dit graag zsm doorgeven, ook aan [redacted] die bij de HWP aanwezig is. 10.2.e
Groet,
[redacted]

**Van:** [redacted] BD/DAS/AS
**Verzonden:** maandag 16 juli 2018 15:09
**Aan:** [redacted] BD/DCS/ACSB; [redacted] BD/DCS/ACSB
**CC:** [redacted] BD/DRC/CV
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** [redacted]
**Datum:** maandag 16 jul. 2018 12:25 PM
**Aan:** [redacted] BD/DAS/AS <[redacted]@nctv.minvenj.nl>, [redacted] BD/DCS/ACSB <[redacted]@nctv.minvenj.nl>, [redacted] BD/DCS/ACSB <[redacted]@nctv.minvenj.nl>
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minvenj.nl>
**Onderwerp:** RE: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

11.1

[redacted]

**From:** [redacted]
**Sent:** maandag 16 juli 2018 11:26
**To:** [redacted] BD/DAS/AS <[redacted]@nctv.minvenj.nl>; [redacted]@nctv.minvenj.nl; [redacted] BD/NCTV/DCS/ACSB ([redacted]@nctv.minvenj.nl)' <[redacted]@nctv.minvenj.nl>
**Cc:** [redacted]
**Subject:** FW: HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted]

**From:** [redacted]

**Sent:** maandag 16 juli 2018 11:17
**To:** [redacted]

**Cc:** [redacted]

**Subject:** HWP on Cyber Issues on 17 July 2018 / Regarding tomorrow's TOP Encryption

[redacted] 10.2.a

**Von:** [redacted]
**Gesendet:** Freitag, 13. Juli 2018 11:47

[redacted]

**Cc:** [redacted]
**Betreff:** HWP on Cyber Issues on 17 July 2018: Encryption and [redacted]
**Wichtigkeit:** Hoch

[redacted]

---



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

---

Help save paper! Do you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the

addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/KS
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/NCSC/SK; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PACT
**Onderwerp:** RE: OTT (en 5G) dilemma paper
**Datum:** dinsdag 12 maart 2019 14:54:00
**Bijlagen:** Dilemma paper OTT en interceptie_tvdb.docx

10.2.e

[redacted]

11.1

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 maart 2019 9:55
**Aan:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PNDV
**Onderwerp:** FW: OTT (en 5G) dilemma paper

10.2.e

[redacted]

Moet ik jullie even aanhaken op dit stuk tbv crypto [redacted]

ben jij nog crypto aanspreekpunt?

11.1

[redacted]

**Van:** [redacted] BD/DRC/FO <[redacted]@minvenj.nl>
**Datum:** woensdag 06 mrt. 2019 9:40 AM
**Aan:** [redacted] @klpd-uli.nl>, [redacted] @politie.nl)' [redacted] @politie.nl>, [redacted] @om.nl' [redacted] @om.nl>, [redacted] (Landelijk Parket)' <[redacted] @om.nl>, [redacted] BD/DGPenV/PPBT/PBO <[redacted] @minvenj.nl>, [redacted] @mindef.nl' [redacted] @mindef.nl>, [redacted] BD/DRC/CV <[redacted] @minvenj.nl>, [redacted] )' [redacted] @minez.nl>, [redacted] BD/KS <[redacted] @nctv.minvenj.nl>, [redacted] BD/PIDS <[redacted] @minvenj.nl>, [redacted] BD/DRC/CV <[redacted] @minvenj.nl>, [redacted] BD/DRC/CV <[redacted] @minvenj.nl>

10.2.e

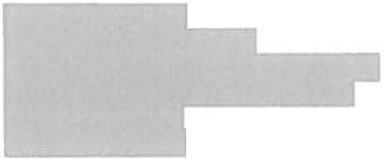
**Onderwerp:** OTT (en 5G) dilemma paper

Dag allen,
Het heeft wat langer geduurd dan ik had gehoopt, maar bijgesloten vinden jullie een concept van de dilemma paper OTT en opsporing die we hebben besproken op 24 oktober (of bilateraal naderhand). Ook het 5G vraagstuk dat op onderdelen dezelfde

dilemma's kent heb ik daarin meegenomen.
Mijn voorstel in het paper is om op korte termijn onze bestuurders over de daarin geformuleerde dilemma's en mogelijke stappen om het vraagstuk verder te brengen van gedachten te laten wisselen. Hierbij wil ik jullie vragen of de paper en daarin voorgestelde stappen te bekijken en eventueel van commentaar te voorzien. Van enkelen van jullie heb ik dat al gekregen. Daarna leg ik het hier aan de DG en mijn MT voor.
Ik wil jullie vragen om, als dat kan, uiterlijk volgende week woensdag hierop te reageren.
Veel dank.
Groet

Coördinerend beleidsadviseur
.....
**Ministerie van Veiligheid en Justitie**
**DGRR-DRC-Afdeling Fraude en Ordening**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

10.2.e



**Van:** [redacted] BD/NCSC/SK
**Aan:** [redacted] - BD/PNDV
**Onderwerp:** RE: OTT (en 5G) dilemma paper
**Datum:** dinsdag 19 maart 2019 13:12:14

10.2.e

Hoi [redacted],

[redacted]

11.1

Hartelijke groeten,

[redacted]

**Van:** [redacted] BD/PNDV
**Verzonden:** dinsdag 12 maart 2019 14:55
**Aan:** [redacted] BD/KS
**CC:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/NCSC/SK; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PACT
**Onderwerp:** RE: OTT (en 5G) dilemma paper

[redacted]

11.1

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 maart 2019 9:55
**Aan:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PACT; [redacted] BD/PNDV
**Onderwerp:** FW: OTT (en 5G) dilemma paper

10.2.e

Hoi [redacted],

Moet ik jullie even aanhaken op dit stuk tbv crypto [redacted]

, ben jij nog crypto aanspreekpunt?

[redacted]

11.1

Gr

[redacted]

**Van:** [redacted] BD/DRC/FO <[redacted]@minvenj.nl>
**Datum:** woensdag 06 mrt. 2019 9:40 AM
**Aan:** [redacted]
BD/DGPenV/PPBT/PBO <[redacted]@minvenj.nl>,
BD/DRC/CV <[redacted]@minvenj.nl>, [redacted] 10.2.e
BD/KS <[redacted]@nctv.minvenj.nl>, BD/PIDS <[redacted]@minvenj.nl>,
[redacted] BD/DRC/CV <[redacted]@minvenj.nl>, [redacted] BD/DRC/CV
<[redacted]@minvenj.nl>
**Onderwerp:** OTT (en 5G) dilemma paper

Dag allen,
Het heeft wat langer geduurd dan ik had gehoopt, maar bijgesloten vinden jullie een concept van de dilemma paper OTT en opsporing die we hebben besproken op 24 oktober (of bilateraal naderhand). Ook het 5G vraagstuk dat op onderdelen dezelfde dilemma's kent heb ik daarin meegenomen.
Mijn voorstel in het paper is om op korte termijn onze bestuurders over de daarin geformuleerde dilemma's en mogelijke stappen om het vraagstuk verder te brengen van gedachten te laten wisselen. Hierbij wil ik jullie vragen of de paper en daarin voorgestelde stappen te bekijken en eventueel van commentaar te voorzien. Van enkelen van jullie heb ik dat al gekregen. Daarna leg ik het hier aan de DG en mijn MT voor.
Ik wil jullie vragen om, als dat kan, uiterlijk volgende week woensdag hierop te reageren.
Veel dank.
Groet

[redacted]
Coördinerend beleidsadviseur
.....
**Ministerie van Veiligheid en Justitie**
**DGRR-DRC-Afdeling Fraude en Ordening**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

**T** 06 – [redacted]
[redacted]@minvenj.nl
Secretariaat - [redacted] 10.2.e
**@** [redacted]@minvenj.nl
**T** 06 - [redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/DRC/FO
**Onderwerp:** RE: OTT (en 5G) dilemma paper
**Datum:** maandag 25 maart 2019 14:00:21
**Bijlagen:** Dilemma paper OTT en interceptie comments NCTV.docx

10.2.e

[redacted]

11.1

**From:** [redacted] BD/DRC/FO
**Sent:** maandag 25 maart 2019 13:21
**To:** [redacted] BD/KS
**Subject:** RE: OTT (en 5G) dilemma paper

Hi,
Lukt het je om vandaag de opmerkingen aan te leveren? Ik wil de memo vandaag de lijn in doen.
Thanks.
Groet
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** dinsdag 19 maart 2019 14:34
**Aan:** [redacted] BD/PSD; [redacted] BD/DRC/FO
**Onderwerp:** RE: OTT (en 5G) dilemma paper

[redacted]

11.1

[redacted]

**Van:** [redacted] BD/PSD <[redacted]@nctv.minvenj.nl>
**Datum:** dinsdag 19 mrt. 2019 2:29 PM
**Aan:** [redacted] BD/DRC/FO <[redacted]@minvenj.nl>
**Kopie:** [redacted] BD/PSD <[redacted]@nctv.minvenj.nl>, [redacted] BD/PSD <[redacted]@nctv.minvenj.nl>, [redacted] BD/KS <[redacted]@nctv.minvenj.nl>
**Onderwerp:** RE: OTT (en 5G) dilemma paper

[redacted]

[redacted] 11.1

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 maart 2019 9:49
**Aan:** [redacted] BD/DRC/FO
**CC:** [redacted] BD/PSD; [redacted] BD/PSD; [redacted] BD/PSD
**Onderwerp:** FW: OTT (en 5G) dilemma paper

[redacted] 11.1

**Van:** [redacted] BD/DRC/FO <[redacted]@minvenj.nl>
**Datum:** woensdag 06 mrt. 2019 9:40 AM
**Aan:** [redacted]@klpd-uli.nl>, [redacted]@politie.nl) [redacted]@politie.nl>, [redacted]@om.nl' [redacted]@om.nl>, [redacted] (Landelijk Parket)' [redacted]@om.nl>, [redacted] BD/DGPenV/PPBT/PBO [redacted]@minvenj.nl>, [redacted]@mindef.nl' [redacted]@mindef.nl>, [redacted] BD/DRC/CV <[redacted]@minvenj.nl>, [redacted]@minez.nl>, BD/KS <[redacted]@nctv.minvenj.nl>, [redacted] BD/PIDS <[redacted]@minvenj.nl>, [redacted] BD/DRC/CV <[redacted]@minvenj.nl>, [redacted] BD/DRC/CV <[redacted]@minvenj.nl>
**Onderwerp:** OTT (en 5G) dilemma paper

Dag allen,
Het heeft wat langer geduurd dan ik had gehoopt, maar bijgesloten vinden jullie een concept van de dilemma paper OTT en opsporing die we hebben besproken op 24 oktober (of bilateraal naderhand). Ook het 5G vraagstuk dat op onderdelen dezelfde dilemma's kent heb ik daarin meegenomen.
Mijn voorstel in het paper is om op korte termijn onze bestuurders over de daarin geformuleerde dilemma's en mogelijke stappen om het vraagstuk verder te brengen van gedachten te laten wisselen. Hierbij wil ik jullie vragen of de paper en daarin voorgestelde stappen te bekijken en eventueel van commentaar te voorzien. Van enkelen van jullie heb ik dat al gekregen. Daarna leg ik het hier aan de DG en mijn MT

voor.
Ik wil jullie vragen om, als dat kan, uiterlijk volgende week woensdag hierop te reageren.
Veel dank.
Groet

Coördinerend beleidsadviseur
.....
**Ministerie van Veiligheid en Justitie**
**DGRR-DRC-Afdeling Fraude en Ordening**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

**T**
r@minvenj.nl
Secretariaat -
@minvenj.nl
**T**

10.2.e

20190516

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/PNDV
**Onderwerp:** RE: OTT en intercetpie bijeenkomst maandag
**Datum:** donderdag 16 mei 2019 16:17:07
**Bijlagen:** image001.png

10.2.e

[redacted]

11.1

**From:** [redacted] BD/PNDV
**Sent:** dinsdag 14 mei 2019 17:29
**To:** [redacted] BD/KS
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Subject:** RE: OTT en intercetpie bijeenkomst maandag

10.2.e

[redacted]

11.1

[redacted] 11.1

[redacted]

[redacted]
Coördinerend beleidsmedewerker

.....
**Ministerie van Justitie en Veiligheid**
**PNDV**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag

10.2.e

.....
[redacted] nctv.minjenv.nl
www.nctv.nl
.....
**Voor een rechtvaardige en veilige samenleving**
.....
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** maandag 13 mei 2019 17:59
**Aan:** [redacted] BD/PNDV; [redacted] BD/PACT; [redacted] BD/PNDV; [redacted] BD/PPAC; [redacted] BD/PSD; [redacted] BD/PACT; [redacted] BD/PLS; [redacted] BD/PSD; [redacted] BD/KS; [redacted] - BD/PNDV
**Onderwerp:** FW: OTT en intercetpie bijeenkomst maandag

10.2.e

[redacted] 11.1

[redacted]

10.2.e

[redacted] BD/DRC/FO <[redacted]@minjenv.nl>
**Datum:** donderdag 09 mei 2019 4:34 PM

**Aan:** [redacted] BD/PIDS < [redacted] @minjenv.nl>, [redacted] BD/KS < [redacted] @nctv.minvenj.nl>, [redacted] BD/DRC/CV < [redacted] @minjenv.nl>, [redacted] BD/DRC/CV < [redacted] @minjenv.nl>, [redacted] BD/PIDS < [redacted] @minjenv.nl>, [redacted] (PaG Den Haag)' [redacted] @om.nl>, [redacted] @om.nl>, [redacted] @politie.nl>, [redacted] - BD/DRC/CV < [redacted] @minjenv.nl>, [redacted] @minbzk.nl>, [redacted] @mindef.nl' [redacted] @mindef.nl>, [redacted] [redacted] @minez.nl>, [redacted] - BD/DGPenV/PPM/EBF < [redacted] @minjenv.nl>, [redacted] BD/IBO [redacted] @ibo.justid.nl>, [redacted] (Landelijk Parket Rotterdam)' [redacted] @om.nl>

10.2.e

**Onderwerp:** OTT en intercetpie bijeenkomst maandag

Dag allen,

[redacted]

11.1

Tot maandag.

Groet,

[redacted]

.....

**Ministerie van Veiligheid en Justitie**
**DGRR-DRC-Afdeling Fraude en Ordening**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

.....

[redacted]

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/PNDV; [redacted] BD/KS
**Onderwerp:** RE: Points/Questions on encryption policy
**Datum:** donderdag 26 september 2019 08:14:50
**Bijlagen:** image001.png
image002.jpg

10.2.e

[redacted]

[redacted]

10.2.a

[redacted]

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Datum:** donderdag 26 sep. 2019 08:07
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: Points/Questions on encryption policy

10.2.e

Goedemorgen beiden,

Het is helaas nog niet gelukt om een afspraak te houden. Nieuw voorstel volgt zsm. Verwacht komende maandag.

Gr. [redacted]

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Datum:** maandag 23 sep. 2019 6:23 PM
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Points/Questions on encryption policy

10.2.e

[redacted]

[redacted]

10.2.a

[redacted]

[redacted]

[redacted]

---

**Van:** [redacted]
**Datum:** vrijdag 20 sep. 2019 14:57
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl> 10.2.e
**Onderwerp:** Points/Questions on encryption policy

[redacted] 10.2.a

[redacted]

[redacted] 10.2.a; 10.2.e

[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PSD
**Onderwerp:** RE: Input annotatie [redacted]
**Datum:** vrijdag 4 oktober 2019 13:45:07
**Bijlagen:** Inbreng anno [redacted] NCTV bezoek oktober 2019.docx

10.2.e
10.2.a

Hierbij aanpassing, spreekpunten, essentie en toelichting zijn aangepast met bullits over [redacted]

**From:** [redacted] BD/KS
**Sent:** vrijdag 4 oktober 2019 13:33
**To:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PSD
**Subject:** RE: Input annotatie [redacted]

10.2.e

Wacht! Anno moet aangepast. Speelt in [redacted] Moet ik even specifiek aanpassen

10.2.a

**From:** [redacted] BD/KS
**Sent:** vrijdag 4 oktober 2019 10:35
**To:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PSD
**Subject:** RE: Input annotatie [redacted]

Julia,
As promised input op crypto. Het is vrij uitgebreid maar dat komt omdat Pieter Jaap hier [redacted] niet op is geinformeer.d

10.2.a

[redacted]

10.2.a
11.1
L

**From:** [redacted] BD/KS
**Sent:** woensdag 2 oktober 2019 15:06
**To:** [redacted] BD/PNDV; [redacted] BD/KS
**Cc:** [redacted] BD/PSD
**Subject:** RE: Input annotatie [redacted]

Ja ik lever wat op crypto aan.
ik zou ook bullit over [redacted] (beeld [redacted] van [redacted]). en
misschien evt ook [redacted] (Juist omdat we dat even highlighten met [redacted]
Met [redacted] enzo toch?
Kan ik vrijdag aanleveren?

10.2.a
L
11.1
10.2.a

[redacted]

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 02 okt. 2019 2:31 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted] BD/PSD <[redacted]@nctv.minjenv.nl>
**Onderwerp:** Input annotatie [redacted]

10.2.e
10.2.a

Hoi [redacted]
Heb je een goede week?
Heb je nog input voor de annotatie van PJA voor zijn bezoek naar [redacted]
Opzet zal lijken op [redacted] [redacted] sluit aan op anno tbv gesprek met cyberambassadeur. [redacted] levert de EU input.
Heb jij hier aanvullingen op?
Ontvang deze graag uiterlijk.
Gr. [redacted]

L
11.1
10.2.a

**Inbreng anno [redacted] NCTV bezoek oktober 2019**

- NL stresses that increased use of encryption is a positive development, nece[redacted] for protecting human rights, privacy, confidentiality of communication, to stimulate economic growth and innovation, and cybersecurity; 10.2.a
- at the same time, NL acknowledges that there is a need for competent authorities to be able to access encrypted information.
- Over the Tops-providers (OTT's) and telecom providers are not in the same level playing field as regards interception.
- How do you regard the problem for law enforcement (and intelligence)? And what do you think about options to regulate with regard to Internet Service Providers and Over the Top providers (OTT's[1]), in order to comply with requests for (decrypted) information? 10.2.a
- [redacted]
- NL finds that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption. However, we are currently reflecting on encryption at national and European level. And curious on your position with regard to interception and OTT's.

## 1. Essentie boodschap

**Prioriteiten inzake encryptie**

- Nationaal: binnen de marges van het kabinetsstandpunt encryptie van 2016 wordt bezien welke (technische en beleidsmatige) oplossingen mogelijk zijn t.b.v. doorbreken/omzeilen van encryptie voor rechtmatige doeleinden.
- [redacted] 11.1
- Internationaal: volgen van EU discussie, [redacted] 11.1
- [redacted] 10.2.a

## 2. Achtergrond

**NL kabinetsstandpunt**

- Vaak wordt de discussie over encryptie voorgesteld als een keus tussen veiligheid en privacy. Dat is echter een onjuiste vereenvoudiging van feiten. Cybersecurity (veiligheid in het digitale domein) is bijvoorbeeld gebaat bij encryptie; terwijl tegelijkertijd het zicht op communicatie van kwaadwillenden onder gebruik van encryptie te lijden heeft. Ook economische belangen spelen een rol, zoals level playing field tussen ouderwetse telecomproviders die onder hoofdstuk 13 Telecomwet vallen, en de OTT's die hier niet onder vallen (MinEZK).

[1] OTT's zijn diensten die 'over de top' van internet-infrastructuur zoals die door Internet Service Providers (ISP's) en telecomnetwerken geleverd worden, aangeboden worden zoals Skype, Telegram, Whatsapp, Facebook etc.

- "Het Kabinet onderschrijft in het kabinetsstandpunt van 4 januari 2016 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 kabinet heeft daarnaast tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen en onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Het kabinet is 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."
- "Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptieproducten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Het kabinet vindt van belang dat bevoegde autoriteiten op rechtmatige wijze bij versleutelde informatie kunnen. Daarom vindt binnen de afzonderlijke diensten, maar ook in interdisciplinair overleg onderling, onderzoek plaats naar de mogelijkheden voor overheidsdiensten om in dat verband bij versleutelde informatie te kunnen komen om georganiseerde criminaliteit het hoofd te bieden en de nationale veiligheid te waarborgen. Het doel is om de beleidsmatige en operationele mogelijkheden te bezien, en mogelijkheden te benutten van kruisbestuiving, bijvoorbeeld in relatie tot contact met digitale dienstverleners. Uiteraard blijven de verschillende diensten verantwoordelijk voor de uitoefening van hun eigen taken en bevoegdheden, zoals die hun in wetgeving zijn toegekend."
- Het kabinetsstandpunt is op 4 januari 2016 geformuleerd door de volgende partners: V&J NCTV, DGRR, NCSC/ BZK CZW (grondrechten) en AIVD/ BZ/ DEF MIVD/ EZ.
- [redacted] 10.2.a
- De Minister van JenV zal op 4 oktober reageren (NOS) dat we ons bewust zijn van de risico's van versleuteling voor opsporing en vervolging.

**Van:** [redacted] - BD/KS
**Aan:** [redacted] - BD/PNDV; [redacted] BD/PNDV; [redacted] - BD/PACT; [redacted] - BD/PACT; [redacted] - BD/NCTV; [redacted] - BD/NCTV
**Cc:** [redacted] BD/KS; [redacted] W. - BD/KS; [redacted] - BD/KS; [redacted] - BD/KS; [redacted] - BD/KBV; [redacted] - BD/KS; [redacted] - BD/PNDV 10.2.e
**Onderwerp:** Terugkoppeling presentatie OTT aan MinJenV (encryptie)
**Datum:** vrijdag 4 oktober 2019 11:29:05
**Bijlagen:** Inbreng anno [redacted] NCTV bezoek oktober 2019.docx 10.2.A

Beste collega's,
Afgelopen woensdag zat ik met DGRR ([redacted]) bij MJenV t.b.v. een presentatie over de Over The Top diensten (OTT: Signal, telegram, whatsapp etc). In het bijzonder: het dilemma voor opsporing (en inlichtingen) dat zij geen toegang meer kunnen krijgen tot versleutelde communicatie vanwege de wijdverspreide end-to-end encryptie, en het ontbreken van wetgeving over interceptie die van toepassing is op OTTs. De Telecomwet (hoofdstuk 13 interceptie) is wel van toepassing op ISPs, maar niet van toepassing op OTTs.

**Sonderen**

Minister is gewezen op de risicos van het openbreken van het encryptiestandpunt van 2016; dat wetende is hij akkoord met het inventariseren van een Europese oplossing voor het interceptievraagstuk v.w.b. OTT diensten. Dit inventariseren gaat gebeuren met bepaalde EU partners en hij heeft graag dat we dit snel afronden. Hij vroeg nadrukkelijk waarom we dit niet eerst nationaal gingen regelen m.h.o.o. de snelheid; daar hebben we beiden negatief op geadviseerd gezien beperkte effectiviteit en handhaafbaarheid (Skype zaak Belgie; OTTs vaak in buitenland gevestigd). Minister is zich bewust van de waardenspanning. De minister heeft geen akkoord gegeven op het direct inzetten op Europese regelgeving hierop, maar ingestemd met het Europees sonderen hiervan. Zaak is om het klein en vertrouwelijk te houden.
Voorkeur heeft een Europese Regeling ivm handhaafbaarheid van een bevel/concurrentie positie NL bedrijven en level playing field tussen telco's en OTT's.
Luistert erg nauw, raakt aan encryptiestandpunt en we willen geen E-evidence voorstel voor tappen.
DGRR zal via hun beleidscollega's informeel gaan inventariseren hoe zij tegen een mogelijke Europese regeling hiervoor aankijken [redacted] Voor het bezoek van Pieter Jaap aan [redacted] is bijgaande anno terzake opgemaakt. 10.2.a

**Tweede kamer**

[redacted] 11.1

Groet,
[redacted] 10.2

**Van:** [redacted] BD/PSD
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: [redacted] dossier pieter jaap
**Datum:** maandag 7 oktober 2019 09:59:50

10.2.e

10.2.A

Joe, neem ik mee!

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** maandag 07 okt. 2019 6:23 PM
**Aan:** [redacted] BD/PSD <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: [redacted] dossier pieter jaap

10.2.A

Ha [redacted] zie onder svp relevante vraag voor in t dossier over encryptie. Kun jij due svp meenemen? En vooral ern contact achterhalen als we niet direct antwoord krijgen?

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** vrijdag 04 okt. 2019 5:51 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted] BD/PIDS <[redacted]@minjenv.nl>
**Onderwerp:** RE: [redacted] dossier pieter jaap

10.2.A

Ha [redacted]
Heb jij toevallig een counterpart in [redacted] met wie je het werkbezoek voorbereidt?

[redacted]

11.1

[redacted]

[redacted]

10.2.a

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] 10.2.a

[redacted] BD/KS
**Verzonden:** vrijdag 4 oktober 2019 13:53
**Aan:** [redacted] BD/DRC/CV
**Onderwerp:** RE: [redacted] dossier pieter jaap 10.2.A
Held, thanks!

**From:** [redacted] BD/DRC/CV
**Sent:** vrijdag 4 oktober 2019 13:14
**To:** [redacted] BD/KS
**Subject:** RE: [redacted] dossier pieter jaap

[redacted] 10.2.A; 11.1

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** vrijdag 4 oktober 2019 11:47
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Onderwerp:** RE: [redacted] dossier pieter jaap 10.2.A
Ja, [redacted] ☺

**From:** [redacted] BD/DRC/CV
**Sent:** vrijdag 4 oktober 2019 11:45
**To:** [redacted] BD/KS
**Subject:** RE: [redacted] dossier pieter jaap 10.2.A
Ha [redacted],
Dit is [redacted] neem ik aan toch? Niet [redacted]
In het geval van [redacted] verwerk ik nog even wat achtergrond over wat [redacted] tot nu toe heeft gedaan.

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** vrijdag 4 oktober 2019 10:38

**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>

**Onderwerp:** [redacted] dossier pieter jaap

[redacted] klopt ie zo?

Moest anno aanleveren omdat Pieter Jaap komende week naar [redacted] gaat. feel free to use for own missions.

Aanpassingen ontvang ik ook graag!

10.2.A

[redacted]

10.2.e

**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
Afdeling Strategie
Postbus 16950 | 2500 BZ | Den Haag

[redacted]
[redacted]@nctv.minjenv.nl
www.nctv.nl

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'
**Datum:** zaterdag 12 oktober 2019 20:30:53

10.2.e

Dank, sorry ik heb niet gereageerd zie ik.. Ik heb de annotatie opgenomen onder WVTTK.
Groet!
[redacted]

10.2.e

.....
**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
**Kerneenheid Strategie**
Turfmarkt 147| 2511 DP | Den Haag |
Postbus 16950 | 2500 BZ | Den Haag
.....
**T** 06 [redacted]

[redacted]@nctv.minjenv.nl
www.nctv.nl
.....
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** vrijdag 11 oktober 2019 12:47
**Aan:** [redacted] BD/KS; [redacted] BD/PNDV
**CC:** [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/PACT
**Onderwerp:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'
**Urgentie:** Hoog

10.2.e

[redacted] anno voor Patricia:

**Encryptie en Verhoeven (passief/ en marge – DGRR tracht nog een vooroverleg te organiseren)**

[redacted] 30 oktober is het AO Cybersecurity.

11.1

- Minister heeft vorige week groen licht gegeven aan DGRR om bij likeminded te gaan sonderen hoe zij met end-to-end encryptie in relatie tot opsporing willen omgaan (in het bijzonder: verkennen van Europese regelgeving die OTT's gelijkstelt aan telecomproviders en daarmee een interceptie-plicht oplegt). Een plicht om informatie ontsleuteld aan te leveren kan betekenen dat end-to-end-encryptie niet langer mogelijk is (volgens algemeen begrip van de term).
- In het kabinetsstandpunt is er sprake van dat NL het standpunt ook internationaal uitdraagt.
- Evt. aanpassing van het kabinetsstandpunt vergt nadrukkelijk afstemming binnen het kabinet (i.h.b. EZK, BZK en BZ).
- Mogelijke woordvoering indien noodzakelijk:

[redacted]

11.1

[redacted]

**From:** [redacted] BD/KS
**Sent:** woensdag 9 oktober 2019 16:56
**To:** [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/PACT 10.2.e
**Cc:** [redacted] BD/KS
**Subject:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'
**Importance:** High

Is er Staf met Min volg week?

[redacted] 11.1

**From:** [redacted] BD/DRC/CV
**Sent:** woensdag 9 oktober 2019 16:37
**To:** [redacted] BD/DBAenV/IenK; [redacted] BD/DRC/CV; [redacted] BD/KS
**Subject:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Faceb 10.2.e

TI, nog niet gelezen.

**Van:** [redacted] @minjenv.nl
**Verzonden:** woensdag 9 oktober 2019 16:11
**Aan:** [redacted] BD/CSR ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/KS ; [redacted] BD/PACT ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGPenV/Staf ; [redacted] BD/DGPenV/PPM/PP ; [redacted] BD/DGM/DRM/B&S ; [redacted] , [redacted] - BD/PSD ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGM/DMB/LVV ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGRR/STAF ; [redacted] BD/DJOA/JBOZ ; [redacted] BD/DGM/DRM ; [redacted] BD/KS ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DGPenV/PPBT/DG Staf ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DGM/DRM/B&S ; [redacted] BD/STAF_DGSenB ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DVB/IV ; [redacted] BD/DGM/DRM/B&S ; [redacted] BD/KS 10.2.e
**CC:** [redacted] ; [redacted] DC/PIV ; [redacted] ; [redacted]
**Onderwerp:** Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

Geachte mevrouw/heer,

Er is een nieuwe kamervraag aangemaakt op uw directie inzake "het bericht 'Minister bezorgd om versleuteling Facebook'".

Wilt u svp een directie/medewerker koppelen aan dit stuk?

link naar detailrapport of zoek op ID-nummer 102076

Voor vragen kunt u een mail sturen naar [redacted] @minjenv.nl of bellen naar tst. [redacted]

Met dank & vriendelijke groet,

[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/DRC/CV
**Onderwerp:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'
**Datum:** maandag 14 oktober 2019 19:47:14
**Bijlagen:** DetailRapport.docx
Encryptie mondelinge vraag Verhoeven .msg
**Prioriteit:** Hoog

10.2.e

[redacted], dit was mijn passieve anno voor onze staf, feel free to use, geen commentaar mijnerzijds op jouw anno.
Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** vrijdag 11 okt. 2019 12:49 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

[redacted] anno voor Patricia:
**Encryptie en Verhoeven (passief/ en marge – DGRR tracht nog een vooroverleg te organiseren)**

- [redacted]. Op 30 oktober is het AO Cybersecurity.
- Minister heeft vorige week groen licht gegeven aan DGRR om bij likeminded te gaan sonderen hoe zij met end-to-end encryptie in relatie tot opsporing willen omgaan (in het bijzonder: verkennen van Europese regelgeving die OTT's gelijkstelt aan telecomproviders en daarmee een interceptie-plicht oplegt). Een plicht om informatie ontsleuteld aan te leveren kan betekenen dat end-to-end-encryptie niet langer mogelijk is (volgens algemeen begrip van de term).
- In het kabinetsstandpunt is er sprake van dat NL het standpunt ook internationaal uitdraagt.
- Evt. aanpassing van het kabinetsstandpunt vergt nadrukkelijk afstemming binnen het kabinet (i.h.b. EZK, BZK en BZ).
- Mogelijke woordvoering indien noodzakelijk:
  - [redacted]

11.1

[redacted]

**From:** [redacted] BD/KS
**Sent:** woensdag 9 oktober 2019 16:56
**To:** [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/PACT
**Cc:** [redacted] BD/KS
**Subject:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'
**Importance:** High

Is er Staf met Min volg week?

[redacted]

11.1

**From:** [redacted] BD/DRC/CV
**Sent:** woensdag 9 oktober 2019 16:37
**To:** [redacted] BD/DBAenV/IenK; [redacted] BD/DRC/CV; [redacted]
- BD/KS
**Subject:** FW: Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

TI, nog niet gelezen.

**Van:** [redacted]@minjenv.nl
**Verzonden:** woensdag 9 oktober 2019 16:11
**Aan:** [redacted] BD/CSR ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/KS ; [redacted] BD/PACT ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGPenV/Staf ; [redacted] BD/DGPenV/PPM/PP ; [redacted] BD/DGM/DRM/B&S ; [redacted] BD/PSD ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGM/DMB/LVV ; [redacted] BD/DJOA/AJO ; [redacted] BD/DGRR/STAF ; [redacted] BD/DJOA/JBOZ ; [redacted] BD/DGM/DRM ; [redacted] BD/KS ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DGPenV/PPBT/DG Staf ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DGM/DRM/B&S ; [redacted] BD/STAF_DGSenB ; [redacted] BD/DGM/DMB/JAZ ; [redacted] BD/DVB/IV ; [redacted] BD/DGM/DRM/B&S ; [redacted] BD/KS
**CC:** [redacted]
**Onderwerp:** Nieuwe Kamervraag inzake het bericht 'Minister bezorgd om versleuteling Facebook'

Geachte mevrouw/heer,

Er is een nieuwe kamervraag aangemaakt op uw directie inzake "het bericht 'Minister bezorgd om versleuteling Facebook'".

Wilt u svp een directie/medewerker koppelen aan dit stuk?

[redacted]

Voor vragen kunt u een mail sturen naar [redacted]@minjenv.nl of bellen naar tst. [redacted]

Met dank & vriendelijke groet,

[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/PNDV; [redacted] BD/PACT; [redacted] BD/KA; [redacted] BD/NCSC/SR; [redacted] BD/PACT
**Onderwerp:** FW: Non paper interception OTT
**Datum:** woensdag 23 oktober 2019 08:04:43
**Bijlagen:** non paper interception OTT.docx

10.2.e

ter info en reactie.

[redacted]

11.1

[redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 21 okt. 2019 10:49 PM
**Aan:** [redacted] BD/PIDS <[redacted]@minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted]
**Onderwerp:** Non paper interception OTT

10.2.e

Hallo allemaal,
Zoals jullie weten heeft de minister het akkoord gegeven om bij enkele lidstaten te inventariseren of zij interesse hebben in Europese regelgeving rond het kunnen aftappen van OTT's.

11.1

In overleg met de internationale directie heb ik een non-paper gemaakt. Dit paper stelt haar in staat om te inventariseren bij een beperkte groep LS om te bezien of zij ook oren hebben naar een Europese regeling om OTT's af te tappen.
Een non-paper zou de probleemstelling, context en oplossingsrichting duidelijk moeten maken.
Ik heb dit geprobeerd in bijgevoegde non-paper, zouden jullie er eens naar willen kijken? Brengt dit paper de noodzaak duidelijk genoeg naar voren? Ik verspreid het paper bewust nog even onder de JenV organisaties, dus verspreid h'm svp niet.
Groeten,
[redacted]
Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
M 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/DRC/CV 10.2.e
**Onderwerp:** RE: Concept AO-dosier
**Datum:** woensdag 23 oktober 2019 17:32:53

---

Tnx [redacted], 10.2.e
Ja, al moet 1 QA anders (die was van Blok:

**Q:** Wat wordt de inzet van de MJenV richting zijn collega's in Washington?
**A:**

- Uiteraard zal ik het encryptiestandpunt internationaal uitdragen.
- [redacted] – 11.1
- dat betekent niet dat ik met mijn Amerikaanse collegas niet van gedachten kan wisselen hoe om te gaan met het dilemma van opsporing en zoeken naar oplossingen.

[redacted]
NCTV
[redacted] 10.2.e

---

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 23 okt. 2019 5:04 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Concept AO-dosier

Ha [redacted],
Heb jij meegelezen op de QA over encryptie?
Gr. [redacted]

---

**Van:** [redacted] BD/PNDV 10.2.e
**Verzonden:** dinsdag 22 oktober 2019 15:28
**Aan:** [redacted] BD/KS
**Onderwerp:** Concept AO-dosier
Ha [redacted],
Zie bijgaand:

- Inhoudsopgave
- Nota
- Convocatie
- Spreektekst
- QenA's

Groet,
[redacted]

**Van:** [redacted] BD/NCSC/SK
**Aan:** [redacted] BD/PNDV; [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/KA; [redacted] BD/PAC1 10.2.e
**Onderwerp:** RE: Non paper interception OTT
**Datum:** donderdag 24 oktober 2019 10:56:42

---

Hoi [redacted],
Bedankt voor het delen – [redacted] 11.1

[redacted] 11.1

Hartelijke groeten,
[redacted]

**Van:** [redacted] BD/PNDV
**Verzonden:** woensdag 23 oktober 2019 10:40
**Aan:** [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/KA; [redacted] BD/NCSC/SK; [redacted] BD/PACT
**Onderwerp:** RE: Non paper interception OTT

Hallo [redacted],

[redacted] 11.1

Groet,
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 23 oktober 2019 09:05
**Aan:** [redacted] BD/PNDV ; [redacted] BD/PACT ; [redacted] BD/KA ; [redacted] BD/NCSC/SK ; [redacted] BD/PACT
**Onderwerp:** FW: Non paper interception OTT

ter info en reactie.
Eerder informeerde ik jullie al dat de minister sterk neigt naar opties verkennen, waarbij een optie is : EU regelgeving [redacted] 11.1

[redacted]
NCTV
[redacted]

---

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 21 okt. 2019 10:49 PM
**Aan:** [redacted] (PaG Den Haag) ([redacted]@om.nl) <[redacted]@om.nl>, [redacted]@om.nl <[redacted]@om.nl>, [redacted]@politie.nl <[redacted]@politie.nl>, [redacted]. - BD/PIDS <[redacted]@minjenv.nl>, [redacted] - BD/KS <[redacted]@nctv.minjenv.nl> 10.2.e
**Kopie:** [redacted] (Parket-Generaal) [redacted]@om.nl)' [redacted]@om.nl) [redacted]@om.nl>, [redacted]@om.nl <[redacted]@om.nl>
**Onderwerp:** Non paper interception OTT

Hallo allemaal,
Zoals jullie weten heeft de minister het akkoord gegeven om bij enkele lidstaten te inventariseren of zij interesse hebben in Europese regelgeving rond het kunnen aftappen van OTT's.
In overleg met de internationale directie heb ik een non-paper gemaakt. Dit paper stelt haar in staat om te inventariseren bij een beperkte groep LS om te bezien of zij ook oren hebben naar een Europese regeling om OTT's af te tappen.
Een non-paper zou de probleemstelling, context en oplossingsrichting duidelijk moeten maken.
Ik heb dit geprobeerd in bijgevoegde non-paper, zouden jullie er eens naar willen kijken? Brengt dit paper de noodzaak duidelijk genoeg naar voren? Ik verspreid het

paper bewust nog even onder de JenV organisaties, dus verspreid h'm svp niet.
Groeten,

Met vriendelijke groet,

Beleidsadviseur cybercrime
**M** 06
@minvenj.nl

20191024A

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Onderwerp:** QenA encryptie en scanfaciliteit.docx
**Datum:** donderdag 24 oktober 2019 11:46:29
**Bijlagen:** QenA encryptie [redacted].docx

10.2.e

L

Ha [redacted]
Mag paar laatste puntjes op de i in tracks voor [redacted].

Groet,
[redacted]

10.2.e
L

**Factsheet – Kabinetsstandpunt encryptie**

| | |
|---|---|
| Dossierhouder | |
| Bereikbaarheid | |

| | |
|---|---|
| Encryptie stelt 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. Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Dit komt de volgende toepassingen ten goede: | |
| 1. | De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups. |
| 2. | Overheidscommunicatie met haar burgers en diensten waarbij vertrouwelijke gegevens worden uitgewisseld |
| 3. | De bescherming van de communicatie binnen de overheid (diplomatiek berichtenverkeer en militaire communicatie) |
| 4. | Veilig te kunnen bewaren en versturen van bedrijfsinformatie. Encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat. |
| 5. | Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers |
| Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die | |

| | |
|---|---|
| gegevens. Dit kan worden onderverdeeld in: | |
| 1. | Belemmeringen wanneer opsporings-, inlichtingen- en veiligheidsdiensten 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. |
| 2. | Criminelen, terroristen en tegenstanders in gewapende conflicten hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. |
| 3. | Het 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. |
| 4. | Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook Criminelen, terroristen en tegenstanders in gewapende conflicten gebruik kunnen maken. |
| Conclusie: | |
| 1. | 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. |

| | |
|---|---|
| 2. | 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. |
| 3. | 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. |
| 4. | 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. |

**Onderwerp: Encryptie (kabinetsstandpunt)**

Naam:

Fractie:

**Q:** Onderschrijft de minister het kabinetsstandpunt inzake encryptie?

**A:**

- Ja, 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.

  - Maar blijft ook oog hebben voor de effecten die dit heeft op de opsporings-, inlichtingen- en veiligheidsdiensten.

**Onderwerp: Encryptie (Uitlatingen MJenV)**

Naam:

Fractie:

**Q:** Hoe verhouden de uitlatingen van de MJenV zich tot het kabinetsstandpunt van encryptie?

A:

- Ik heb begrip getoond voor de zorgen van de Amerikanen, Britten en Australiërs voor de opsporing wanneer Facebook twee andere diensten end-to-end encrypt.
- Wanneer privacy een schild wordt voor criminelen is dit zorgelijk.
- Het zijn ernstige strafbare feiten waarvan de opsporing wordt bemoeilijkt: kinderporno, terrorisme en zware criminaliteit.
- In de conceptbrief wordt opgeroepen om:
  1)het maatschappelijk effect van dit soort beslissingen mee te wegen in de besluitvorming en
  2) in gesprek te gaan over mogelijkheden om het negatief effect op de opsporing tot een minimum beperken.
- Deze dialoog en het gezamenlijk vinden van oplossingen juich ik van harte toe, binnen het kader van het encryptiestandpunt. In dit licht lees ik de conceptbrief.

**Onderwerp: Encryptie (Inzet richting VS)**

Naam:

Fractie:

**Q:** Wat wordt de inzet van de MJenV richting zijn collega's in Washington?

**A:**

- Onderdeel van het kabinetsstandpunt is ook dat het encryptiestandpunt internationaal wordt uitgedragen.
- Ik zal dat dus ook tijdens mijn bezoek aan Washington doen.
- Dat betekent niet dat ik met mijn Amerikaanse collega's niet van gedachten kan wisselen hoe om te gaan met het dilemma van opsporing en zoeken naar oplossingen.

**Onderwerp: Encryptie (Welke oplossing acceptabel)**

Naam:

Fractie:

**Q:** Kunt u aangeven welke 'oplossingen voor encryptie' u wél acceptabel vindt?

**A:**

- Op dit moment heb ik ook nog niet de oplossing.
- Ik juich de dialoog van harte toe en zal de uitkomsten beoordelen aan de hand van het encryptiestandpunten.

[redacted]

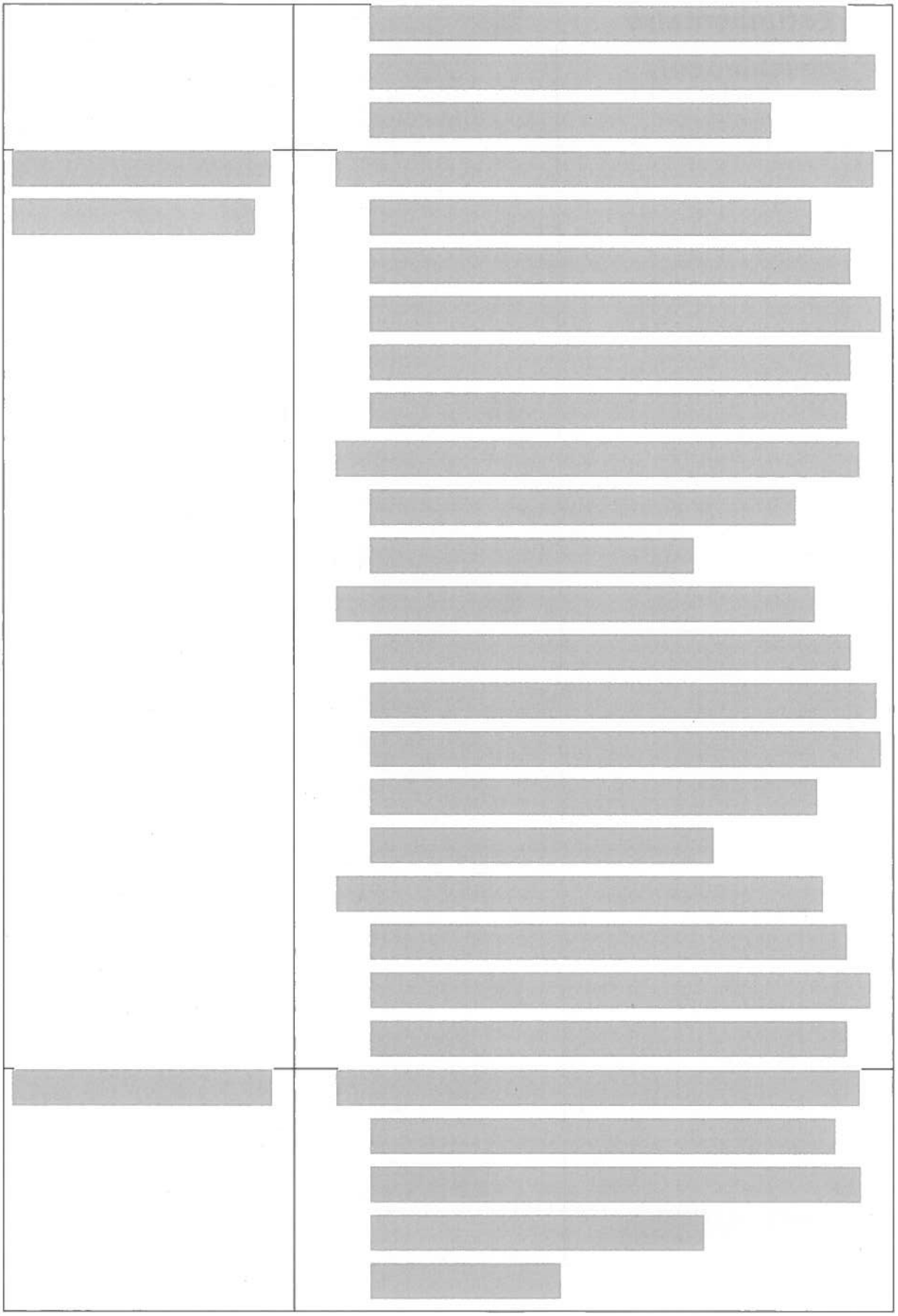
| | |
|---|---|
| Dossierhouder | [redacted] |
| Bereikbaarheid | [redacted] |

L

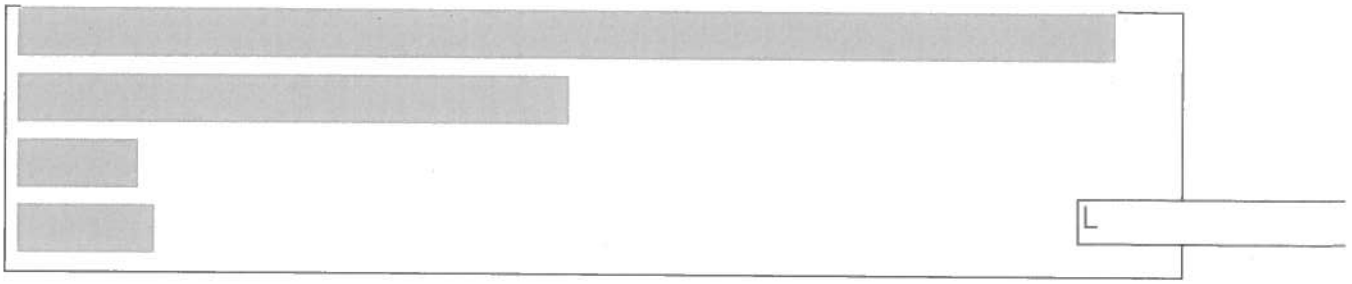
10.2.e

[redacted]

L



| | |
|---|---|
| **Parlementaire geschiedenis** | [redacted] |
| [redacted] | |



**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PNDV; [redacted] BD/KS; [redacted] BD/PNDV
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Datum:** dinsdag 29 oktober 2019 09:51:06
**Bijlagen:** Input interview Nieuwsuur.docx
**Prioriteit:** Hoog

10.2.e

---

[redacted] is goed om even op het netvlies te hebben voor morgen AO. Minister zal met Nieuwsuur spreken over encryptie.
[redacted]: weet jij wanneer dit interview voorzien is voor uitzending? Als het vanavond nog uit wordt gezonden, komt het morgen misschien al terug in het AO.

11.1

[redacted]
Groet,
[redacted]

---

**Van:** [redacted] BD/KS
**Verzonden:** maandag 28 oktober 2019 23:02
**Aan:** [redacted] BD/NCTV
**CC:** [redacted] BD/PNDV ; [redacted] BD/PNDV
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Urgentie:** Hoog

10.2.e

Patricia,
Goed om te weten dat de minister morgen Nieuwsuur te woord staat over de end-to-end versleuteling door Facebook. [redacted]
Gr [redacted]

[redacted]
NCTV
[redacted]

---

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 28 okt. 2019 6:57 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] - BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

10.2.e

Hallo [redacted],
Zoals gezegd heeft de minister morgen een interview met Nieuwsuur, hierbij onze input. Wanneer je echt prangende punten naar voren wilt brengen kun je het ZSM laten weten? De minister staat Nieuwsuur te woord in de schorsing van de APB in de EK.
Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
**M** 06 [redacted]

[redacted]@minvenj.nl

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 18:54
**Aan:** [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>; [redacted] BD/DRC <[redacted]@minjenv.nl>
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo [redacted],
Hierbij de input van Nieuwsuur die [redacted] en ik hebben opgesteld.
Groeten,
[redacted]

**Van:** [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl> 10.2.e
**Verzonden:** maandag 28 oktober 2019 16:59
**Aan:** [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]r@minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hi all,
Ik heb nog even gebeld met Nieuwsuur. Zie hieronder.
Heb de punten van de vorige keer ook weer gebruikt. Graag nog evt jullie aanvulling/het ravijn-kader. Dan bundel ik alles en stuur het naar de minister. Afhankelijk van tijdstip schorsing, wordt het dus tussen 12-14 opgenomen morgen.
Nog niet bekend wanneer de uitzending is.
[redacted]

**Insteek uitzending**

[redacted] 10.2.a; 11.1

**Vragen aan Ferd:**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?
  - [redacted] 11.1
- Is dit een nieuw probleem of al bekend?
  - [redacted]
- Wat zijn deze zorgen precies?
-

Waarom precies kinderporno?

- [redacted]

- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?

[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/PNDV
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Datum:** dinsdag 29 oktober 2019 09:09:40

10.2.e

Ja snap ik, [redacted] tnx voor je reactie

11.1

[redacted]
NCTV
[redacted]

10.2.e

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Datum:** dinsdag 29 okt. 2019 8:56 AM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

10.2.e

Hallo [redacted],
[redacted]

11.1

Groet,
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** maandag 28 oktober 2019 23:02
**Aan:** [redacted] BD/NCTV
**CC:** [redacted] BD/PNDV ; [redacted] BD/PNDV
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Urgentie:** Hoog

10.2.e

Patricia,
Goed om te weten dat de minister morgen Nieuwsuur te woord staat over de end-to-end versleuteling door Facebook. [redacted]

11.1

Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 28 okt. 2019 6:57 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl> 10.2.e
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo [redacted],

Zoals gezegd heeft de minister morgen een interview met Nieuwsuur, hierbij onze input. Wanneer je echt prangende punten naar voren wilt brengen kun je het ZSM laten weten? De minister staat Nieuwsuur te woord in de schorsing van de APB in de EK.

Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
M 06 [redacted]
[redacted]@minvenj.nl

---

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 18:54
**Aan:** [redacted] BD/DCOM/P&B <[redacted]s@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] den - BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>; [redacted] BD/DRC <[redacted]@minjenv.nl> 10.2.e
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hallo [redacted],

Hierbij de input van Nieuwsuur die Pepijn en ik hebben opgesteld.

Groeten,

[redacted]

---

**Van:** [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>
**Verzonden:** maandag 28 oktober 2019 16:59
**Aan:** [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl> 10.2.e
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

Hi all,

Ik heb nog even gebeld met Nieuwsuur. Zie hieronder.

Heb de punten van de vorige keer ook weer gebruikt. Graag nog evt jullie aanvulling/het ravijn-kader. Dan bundel ik alles en stuur het naar de minister. Afhankelijk van tijdstip schorsing, wordt het dus tussen 12-14 opgenomen morgen.

Nog niet bekend wanneer de uitzending is.

[redacted]

**Insteek uitzending**

- [redacted]
  [redacted]
  [redacted]
  [redacted]
  [redacted]

10.2.A'; 11.1

[redacted]

**Vragen aan Ferd:**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?

[redacted]

- Is dit een nieuw probleem of al bekend?

[redacted]

- Wat zijn deze zorgen precies?
- Waarom precies kinderporno?

[redacted]

- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?

[redacted]

[redacted]

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Datum:** dinsdag 29 oktober 2019 12:46:30

10.2.e

Ok, goed te weten en dank!

**Van:** [redacted] BD/KS
**Verzonden:** dinsdag 29 oktober 2019 12:20
**Aan:** [redacted] BD/PNDV; [redacted] BD/PNDV
**CC:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen

10.2.e

In de bijlage bij [redacted] mail zitten ook andere QAs, goed om mee te nemen naar AO.
Uitzending is wrsl niet vanavond, maar wrsl zondag.
Gr [redacted]

**From:** [redacted] BD/PNDV
**Sent:** dinsdag 29 oktober 2019 9:51
**To:** [redacted] BD/PNDV
**Cc:** [redacted] BD/PNDV; [redacted] BD/KS; [redacted] BD/PNDV
**Subject:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Importance:** High

10.2.e

[redacted]
Onderstaande is goed om even op het netvlies te hebben voor morgen AO. Minister zal met Nieuwsuur spreken over encryptie.
@[redacted]: weet jij wanneer dit interview voorzien is voor uitzending? Als het vanavond nog uit wordt gezonden, komt het morgen misschien al terug in het AO.
Op zich gelden de QenA's zoals reeds opgesteld voor het dossier nog steeds denk ik.
Groet,
[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** maandag 28 oktober 2019 23:02
**Aan:** [redacted] BD/NCTV
**CC:** [redacted] BD/PNDV ; [redacted] BD/PNDV
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
**Urgentie:** Hoog

Patricia,
Goed om te weten dat de minister morgen Nieuwsuur te woord staat over de end-to-end versleuteling door Facebook. [redacted]

11.1

Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 28 okt. 2019 6:57 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] - BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>

10.2.e

**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
Hallo [redacted],
Zoals gezegd heeft de minister morgen een interview met Nieuwsuur, hierbij onze input. Wanneer je echt prangende punten naar voren wilt brengen kun je het ZSM laten weten? De minister staat Nieuwsuur te woord in de schorsing van de APB in de EK.
Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
**M** 06 [redacted]
[redacted]@minvenj.nl

---

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 28 oktober 2019 18:54
**Aan:** [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>; [redacted] BD/DRC <[redacted]@minjenv.nl>
**Onderwerp:** RE: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
Hallo [redacted],
Hierbij de input van Nieuwsuur die [redacted] en ik hebben opgesteld.
Groeten,
[redacted]

---

**Van:** [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>
**Verzonden:** maandag 28 oktober 2019 16:59
**Aan:** [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBO <[redacted]@minjenv.nl>; [redacted] BD/DCOM/P&B <[redacted]@minjenv.nl>
**Onderwerp:** FW: Nieuwsuur: Reactie Minister Grapperhaus Facebook E2E-plannen
Hi all,
Ik heb nog even gebeld met Nieuwsuur. Zie hieronder.
Heb de punten van de vorige keer ook weer gebruikt. Graag nog evt jullie aanvulling/het ravijn-kader. Dan bundel ik alles en stuur het naar de minister. Afhankelijk van tijdstip schorsing, wordt het dus tussen 12-14 opgenomen morgen.
Nog niet bekend wanneer de uitzending is.
[redacted]
**Insteek uitzending**

[redacted]

10.2.a

11.1

**Vragen aan Ferd:**

- Hoe kijkt de Minister naar de zorgen van de Anglosaksische collega's omtrent Facebook's E2E-plannen? Deelt hij die volledig?
  - [redacted]

[redacted]

- Is dit een nieuw probleem of al bekend?

11.1

[redacted]

- Wat zijn deze zorgen precies?
- Waarom precies kinderporno?

[redacted]

11.1

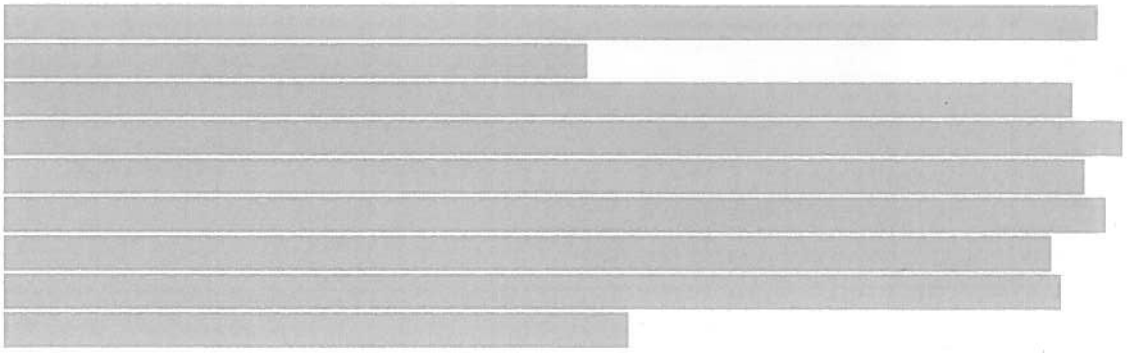
[redacted]

- In hoeverre wijken deze zorgen af van het kabinetsstandpunt over versleuteling?

[redacted]

11.1

[redacted]



**Van:** BD/KS
**Aan:** BD/PNDV; BD/NCTV; BD/PNDV; BD/PNDV; BD/PNDV; BD/PNDV; BD/KS; BD/KS; BD/NCSC/Staf; BD/NCSC/Staf; BD/NCSC; BD/NCSC/SK; BD/PSD; BD/KA; BD/NCC/ECO; BD/NCC/ECO 10.2.e
**Cc:** BD/KS
**Onderwerp:** RE: Bespreekpunten MOCO 5 november
**Datum:** maandag 4 november 2019 15:19:17

---

Allen, lijkt me goed om de mindmap te bespreken.

gaat nota opstellen (iam ons) om opties te duiden en richting van de minister te krijgen, en zal ook het initiatief nemen om met de kabinetsstandpunt partners om de tafel te gaan op redelijk korte termijn (maar na duiding minister). 11.1

Groet,

**From:** BD/PNDV
**Sent:** maandag 4 november 2019 14:25
**To:** BD/NCTV; BD/PNDV; BD/PNDV; BD/PNDV; BD/PNDV; BD/KS; BD/KS; BD/KS; BD/NCSC/Staf; BD/NCSC/Staf; BD/NCSC; BD/NCSC/SK; BD/PSD; BD/KA; BD/NCC/ECO; BD/NCC/ECO 10.2.e
**Subject:** Bespreekpunten MOCO 5 november

Dag allen,
Morgen wordt in het MOCO gesproken over de volgende zaken:

- Encryptie (n.a.v. berichtgeving afgelopen weekend) (zie ook bijgevoegde mindmap van L

Groet,

Senior beleidsmedewerker
.....
**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid** 10.2.e
**Programma Nederland Digitaal Veilig**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
**M** 06
@nctv.minjenv.nl

**Van:** [redacted] (NCSC-NL)
**Aan:** [redacted] - BD/KA
**Onderwerp:** RE: Input terts
**Datum:** maandag 4 november 2019 10:25:00

10.2.e

Cool!

**From:** [redacted] - BD/KA <[redacted]@nctv.minjenv.nl>
**Sent:** maandag 4 november 2019 09:06
**To:** [redacted] - BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] (NCSC-NL) <[redacted]@ncsc.nl>
**Subject:** FW: Input terts

Hi [redacted]

Zie ook onder, ik heb onze actie in terts laten opnemen

Gr, [redacted]

**Van:** [redacted] - BD/KA
**Verzonden:** maandag 4 november 2019 08:51
**Aan:** [redacted] - BD/KA [redacted]@nctv.minjenv.nl>
**CC:** [redacted]@ncsc.nl; [redacted]@ncsc.nl' [redacted]@ncsc.nl>; [redacted] - BD/NCSC/SK <[redacted]@minjenv.nl>
**Onderwerp:** Input terts

Hi [redacted]

Zie onder, ik schakel nog ff met NCSC

Gr, [redacted]

**Minister oppert 'achterdeur' in sociale media (ANP, zondag)** Justitieminister Ferd Grapperhaus wil dat chatdiensten als Whatsapp een 'achterdeur' inbouwen. Als er iets verdachts gebeurt, moet justitie de sleutel kunnen opvragen om een gesprek te kunnen inzien, zegt hij tegen Nieuwsuur. Grapperhaus' uitlatingen zijn geen kabinetsbeleid. Het kabinet vindt nog steeds dat het inperken van de versleuteling van chat- en berichtendiensten "onwenselijk" is. De sleutel van zo'n 'achterdeur' zou in verkeerde handen kunnen vallen. [redacted]

11.1

Ministerie van Justitie en Veiligheid



Ministry of Justice and Security

**Van:** [redacted] BD/PACT
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: toegang tot versleutelde berichten
**Datum:** maandag 4 november 2019 21:36:44

10.2.e

Ha [redacted]
[redacted] 10.1.d
Ik ga even na wie bij CT het encryptie-dossier doet.
Groet [redacted]

**Van:** [redacted] BD/KS
**Verzonden:** maandag 4 november 2019 15:15
**Aan:** [redacted] BD/PACT
**CC:** [redacted] BD/PLR; [redacted] BD/PACT; [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/PNDV
**Onderwerp:** RE: toegang tot versleutelde berichten

10.2.e

Hoi,
Ja, loopt met DGRR. [redacted] . [redacted] gaat nota opstellen om opties te duiden en [redacted], en zal ([redacted]) ook initiatief nemen om met de kabinetsstandpunt-partners om de tafel te gaan op redelijk korte termijn ([redacted]).
Ter info een mindmap die Analyse met NCSC heeft opgemaakt nav terts. [redacted] 11.1
[redacted]
In principe zijn [redacted] (cybersecurity) en [redacted] (CT) mijn encryptie-afstemmingscollega's: willen jullie ook aangehaakt?
Gr [redacted]

**From:** [redacted] BD/PACT
**Sent:** maandag 4 november 2019 11:21
**To:** [redacted] BD/KS
**Cc:** [redacted] BD/PLR; [redacted] BD/PACT; [redacted] BD/KS
**Subject:** toegang tot versleutelde berichten

Hi [redacted]
Eerder was je bezig met de encryptie. Was even benieuwd naar de betrokkenheid van NCTV bij de laatste berichtgeving.
https://www.nu.nl/tech/6008720/minister-grapperhaus-wil-toegang-tot-versleutelde-berichtendiensten.html
[redacted] L
Groet [redacted]
Met vriendelijke groet,
[redacted]
Programmamanager Online Terrorisme en Extremisme
Ministerie van Justitie en Veiligheid
Nationaal Coordinator Terrorismebestrijding en Veiligheid
06-[redacted]

**Van:** [redacted] BD/KA
**Aan:** [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/KS
**Cc:** [redacted] BD/NCSC/SK
**Onderwerp:** RE: Non paper interception OTT
**Datum:** maandag 4 november 2019 11:53:10
**Bijlagen:** OTTs en Encryptie-v0c.pdf

10.2.e

---

Collega's,
Paar tikfouten er uit + leesbaarheid zonder leesbril omhoog ;)
Gr, [redacted]

**Van:** [redacted] BD/KA
**Verzonden:** maandag 4 november 2019 10:40
**Aan:** [redacted] BD/KS ; [redacted] BD/PNDV ; [redacted] BD/KS
**CC:** [redacted] BD/NCSC/SK
**Onderwerp:** RE: Non paper interception OTT
Hi [redacted],

[redacted] Hierbij aangepaste versie van de mindmap, ik bel je zo ff

11.1

Gr, [redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** donderdag 31 oktober 2019 13:35
**Aan:** [redacted] BD/KA <[redacted]@nctv.minjenv.nl>; [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**CC:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Non paper interception OTT
Wow super, goed als ik er volgende week even goed naar kijk?

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/KA <[redacted]@nctv.minjenv.nl>
**Datum:** donderdag 31 okt. 2019 1:02 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Non paper interception OTT
Hi [redacted],
[redacted] en ik hebben document/mindmap gemaakt om de verschillende aspecten van deze problematiek in kaart te brengen. Doel is om deelnemers in de discussie (zoals bijv Pieter-Jaap en Patricia) voldoende handvaten te geven op de discussie te kunnen voeren.
Graag ontvangen wij jullie feedback,
Gr, [redacted]

10.2.e

**Van:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>
**Verzonden:** donderdag 24 oktober 2019 10:57
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>; [redacted] BD/KA <[redacted]@nctv.minjenv.nl>; [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>

10..2.e

**Onderwerp:** RE: Non paper interception OTT

Hoi [redacted],

Bedankt voor het delen –

[redacted] 11.1

Hartelijke groeten,

[redacted]

**Van:** [redacted] BD/PNDV
**Verzonden:** woensdag 23 oktober 2019 10:40
**Aan:** [redacted] BD/KS; [redacted] BD/PACT; [redacted]
BD/KA; [redacted] BD/NCSC/SK; [redacted] BD/PACT
**Onderwerp:** RE: Non paper interception OTT 11.1

Hallo [redacted],

[redacted]

[redacted]

Groet,

[redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** woensdag 23 oktober 2019 09:05
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>; [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>; [redacted] BD/KA <[redacted]@nctv.minjenv.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Non paper interception OTT

ter info en reactie.
Eerder informeerde ik jullie al dat de minister sterk neigt naar opties verkennen, waarbij een optie is : EU regelgeving [redacted] 11.1

[redacted]

NCTV

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 21 okt. 2019 10:49 PM
**Aan:** [redacted] 10.2.e
BD/PIDS <[redacted]@minjenv.nl>, [redacted]
BD/KS <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted]
**Onderwerp:** Non paper interception OTT

Hallo allemaal,
Zoals jullie weten heeft de minister het akkoord gegeven om bij enkele lidstaten te inventariseren of zij interesse hebben in Europese regelgeving rond het kunnen aftappen van OTT's.
In overleg met de internationale directie heb ik een non-paper gemaakt. Dit paper stelt haar in staat om te inventariseren bij een beperkte groep LS om te bezien of zij ook oren hebben naar een Europese regeling om OTT's af te tappen.
Een non-paper zou de probleemstelling, context en oplossingsrichting duidelijk moeten maken.
Ik heb dit geprobeerd in bijgevoegde non-paper, zouden jullie er eens naar willen kijken? Brengt dit paper de noodzaak duidelijk genoeg naar voren? Ik verspreid het paper bewust nog even onder de JenV organisaties, dus verspreid h'm svp niet.
Groeten,

[redacted]

10.2.e

Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
**M** 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] BD/KA
**Aan:** BD/KA; [redacted] BD/KA; [redacted] BD/NCTV
**Cc:** [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/NCSC/SK; [redacted] BD/KA; [redacted] BD/KA; [redacted] BD/KA; [redacted] BD/KA
**Onderwerp:** FW: Mindmap/input tbv bespreekpunt MOCO
**Datum:** maandag 4 november 2019 12:05:45
**Bijlagen:** OTTs en Encryptie-v0c.pdf

10.2.e

---

Collega's,
Nav het terts-actiepunt dat KA en NCSC een mindmap zouden voorbereiden om de verschillende aspecten van encryptie in relatie tot diensten als Whatsapp te belichten. In attachment de mindmap. Deze mindmap is geagendeerd voor het Cyber MOCO morgen,

Gr, [redacted]

10.2.e

**Van:** [redacted] BD/KA
**Verzonden:** maandag 4 november 2019 12:00
**Aan:** [redacted] BD/PNDV
**CC:** [redacted] BD/NCSC/SK
**Onderwerp:** Mindmap/input tbv bespreekpunt MOCO

10.2.e

Hi [redacted],
Zou jij attachment willen toevoegen aan de agenda?

Tnx,

Gr, [redacted]

**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
Postbus 16950 | 2500 BZ | Den Haag | The Netherlands
**M** +31 6 [redacted]
[redacted]@nctv.minjenv.nl
http://www.nctv.nl

**Van:** [redacted] - BD/KA
**Aan:** [redacted] . - BD/DVB/BA; [redacted] . BD/NCTV; [redacted] - BD/PNDV; [redacted] - BD/PNDV; [redacted] - BD/PNDV; [redacted] - BD/PNDV; [redacted] - BD/KS; [redacted] BD/KS; [redacted] - BD/KS; [redacted] - BD/NCSC/Staf; [redacted] BD/NCSC/Staf; [redacted] - BD/NCSC; [redacted] drs. R.S.A. - BD/NCSC/SK; [redacted] BD/PSD; [redacted] - BD/NCC/ECO; [redacted] - BD/NCC/ECO
**Cc:** [redacted] - BD/NCSC/SK
**Onderwerp:** RE: Bespreekpunten MOCO 5 november
**Datum:** woensdag 6 november 2019 10:02:32
**Bijlagen:** OTTs en Encryptie-v0d.pdf

10.2.e

---

Beste collega's,

Hierbij zoals beloofd en naar aanleiding van het MOCO aangepaste versie van de mindmap met o.a. de verschillen tussen tradionele tap en OTT-tap. Mocht er behoefte zijn aan een toelichting dan hoor ik dat graag,

Gr, [redacted]

---

**Van:** [redacted] @nctv.minjenv.nl>
**Verzonden:** maandag 4 november 2019 14:25
**Aan:** [redacted] - BD/NCTV < [redacted] @nctv.minjenv.nl>; [redacted] - BD/PNDV [redacted] @nctv.minjenv.nl>; [redacted] BD/PNDV < [redacted] @nctv.minjenv.nl>; [redacted] - BD/PNDV < [redacted] @nctv.minjenv.nl>; [redacted] - BD/PNDV < [redacted] @nctv.minjenv.nl>; [redacted] - BD/KS [redacted] @nctv.minjenv.nl>; [redacted] BD/KS < [redacted] @nctv.minjenv.nl>; [redacted] . - BD/KS < [redacted] @nctv.minjenv.nl>; [redacted] - BD/NCSC/Staf < [redacted] @minjenv.nl>; [redacted] BD/NCSC/Staf < [redacted] @minjenv.nl>; [redacted] - BD/NCSC < [redacted] @minjenv.nl>; [redacted] - BD/NCSC/SK < [redacted] @minjenv.nl>; [redacted] BD/PSD < [redacted] @nctv.minjenv.nl>; [redacted] - BD/KA < [redacted] @nctv.minjenv.nl>; [redacted] - BD/NCC/ECO < [redacted] @nctv.minjenv.nl>; [redacted] - BD/NCC/ECO [redacted] @minjenv.nl>
**Onderwerp:** Bespreekpunten MOCO 5 november

10.2.e

Dag allen,

Morgen wordt in het MOCO gesproken over de volgende zaken:

- Encryptie (n.a.v. berichtgeving afgelopen weekend) (zie ook bijgevoegde mindmap van [redacted]
- Korte terugkoppeling van het AO Cybersecurity van vorige week
- W.v.t.t.k.

Groet,
[redacted]

[redacted] [redacted]
Senior beleidsmedewerker
.....
**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
**Programma Nederland Digitaal Veilig**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
[redacted] nctv.minjenv.nl

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/NCSC/SK; [redacted] BD/KS; [redacted] BD/PNDV
**Onderwerp:** FW: Encryptie berichtendiensten
**Datum:** dinsdag 5 november 2019 14:35:58

10.2.e

Zoals net besproken hierbij ter info. het bericht van [redacted]

Kind Regards,

[redacted]
Cyber Security Policy Department
National Coordinator Security and CT

**Van:** [redacted] @ncsc.nl>
**Datum:** maandag 04 nov. 2019 17:24
**Aan:** [redacted] BD/PNDV < [redacted] @nctv.minjenv.nl>, [redacted] BD/PNDV < [redacted] @nctv.minjenv.nl>, [redacted] BD/NCSC/IVT < [redacted] @minjenv.nl>
**Kopie:** [redacted] BD/NCSC < [redacted] @ncsc.nl>, [redacted] BD/NCSC/OP [redacted] @minjenv.nl>, [redacted] BD/NCSC/Staf <[redacted] s@ncsc.nl>, [redacted] - BD/NCSC/OP [redacted] @minjenv.nl>, [redacted] BD/NCSC/Staf < [redacted] @minjenv.nl>
**Onderwerp:** Encryptie berichtendiensten

10.2.e

Beste [redacted],
Gisteren lichtte de Minister toe in Nieuwsuur dat hij wil dat Justitie toegang krijgt tot versleutelde berichten op diensten als Whatsapp en Telegram als daarin kinderporno wordt gedeeld. Voor zover nog niet onder jullie aandacht, willen we graag wijzen op het kabinetsstandpunt encryptie uit 2016. [redacted]

Kabinetsstandpunt: https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie
Mocht dit nadere toelichting vragen, hoor ik het graag.

Met vriendelijke groet,

[redacted]
Adviseur bestuurlijke ondersteuning

**Nationaal Cyber Security Centrum**
**Ministerie van Justitie en Veiligheid**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 117 | 2501 CC | Den Haag

**T** 06 [redacted]
[redacted] @minjenv.nl
www.ncsc.nl

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** donderdag 7 november 2019 08:11:17

10.2.e

Ja had ik gezien. Ik dacht check even voordat ik nog eventueel commentaar op het stuk ga maken.

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 november 2019 20:21
**Aan:** [redacted] BD/PNDV
**Onderwerp:** RE: Gespreksnota encryptie

Ja heb al nieuwe versie, ligt al bij PJ en Patricia

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 06 nov. 2019 5:55 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Hallo [redacted]
Deze is nu al weg toch?

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 17:10
**Aan:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] BD/KA <[redacted]@nctv.minjenv.nl>; [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>; [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>

10.2.e

**Onderwerp:** FW: Gespreksnota encryptie

Ha [redacted],
Onderstaand is uiteraard gewoon aan beleid, maar mochten jullie slimme zinnen / tracks hebben (met referte aan de discussie in MOCO cyber) op de nota van dgrr dan houd ik me warm aanbevolen.
Snap ook als t niet lukt om hier voor morgenochtend goed naar te kijken, maar gezien ook Moco vanmiddag wil ik jullie in ieder geval graag kans geven voor inbreng.
(Wel wetende dat we al wel eerder zijn meegegaan in verkennen van opties voor opsporing!)
[redacted]

11.1

Gr [redacted]
[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 3:31 PM
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]r@minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>

**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted]
BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om [redacted] 11.1

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted] 11.1 Uiteraard houd ik jullie hoe dan ook aangesloten.
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?
Groet,
[redacted]

**Van:** [redacted] BD/PNDV
**Aan:** [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/PNDV; [redacted] BD/KA; [redacted] BD/NCSC/SK
**Cc:** [redacted] BD/PNDV
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 09:55:49

10.2.e

Ik heb ook weinig tijd want ontvang zo [redacted] delegatie.

10.2.a

[redacted]

11.1

[redacted]

11.1

Kind Regards,

[redacted]
Cyber Security Policy Department
National Coordinator Security and CT

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 21:06
**Aan:** [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/KA <[redacted]@nctv.minjenv.nl>, [redacted] - BD/NCSC/SK <[redacted]@minjenv.nl>
**Kopie:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Gespreksnota encryptie

Collega's,
Het Moco kwam geen moment te vroeg ;-) DGRR maakt haast van de nota; ik heb een winstwaarschuwing gegeven omdat ik wel onze lijn hierin wil betrekken.
Bijgaand mijn suggesties voor comments richting DGRR en DWJZ. Graag jullie check hierop en

doe zeker een aanpassing als ik iets verkeerds zeg! Verder bij voorkeur alleen noodzakelijke aanvullingen / fout-herstellingen in trackchanges (toelichting kan in de opmerkingen) omdat dit wat mij betreft ook de nota van DGRR moet blijven. Omdat ik niet meer achter een pc kan knutselen morgen, zou ik jullie willen vragen om je comments meteen 'doorstuurbaar' naar DGRR te maken (dus geen interne opmerkingen svp), omdat ik de bijlage blind zal moeten bijvoegen in de mail.

[redacted] 11.1

[redacted] Patricia later informeren (want ik hoop dat DGRR met nieuwe versie komt).

Gr [redacted]

**From:** [redacted] BD/DRC/CV
**Sent:** dinsdag 5 november 2019 17:42
**To:** [redacted] BD/DWJZ/SSR; [redacted] BD/DGRR; [redacted] BD/KS; [redacted] BD/DWJZ/SSR; [redacted] BD/DWJZ/JZW 10.2.e
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DBAenV/IenK
**Subject:** RE: Gespreksnota encryptie

Hallo [redacted],

Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies.
Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat [redacted]

We houden je op de hoogte! 11.1

Groet,

[redacted]

**Van:** [redacted] BD/DWJZ/SSR
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/DGRR ; [redacted] BD/KS ; [redacted] BD/DWJZ/SSR ; [redacted] BD/DWJZ/JZW
**CC:** [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Ha [redacted]

Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. [redacted] 11.1
- Verder moet je je afvragen of [redacted]
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en –diensten). [redacted]

Groet, 11.1

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/SSR 10.2.e

<[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,

Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.

De minister wordt geadviseerd om [redacted]

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted]? Uiteraard houd ik jullie hoe dan ook aangesloten.

Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?

Groet,

[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/NCTV; [redacted] BD/NCTV
**Cc:** [redacted] BD/PNDV; [redacted] BD/KS
**Onderwerp:** FW: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 14:01:13
**Bijlagen:** Gespreksnota.docx

10.2.e

Beste Pieter Jaap en Patricia,

Nav de uitspraken van de minister over end-to-end-encryptie en opsporing, heeft DGRR bijgaande nota afgestemd met DWJZ en ons om de uitspraak van de minister verder vorm te geven. De uitspraak dat er een ontsleutelplicht moet komen voor bestrijding van kinderporno ging buiten de annotatie.

Dgrr start nu een inventarisatie om te komen tot ontsleuteling van vercijferde info. [redacted]

11.1

[redacted]

Jullie zullen als MT NCTV in digijust in de lijn van dgrr worden opgenomen voor akkoord.

Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** woensdag 06 nov. 2019 12:19 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DGRR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

10.2.e

Hallo [redacted],
Dankjewel. Ik heb de nota aangepast. [redacted]
Wat ik niet heb overgenomen is [redacted]

11.1

. De nota leidt tot een gesprek en als er zodanige problemen zijn met deze term kunnen deze daar naar voren worden gebracht.

Is het nodig dat we even bellen?
Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
M 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 november 2019 10:15
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/DWJZ/SSR ; [redacted] BD/DGRR ; [redacted] BD/DWJZ/SSR ; [redacted] BD/DWJZ/JZW
**CC:** [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/lenK
**Onderwerp:** RE: Gespreksnota encryptie
Hoi [redacted] en collega's,
Bijgaand onze aanpassingen op de nota. [redacted] 11.1
Gr. [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 5:42 PM
**Aan:** [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DGRR <[redacted]@minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl> 10.2.e
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/lenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie
Hallo [redacted],
Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies.
Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat [redacted]
We houden je op de hoogte! 11.1

Groet,
[redacted]

**Van:** [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Ha [redacted]
Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. [redacted] 11.1
- Verder moet je je afvragen of [redacted]
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en –diensten). [redacted] 11.1

Groet,
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om [redacted] 11.1
De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted] Uiteraard houd ik jullie hoe dan ook aangesloten.
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?
Groet,
[redacted]

**Van:** [redacted] BD/KA
**Aan:** [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/PNDV; [redacted] BD/NCSC/SK
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 09:53:50

10.2.e

---

Hi [redacted],
Geen aanvullingen; ik stuur je zo aangepaste mindmap.

[redacted]

11.1

Gr, [redacted]

**Van:** [redacted] BD/KS
**Verzonden:** dinsdag 5 november 2019 21:04
**Aan:** [redacted] BD/PACT ; [redacted] BD/PNDV ; [redacted] BD/KA ; [redacted] BD/NCSC/SK
**CC:** [redacted] BD/PNDV ; [redacted] BD/PNDV
**Onderwerp:** FW: Gespreksnota encryptie

10.2.e

Collega's,
Het Moco kwam geen moment te vroeg ;-) DGRR maakt haast van de nota; ik heb een winstwaarschuwing gegeven omdat ik wel onze lijn hierin wil betrekken.
Bijgaand mijn suggesties voor comments richting DGRR en DWJZ. Graag jullie check hierop en doe zeker een aanpassing als ik iets verkeerds zeg! Verder bij voorkeur alleen noodzakelijke aanvullingen / fout-herstellingen in trackchanges (toelichting kan in de opmerkingen) omdat dit wat mij betreft ook de nota van DGRR moet blijven. Omdat ik niet meer achter een pc kan knutselen morgen, zou ik jullie willen vragen om je comments meteen 'doorstuurbaar' naar DGRR te maken (dus geen interne opmerkingen svp), omdat ik de bijlage blind zal moeten bijvoegen in de mail.

[redacted]

11.1

[redacted] Patricia later informeren (want ik hoop dat DGRR met nieuwe versie komt).
Gr [redacted]

**From:** [redacted] BD/DRC/CV
**Sent:** dinsdag 5 november 2019 17:42
**To:** [redacted] BD/DWJZ/SSR; [redacted] BD/DGRR; [redacted] BD/KS; [redacted] BD/DWJZ/SSR; [redacted] BD/DWJZ/JZW
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DBAenV/IenK
**Subject:** RE: Gespreksnota encryptie

10.2.e

Hallo [redacted],
Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies. Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat [redacted]
We houden je op de hoogte!

11.1

Groet,
[redacted]

**Van:** [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl> 10.2.e
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Ha [redacted],
Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. [redacted]
- Verder moet je je afvragen of [redacted]
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en -diensten). [redacted].

Groet, 11.1
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl> 10.2.e
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om [redacted] 11.1
De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted] Uiteraard houd ik jullie hoe dan ook aangesloten.
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de not 11.1
Groet,
[redacted]

**Van:** [redacted] BD/KA
**Aan:** [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/PNDV; [redacted] BD/NCSC/SK
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 10:00:53
**Bijlagen:** OTTs en Encryptie-v0d.pdf
OTTs en Encryptie-v0d.docx

10.2.e

---

Collega's,

Zoals beloofd, aangepaste mindmap, voor het gemak van de knip en plak ook een export naar Word (die enkel geschikt is voor knip-plak)
Gr, [redacted]

**Van:** [redacted] BD/KS
**Verzonden:** dinsdag 5 november 2019 21:04
**Aan:** [redacted] BD/PACT ; [redacted] BD/PNDV ; [redacted] BD/KA ; [redacted] BD/NCSC/SK
**CC:** [redacted] BD/PNDV ; [redacted] BD/PNDV
**Onderwerp:** FW: Gespreksnota encryptie

10.2.e

Collega's,
Het Moco kwam geen moment te vroeg ;-) DGRR maakt haast van de nota; ik heb een winstwaarschuwing gegeven omdat ik wel onze lijn hierin wil betrekken.
Bijgaand mijn suggesties voor comments richting DGRR en DWJZ. Graag jullie check hierop en doe zeker een aanpassing als ik iets verkeerds zeg! Verder bij voorkeur alleen noodzakelijke aanvullingen / fout-herstellingen in trackchanges (toelichting kan in de opmerkingen) omdat dit wat mij betreft ook de nota van DGRR moet blijven. Omdat ik niet meer achter een pc kan knutselen morgen, zou ik jullie willen vragen om je comments meteen 'doorstuurbaar' naar DGRR te maken (dus geen interne opmerkingen svp), omdat ik de bijlage blind zal moeten bijvoegen in de mail.

[redacted]

11.1

[redacted] Patricia later informeren (want ik hoop dat DGRR met nieuwe versie komt).
Gr [redacted]

**From:** [redacted] BD/DRC/CV
**Sent:** dinsdag 5 november 2019 17:42
**To:** [redacted] BD/DWJZ/SSR; [redacted] BD/DGRR; [redacted] N.W.F. - BD/KS; [redacted] BD/DWJZ/SSR; [redacted] BD/DWJZ/JZW
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DBAenV/IenK
**Subject:** RE: Gespreksnota encryptie

10.2.e

Hallo [redacted],
Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies. Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat [redacted]
We houden je op de hoogte!
Groet,
[redacted]

11.1

**Van:** [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] BD/KS

< @nctv.minjenv.nl>; BD/DWJZ/SSR < @minjenv.nl>; BD/DWJZ/JZW < @minjenv.nl> 10.2.e
**CC:** BD/DRC/CV < @minjenv.nl>; BD/DBAenV/IenK < @minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Ha ,
Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten.
- Verder moet je je afvragen of
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en -diensten).

.

Groet,

**Van:** BD/DRC/CV < @minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** BD/DGRR < @minjenv.nl>; BD/KS < @nctv.minjenv.nl>; BD/DWJZ/SSR < @minjenv.nl>; BD/DWJZ/SSR < @minjenv.nl>; BD/DWJZ/JZW < @minjenv.nl> 10.2.e
**CC:** BD/DRC/CV < @minjenv.nl>; BD/DBAenV/IenK < @minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om

De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst
? Uiteraard houd ik jullie hoe dan ook aangesloten.
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de not 11.1
Groet,

**Van:** [redacted] BD/PACT
**Aan:** [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/KA; [redacted] BD/NCSC/SK
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/PACT
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 09:13:15

10.2.e

Beste allemaal,

Sec beredeneerd vanuit CT, heb ik momenteel geen aanvullingen. [redacted]

11.1

[redacted]

Met hartelijke groet,

[redacted]

**From:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Date:** Tuesday, 05 Nov 2019, 9:06 PM
**To:** [redacted] BD/PACT <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/KA <[redacted]@nctv.minjenv.nl>, [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>
**Cc:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Subject:** FW: Gespreksnota encryptie

10.2.e

Collega's,
Het Moco kwam geen moment te vroeg ;-) DGRR maakt haast van de nota; ik heb een winstwaarschuwing gegeven omdat ik wel onze lijn hierin wil betrekken.
Bijgaand mijn suggesties voor comments richting DGRR en DWJZ. Graag jullie check hierop en doe zeker een aanpassing als ik iets verkeerds zeg! Verder bij voorkeur alleen noodzakelijke aanvullingen / fout-herstellingen in trackchanges (toelichting kan in de opmerkingen) omdat dit wat mij betreft ook de nota van DGRR moet blijven. Omdat ik niet meer achter een pc kan knutselen morgen, zou ik jullie willen vragen om je comments meteen 'doorstuurbaar' naar DGRR te maken (dus geen interne opmerkingen svp), omdat ik de bijlage blind zal moeten bijvoegen in de mail.

[redacted]

11.1

[redacted] Patricia later informeren (want ik hoop dat DGRR met nieuwe versie komt).
Gr Nina

**From:** [redacted] BD/DRC/CV
**Sent:** dinsdag 5 november 2019 17:42
**To:** [redacted] BD/DWJZ/SSR; [redacted] BD/DGRR; [redacted] BD/KS; [redacted] BD/DWJZ/SSR; [redacted] BD/DWJZ/JZW
**Cc:** [redacted] BD/DRC/CV; [redacted] BD/DBAenV/IenK
**Subject:** RE: Gespreksnota encryptie

10.2.e

Hallo [redacted],
Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies. Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat dit technisch mogelijk is, maar dit onderzoeken we graag verder met private partijen.
We houden je op de hoogte!
Groet,
[redacted]

**Van:** [redacted] BD/DWJZ/SSR
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/DGRR ; [redacted] BD/KS ; [redacted] BD/DWJZ/SSR ; [redacted] BD/DWJZ/JZW
**CC:** [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Ha [redacted]
Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. [redacted]
- Verder moet je je afvragen of [redacted] 11.1
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en –diensten). [redacted] 11.1

Groet,
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] 10.2.e [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg. 11.1
De minister wordt geadviseerd om [redacted]
De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted] Uiteraard houd ik jullie hoe dan ook aangesloten 11.1
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?
Groet,
[redacted]

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: Gespreksnota encryptie
**Datum:** woensdag 6 november 2019 13:47:16

10.2.e

Sorry ik was in gesprek dus kon niet opnemen
Alles goed zo?

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 06 nov. 2019 1:42 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Fijn thanks!

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 06 nov. 2019 1:14 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

[redacted]

11.1

[redacted]

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 6 november 2019 13:00
**Aan:** [redacted] BD/KS
**Onderwerp:** FW: Gespreksnota encryptie

10.2.e

En dit onze suggesties.

Gaat om wat er NIET is overgenomen (en dan bedoel ik niet perse letterlijk maar qua intentie/strekking).
Als je even zou kunnen bellen zou heel fijn zijn!

[redacted]
NCTV
[redacted]

---

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** woensdag 06 nov. 2019 10:14 AM
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DGRR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl> 10.2.e
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie
Hoi [redacted] en collega's,
Bijgaand onze aanpassingen op de nota. [redacted] 11.1
Graag ontvang ik een definitieve versie om ook met mijn MT verder af te stemmen.
Gr. [redacted]

[redacted]
NCTV
[redacted]

---

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 5:42 PM
**Aan:** [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DGRR <[redacted]@minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>, [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl> 10.2.e.
**Kopie:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>, [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** RE: Gespreksnota encryptie

Hallo [redacted],
Veel dank voor je snelle reactie. Inzake je eerste punt zal ik dit expliciteren in de toelichting op het advies. Inzake je tweede punt gaan we dat inderdaad ontdekken. Wij hebben al wel singalen ontvangen dat dit technisch mogelijk is, maar dit onderzoeken we graag verder met private partijen.
We houden je op de hoogte!
Groet,
[redacted]

**Van:** [redacted] BD/DWJZ/SSR
**Verzonden:** dinsdag 5 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/DGRR ; [redacted] BD/KS ; [redacted] BD/DWJZ/SSR ; [redacted] BD/DWJZ/JZW
**CC:** [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**Onderwerp:** RE: Gespreksnota encryptie

Ha [redacted],
Een paar dingen.

- Als de MJenV dat vindt, tja, dan zul je dus met de bedrijven om de tafel moeten. [redacted]
- Verder moet je je afvragen of [redacted] 11.1
- Voor GSM is indertijd geregeld dat de aanbieder de crypto die hij zelf aanbracht op het signaal (dat betrof het signaal tussen mast en telefoontoestel) eraf moest halen, voor het signaal aan te bieden aan de aftappende instantie (art. 2, onder e, Besluit aftappen openbare telecommunicatienetwerken en –diensten). [redacted]

Groet, 11.1
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 15:31
**Aan:** [redacted] BD/DGRR <[redacted]@minjenv.nl>; [redacted] 10.2.e
[redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/SSR <[redacted]@minjenv.nl>; [redacted] BD/DWJZ/JZW <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**Onderwerp:** Gespreksnota encryptie

Beste collega's,
Afgelopen zondag heeft de minister aangeven een ontsleutelplicht te willen instellen voor OTT communicatiediensten. In het DGRR stafoverleg met de minister is gevraagd om een gespreksnota voor een nader te plannen overleg.
De minister wordt geadviseerd om [redacted] 11.1
De minister nam ook het woord 'wet' in de mond, vandaar dit ook even wetgeving aanschrijf. Meer dan welkom om aan te schuiven, maar misschien is het praktischer om jullie tijd te besparen dat eerst [redacted] Uiteraard houd ik jullie hoe dan ook aangesloten 11.1
Ik zou deze nota graag morgenochtend de lijn in doen. Vinden jullie iets van de nota?
Groet,
[redacted]

**Van:** [redacted] BD/NCSC/SK
**Aan:** [redacted] BD/PNDV; [redacted] BD/KA
**Onderwerp:** RE: Verschil aftappen traditionele telco van PTT
**Datum:** donderdag 7 november 2019 17:01:58

10.2.e

---

Hoi beiden,
Ik lees jullie mails nu pas omdat ik op woensdag vrij ben. [redacted]
[redacted] 11.1
Hartelijke groeten,
[redacted]

**Van:** [redacted] BD/PNDV
**Verzonden:** woensdag 6 november 2019 17:55
**Aan:** [redacted] BD/KA; [redacted] BD/NCSC/SK
**Onderwerp:** RE: Verschil aftappen traditionele telco van PTT 10.2.e
[redacted]

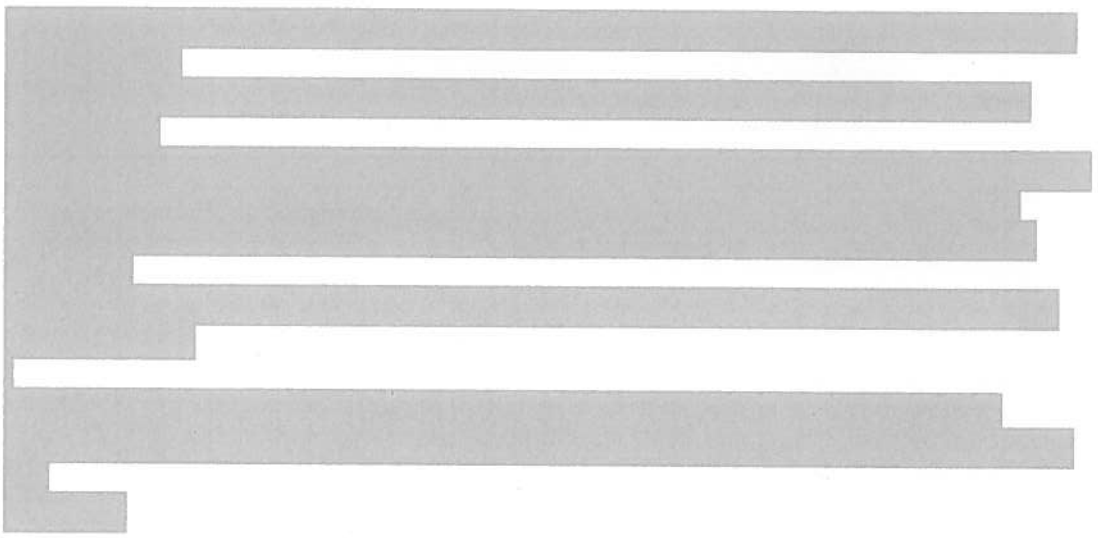
**Van:** [redacted] BD/PNDV
**Verzonden:** woensdag 6 november 2019 17:55
**Aan:** [redacted] BD/KA ; [redacted] BD/NCSC/SK 11.1
**Onderwerp:** RE: Verschil aftappen traditionele telco van PTT
[redacted] ,
Dat zijn denk ik twee hele verhelderende punten over wat je eigenlijk aan het doen bent.

**Van:** [redacted] BD/KA <[redacted]@nctv.minjenv.nl>
**Verzonden:** dinsdag 5 november 2019 18:15
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>; [redacted] .
BD/NCSC/SK <[redacted]@minjenv.nl> 10.2.e
**Onderwerp:** FW: Verschil aftappen traditionele telco van PTT
Hi [redacted]
Mailtjes passeerde elkaar net, zie ook onder mijn tekst (op iPhone) naar [redacted].
Wat je schrijft in je mail klopt globaal; twee puntjes (naarst de tekst in mijn mail)
[redacted] 11.1
Gr [redacted]

Verzonden met BlackBerry Work
(www.blackberry.com)

---

**Van:** [redacted] BD/KA <[redacted]@nctv.minjenv.nl>
**Datum:** dinsdag 05 nov. 2019 5:59 PM
**Aan:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>
**Onderwerp:** Verschil aftappen traditionele telco van PTT
Hi [redacted]
Tnx voor sessie!!
[redacted]



11.1

Verzonden met BlackBerry Work
(www.blackberry.com)

**Van:** [redacted] BD/DRC/CV
**Aan:** [redacted] BD/KS; [redacted] BD/PNDV
**Onderwerp:** RE: [redacted] ] Follow meeting
**Datum:** dinsdag 12 november 2019 08:58:15

10.2.e

10.2.a

Ah Ja ik zie het. Het staat tussen de andere belangen. Zoals je zult begrijpen zet ik het meestal front and centre =D haha. Prima zo.

11.1

**Van:** [redacted] BD/KS
**Verzonden:** dinsdag 12 november 2019 08:53
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/PNDV
**Onderwerp:** RE: [redacted] I] Follow meeting

Tnx voor je reactie [redacted]. Law enforcement stond erboven ook al; [redacted]

10.2.a

Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 11 nov. 2019 6:46 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Onderwerp:** RE: [redacted] ] Follow meeting

10.2.e

Ha [redacted],

10.2.a

Dank je! Kleine toevoeging dat naast nationale veiligheid ook de belangen van de opsporing meetellen.
Wat is [redacted]

10.2.a.

Groet,
[redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Verzonden:** maandag 11 november 2019 11:04
**Aan:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**CC:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Onderwerp:** RE: [redacted] ] Follow meeting

[redacted], sorry voor later aanleveren (cc @ [redacted] die het dossier bij DGRR houdt): [redacted] is correct, en prima zo.

10.2.a; 10.2.e

L

Hierbij bullits 'encryption"
Spreekpunten:

- NL has taken note of the Open Letter of the US, the UK and Australia to Facebook (and other Over The Top players), regarding their intention to use end-to-end encryption for facebook messenger.
- [redacted]

11.1

- NL is looking for solutions which do, preferably, not lead to taking restrictive legal measures as regards the development, availability and use of encryption in the Netherlands.

- However, we are curious as to how [redacted] deals with the issues for law enforcement? Can you explain how [redacted] has handled this problem the last years? Is it something that [redacted] is concerned with? 10.2.a.

Aandachtspunten/ inzet:

- De minister heeft in Nieuwsuur op 3 nov. Zich uitgesproken om een ontsleutelplicht te onderzoeken voor Over The Top diensten. JenV verkent nu met NL partners en internationaal het draagvlak voor regulering van deze OTT's. Een oplossing die binnen de kaders van het kabinetsstandpunt encryptie (4 januari 2016) valt verdient de voorkeur. [redacted] Evt. aanpassing van het kabinetsstandpunt vergt nadrukkelijk afstemming binnen het kabinet (i.h.b. EZK, BZK en BZ).

Bijgevoegd een intern JenV nota terzake en het standpunt ter info als bijlage.

---

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Verzonden:** donderdag 7 november 2019 11:42
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**CC:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: [[redacted]] Follow meeting 10.2.e

Hi [redacted], 10.2.a

Zie bijgaand de laatste versie van de agenda. We zijn ook druk bezig met de annotatie verder uit te werken.

Zou jij vwb encryptie nog wat punten mee willen geven? [redacted] kritische blik daarop is ook fijn! L

Grt,

[redacted]

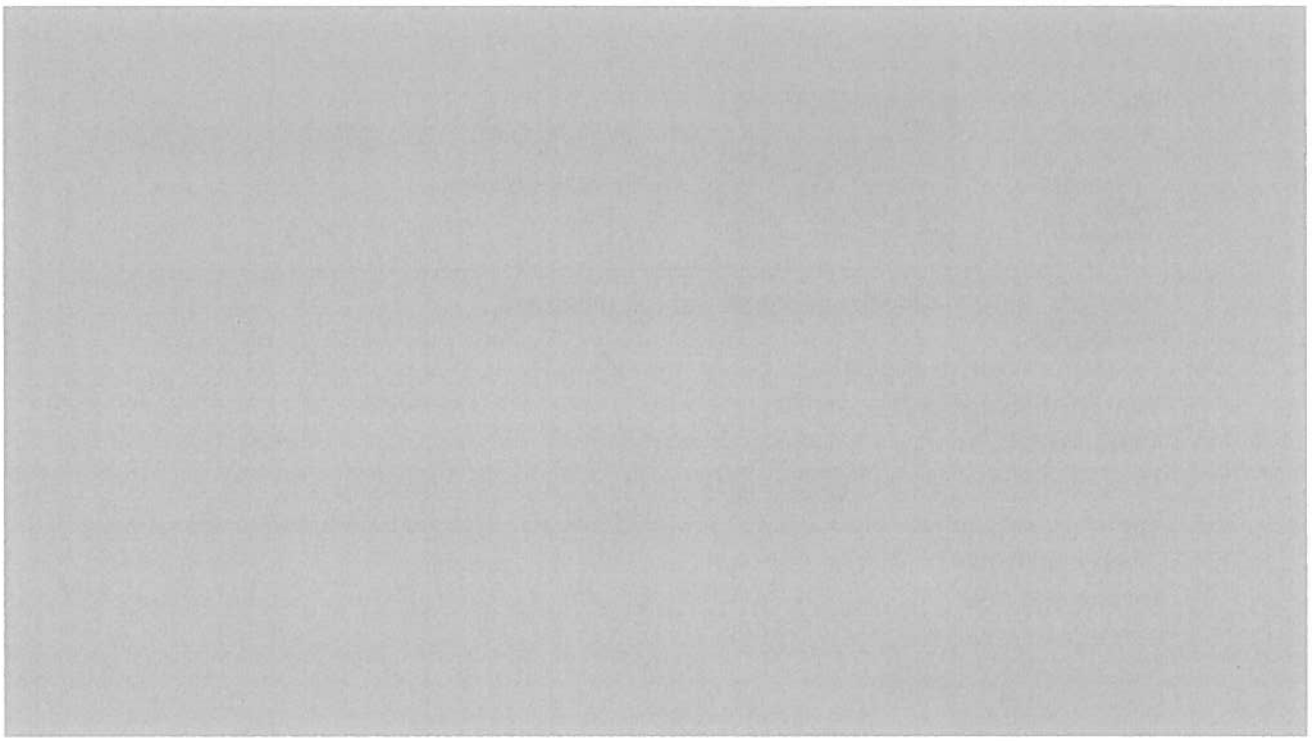
---

**Van:** [redacted]
**Verzonden:** woensdag 6 november 2019 17:35
**Aan:** [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/PNDV; [redacted] BD/NCSC/SK
**Onderwerp:** [redacted] Follow meeting

[redacted] 10.2.a

[redacted] L

[redacted] 10.2.a; 10.2.e



10.2.e

**Van:** [redacted] BD/KA
**Aan:** [redacted] BD/PNDV; [redacted] BD/PACT; [redacted] BD/KS; [redacted] BD/KA
**Onderwerp:** RE: overleg met [redacted] en [redacted] inzake inscriptie en WhatsApp
**Datum:** dinsdag 12 november 2019 15:31:29
**Bijlagen:** QTTs en Encryptie-v0e.pdf

---

Collega's, hierbij aangepaste versie van de mindmap,.
Gr, [redacted]
-----Oorspronkelijke afspraak-----
**Van:** [redacted] BD/NCTV
**Verzonden:** donderdag 7 november 2019 10:56
**Onderwerp:** overleg met [redacted] en [redacted] inzake inscriptie en WhatsApp
**Tijd:** woensdag 13 november 2019 14:00-14:30 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
**Locatie:** N06.159
**Met vriendelijke groet,**

[redacted] *van Patricia Zorko (plv. NCTV, Directeur Cyber Security en Statelijke Dreigingen) en Simone Smit (Directeur Contraterrorisme)*

.....
**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950| 2500 BZ | Den Haag
.....
**T: 070-[redacted]**
**M: 0031 6 [redacted]**
[redacted]@nctv.minjenv.nl

**Van:** [redacted]
**Aan:** [redacted] BD/KS
**Cc:** [redacted] BD/KS
**Onderwerp:** RE: Facebook encryption
**Datum:** woensdag 13 november 2019 15:41:00

10.2.e

[redacted]

10.2.a

10.2.e

**From:** [redacted] BD/KS
**Sent:** 11 November 2019 13:17
**To:** [redacted]
**Cc:** [redacted] BD/KS
**Subject:** RE: Facebook encryption

10.2.e

Dear [redacted],

I believe you are already in touch with [redacted]? He is responsible for the dossier regarding encryption and law enforcement, and he is from DG RR within our Ministry. I think it would be most effective if you get in touch directly. In case you do not yet have his contact details: [redacted]@minjenv.nl.

Best wishes, [redacted]

[redacted]
Advisor cybersecurity international affairs
***Please note that my emailaddress had changed:*** [redacted]*@nctv.minjenv.nl* ***(and no longer*** [redacted]*@nctv.minvenj.nl)***

**Ministry of Justice and Security**
**National Coordinator for Security and Counter Terrorism**
Strategy Division
P.O. box 16950 | 2500 BZ | The Hague

**T** +31 6 [redacted]
[redacted]@nctv.minjenv.nl
www.nctv.nl

**Van:** [redacted]
**Datum:** vrijdag 01 nov. 2019 2:53 PM
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>, [redacted] BD/PSD <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted]
**Onderwerp:** Facebook encryption

[redacted]

10.2.a

[redacted]

10.2.a

**Van:** [redacted] BD/NCTV
**Aan:** [redacted] BD/KS
**Cc:** [redacted] BD/KS
**Onderwerp:** RE: Overleg Encryptie en OTT
**Datum:** maandag 18 november 2019 10:38:39

10.2.e

---

Prima

**Van:** [redacted] BD/KS
**Verzonden:** vrijdag 15 november 2019 17:13
**Aan:** [redacted] BD/NCTV
**CC:** [redacted] BD/KS

10.2.e

**Onderwerp:** FW: Overleg Encryptie en OTT

Hallo Patricia,

Gezien het gesprek afgelopen woensdag over end-to-end encryptie (E2EE; [redacted] is bijgepraat), wil jij hier misschien bij aansluiten, al dan niet met, of ipv mij/vervanger? Zoals je zelf al inschatte, min. is nogal daadkrachtig op deze opsporingsproblematiek, en de effectiviteit behoeft aandacht. Ik heb [redacted] hier niet eerder zelf over gesproken.

[redacted] 10.1.d

*2019 16:45-17:30*

Groet, [redacted]

**From:** [redacted] BD/DRC/CV
**Sent:** vrijdag 15 november 2019 16:54
**To:** [redacted]
**Cc:** [redacted] ; [redacted] BD/DRC/CV; [redacted] BD/DRC/CV; [redacted] BD/DBAenV/IenK; [redacted] BD/DRC/CV; [redacted] BD/KS; [redacted] BD/DBO/ADVIES; [redacted] BD/DBO
**Subject:** Overleg Encryptie en OTT

Beste [redacted],

De minister heeft verzocht om verder te spreken over encryptie en toegang tot bew[redacted] 10.2.e
via Over The Top-dienstverleners. Zou je hier 45 minuten voor in de agenda van de minister willen plannen, lukt dat over twee weken?
Zou je voor dit overleg, [redacted] en mijzelf willen uitnodigen?

Alvast bedankt.

Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime

.....

**Ministerie van Veiligheid en Justitie**
**Directie Rechtshandhaving en Criminaliteitsbestrijding**
**Cybercrime unit**
Turfmarkt 147 | 2511 DP | Den Haag |
Postbus 20301 | 2500 EH | Den Haag
.....
**M** 06 [redacted]
[redacted]@minvenj.nl
www.rijksoverheid.nl/venj

.....

**Voor een veilige en rechtvaardige samenleving**

.....

**Van:** [redacted] BD/DRC/CV
**Aan:** [redacted] BD/KS
**Onderwerp:** RE: Non paper interception OTT
**Datum:** maandag 18 november 2019 16:18:01

10.2.e

Ha [redacted],
Dankjewel. Dit staat even in de koelkast met de gespreksnotitie voor de minister op encryptie en OTT en [redacted].
Zodra er weer behoefte komt aan een deelbaar stuk in de Unie kom ik weer bij je op de lijn.
Groet,
[redacted]

L

**Van:** [redacted] BD/KS
**Verzonden:** woensdag 13 november 2019 16:52
**Aan:** [redacted] BD/DRC/CV
**Onderwerp:** FW: Non paper interception OTT

Hey [redacted],
Weet niet zeker of ik deze reactie al had doorgezet? [redacted]

11.1

Gr [redacted]

**From:** [redacted] BD/NCSC/SK
**Sent:** donderdag 24 oktober 2019 10:57
**To:** [redacted] BD/PNDV; [redacted] BD/KS; [redacted] BD/PACT; [redacted] BD/KA; [redacted] BD/PACT
**Subject:** RE: Non paper interception OTT

10.2.e

[redacted]

[redacted]

NCTV

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Datum:** maandag 21 okt. 2019 10:49 PM
**Aan:** [redacted] (PaG Den Haag) [redacted]@om.nl) <[redacted]@om.nl>, [redacted]@om.nl <[redacted]@om.nl>, [redacted]@politie.nl [redacted]@politie.nl>, [redacted]. - BD/PIDS <[redacted]@minjenv.nl>, [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Kopie:** [redacted] Parket-Generaal) [redacted]@om.nl)' [redacted]@om.nl) [redacted]@om.nl>, [redacted]@om.nl [redacted]@om.nl>

10.2.e.

**Onderwerp:** Non paper interception OTT

Hallo allemaal,

Zoals jullie weten heeft de minister het akkoord gegeven om bij enkele lidstaten te inventariseren of zij interesse hebben in Europese regelgeving rond het kunnen aftappen van OTT's.

In overleg met de internationale directie heb ik een non-paper gemaakt. Dit paper stelt haar in staat om te inventariseren bij een beperkte groep LS om te bezien of zij ook oren hebben naar een Europese regeling om OTT's af te tappen.

Een non-paper zou de probleemstelling, context en oplossingsrichting duidelijk moeten maken.

Ik heb dit geprobeerd in bijgevoegde non-paper, zouden jullie er eens naar willen kijken? Brengt dit paper de noodzaak duidelijk genoeg naar voren? Ik verspreid het paper bewust nog even onder de JenV organisaties, dus verspreid h'm svp niet.

Groeten,

[redacted]

Met vriendelijke groet,

10.2.e

[redacted]
Beleidsadviseur cybercrime
**M** 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] - BD/PNDV
**Aan:** [redacted] - BD/KA
**Cc:** [redacted] - BD/KS; [redacted] - BD/PNDV; [redacted] BD/NCSC/SK; [redacted] - BD/NCSC/SK
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook
**Datum:** maandag 18 november 2019 17:53:01

10.2.e

Hallo [redacted],
Veel dank voor de snelle reactie! ik heb het gedeeld met DGRR. Dergelijke vraagstukken zullen ongetwijfeld nader worden onderzocht nog in de komende trajecten.
Groet,
[redacted]

10.2.e

**Van:** [redacted] BD/KA
**Verzonden:** maandag 18 november 2019 17:27
**Aan:** [redacted] BD/PNDV
**CC:** [redacted]. - BD/KS ; [redacted] - BD/PNDV ; [redacted] - BD/NCSC/SK ; [redacted] - BD/NCSC/SK
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken Barr Encryptie en Facebook

10.2.e

Hi [redacted]

[redacted]

11.1

[redacted]

Gr, [redacted]
PS. [redacted] is met verlof. Met dank aan [redacted] voor de inhoudelijke input; alle fouten die hier boven staan zijn van mij.

10.2.e

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 15:57
**Aan:** [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] BD/KA <[redacted]@nctv.minjenv.nl>
**CC:** [redacted] - BD/KS <[redacted]>; [redacted] - BD/PNDV <[redacted]@nctv.minjenv.nl> 10.2.e
**Onderwerp:** FW: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook [redacted],
Zie bijgevoegd conceptnotitie voor MinJenV voor zijn bezoek aan Washington. [redacted] 11.1
De diagrammen op de laatste twee pagina's hebben wel even jullie aandacht nodig. Hoe zien jullie die? Ik heb niet voldoende kennis van de techniek om die te kunnen beoordelen.
Reactietijd richting DGRR is morgenochtend. Als jullie gekke dingen zien, kun je het laten weten? Dan kan ik ze meegeven in reactie richting DGRR.
Groet,
Tom

**Van:** [redacted] - BD/DRC/CV [redacted]@minjenv.nl>
**Verzonden:** maandag 18 november 2019 14:58
**Aan:** [redacted] - BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] - BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] - BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] - BD/PNDV <[redacted]@nctv.minjenv.nl> 10.2.e
**CC:** [redacted] - BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] - BD/DEIA/IBP [redacted]@minjenv.nl>
**Onderwerp:** Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook
Hallo allen,
Hierbij een voorstel voor het werkbezoek van de minister.
[redacted]
Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
[redacted]@minvenj.nl

10.2.e

**Van:**
**Aan:** BD/KS
**Cc:** BD/NCTV
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken Encryptie en Facebook
**Datum:** dinsdag 19 november 2019 16:59:16

10.2.e

Dankjewel ik zal het in IBABS zetten voor Patricia
**Met vriendelijke groet,**

*Managementassistent van Patricia Zorko (plv. NCTV, Directeur Cyber Security en Statelijke Dreigingen) en Simone Smit (Directeur Contraterrorisme)*

.....

**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950| 2500 BZ | Den Haag

.....

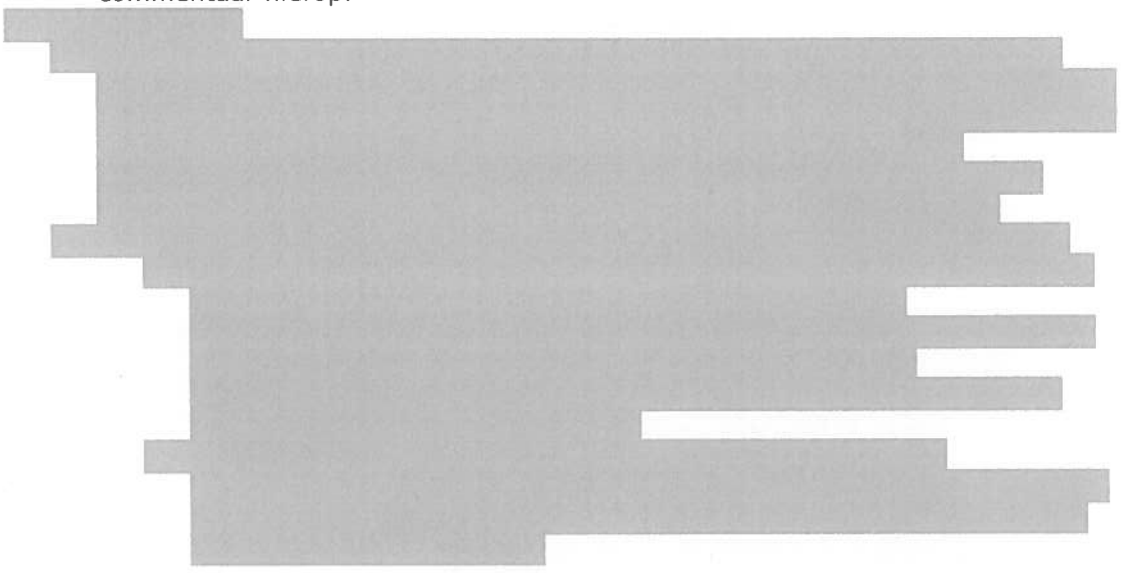
**T: 070-**
**M: 0031 6**
@nctv.minjenv.nl

**Van:** BD/KS
**Verzonden:** dinsdag 19 november 2019 15:48
**Aan:** BD/NCTV ; BD/NCTV
**CC:** BD/KS
**Onderwerp:** FW: Dossiernotitie bilaterale bezoeken Encryptie en Facebook

10.2.e

Patricia,
Tbv het gesprek met de minister as. vrijdag, hierbij een annotatie.
Voor in het dossier ter achtergrond:

1. De gespreksnota minister naar aanleiding waarvan de minister een vervolggesprek wilde;
2. De mindmap van Analyse;
3. Concept-Dossiernotitie voor Barr van DGRR met een aantal visualisaties;
4. Onderstaand commentaar van Analyse en PNDV inzake die visualisaties. DGRR zal opnieuw naar de plaatjes kijken, maar omdat ik niet zeker weet wanneer de minister deze zal ontvangen t.b.v. zijn gesprek met Barr, is het goed Patricia, dat jij op de hoogte bent van deze visualisaties, en je bewust bent van ons commentaar hierop.



[redacted]

Groet, [redacted]

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] - BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

10.2.e

Hallo [redacted],
Goed te weten dat er reeds contact is geweest. Met het oog op de krappe deadline had ik het stuk al bij de experts uitgezet. Zie bijgevoegd de reactie die ik kreeg. Zal niet heel anders zijn dan de punten van [redacted] vermoed ik, maar gezien het werk dat de collega's er op korte tijd in hebben gestoken stuur ik het bij deze ter info door. [redacted]

Groet,

[redacted]

11.1

[redacted] zal maken van een niet-openbare OTT-dienst (gezien de eenvoud van uitrol)

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 18 november 2019 16:17
**Aan:** [redacted] BD/PNDV ; [redacted] BD/KS ; [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**CC:** [redacted] BD/DEIA/IBP ; [redacted] BD/DEIA/IBP 10.2.e
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

Ha [redacted],
Weet dat [redacted] eerder contact heeft gehad met [redacted] over de non-paper. [redacted]. Juist vanwege het bestaan van verschillende optieken wordt nut, noodzaak en haalbaarheid onderzoc 11.1

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 16:11
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] - BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl> 10.2.e
**CC:** [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

Hallo [redacted],
We zullen op tijd reageren. [redacted]; zie enkele verwijderde typo's in de bijlage.
De diagrammen kan ik zelf niet beoordelen; kijkt een expert nog even naar. 11.1
Groet,
[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** maandag 18 november 2019 14:58
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl> 10.2.e
**CC:** [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>
**Onderwerp:** Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

Hallo allen,
Hierbij een voorstel voor het werkbezoek van de minister.

[redacted] 11.1

Met vriendelijke groet,

[redacted]
Beleidsadviseur cybercrime
**M** 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KS
**Cc:** [redacted] BD/PNDV; [redacted] BD/PNDV
**Onderwerp:** FW: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook 10.2.e
**Datum:** dinsdag 26 november 2019 13:35:07
**Bijlagen:** RE advies .msg
Dossiernotitie bilaterale bezoeken [redacted] incl visualisaties conceptversie 20191118.doc
MindmapOTTs en Encryptie-v0e.pdf 10.2.a

Hoi,
Over VS: Ik zag dat dgrr al input voor encryptie heeft geleverd voor de minister; is eerder afgestemd en prima. Wel handig om voor het dossier van Patricia de inhoud van bijgevoegd mailtje hieronder en de bijlagen nog "extra" in haar eigen dossier te voegen. [redacted] 11.1

Gr [redacted]

[redacted]
NCTV
[redacted]

**Van:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Datum:** dinsdag 19 nov. 2019 3:48 PM
**Aan:** [redacted] BD/NCTV <[redacted]@nctv.minjenv.nl>, [redacted] BD/NCTV <[redacted]@nctv.minjenv.nl> 10.2.e
**Kopie:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>
**Onderwerp:** FW: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook 10.2.a

[redacted] Patricia,
Tbv het gesprek met de minister as. vrijdag, hierbij een annotatie.
Voor in het dossier ter achtergrond:

1. De gespreksnota minister naar aanleiding waarvan de minister een vervolggesprek wilde;
2. De mindmap van Analyse;
3. Concept-Dossiernotitie voor Barr van DGRR met een aantal visualisaties;
4. Onderstaand commentaar van Analyse en PNDV inzake die visualisaties. DGRR zal opnieuw naar de plaatjes kijken, maar omdat ik niet zeker weet wanneer de minister deze zal ontvangen t.b.v. zijn gesprek met Barr, is het goed Patricia, dat jij op de hoogte bent van deze visualisaties, en je bewust bent van ons commentaar hierop.

[redacted] 11.1

[redacted]

11.1

Groet, [redacted]

**Van:** [redacted] BD/PNDV
**Verzonden:** maandag 18 november 2019 17:38
**Aan:** [redacted] BD/DRC/CV ; [redacted] BD/KS ; [redacted] - BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**CC:** [redacted] BD/DEIA/IBP ; [redacted] BD/DEIA/IBP
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

10.2.e

Hallo [redacted],

10.2.a

Goed te weten dat er reeds contact is geweest. Met het oog op de krappe deadline had ik het stuk al bij de experts uitgezet. Zie bijgevoegd de reactie die ik kreeg. Zal niet heel anders zijn dan de punten van [redacted] vermoed ik, maar gezien het werk dat de collega's er op korte tijd in hebben gestoken stuur ik het bij deze ter info door. [redacted].

Groet,

11.1

[redacted]

[redacted]

11.1

[redacted]

[redacted]

**Van:** [redacted] BD/DRC/CV
**Verzonden:** maandag 18 november 2019 16:17
**Aan:** [redacted] BD/PNDV ; [redacted] BD/KS ; [redacted] BD/DRC/CV ; [redacted] BD/DBAenV/IenK
**CC:** [redacted] BD/DEIA/IBP ; [redacted] BD/DEIA/IBP
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

10.2.e

Ha [redacted],

10.2.a

Weet dat [redacted] eerder contact heeft gehad met [redacted] over de non-paper. [redacted]. Juist vanwege het bestaan van verschillende optieken word[redacted] noodzaak en haalbaarheid onderzocht.

11.1

**Van:** [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**Verzonden:** maandag 18 november 2019 16:11
**Aan:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] - BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>
**CC:** [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>
**Onderwerp:** RE: Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

10.2.e

Hallo [redacted]

10.2.a

We zullen op tijd reageren. [redacted] zie enkele verwijderde typo's in de bijlage.

11.1

De diagrammen kan ik zelf niet beoordelen; kijkt een expert nog even naar.

Groet,

[redacted]

**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** maandag 18 november 2019 14:58
**Aan:** [redacted] BD/KS <[redacted]@nctv.minjenv.nl>; [redacted] BD/DRC/CV <[redacted]@minjenv.nl>; [redacted] BD/DBAenV/IenK <[redacted]@minjenv.nl>; [redacted] BD/PNDV <[redacted]@nctv.minjenv.nl>
**CC:** [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>; [redacted] BD/DEIA/IBP <[redacted]@minjenv.nl>
**Onderwerp:** Dossiernotitie bilaterale bezoeken [redacted] Encryptie en Facebook

10.2.a

Hallo allen,

Hierbij een voorstel voor het werkbezoek van de minister.

[redacted]

11.1

Met vriendelijke groet,

[redacted]

Beleidsadviseur cybercrime
M 06 [redacted]
[redacted]@minvenj.nl

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/NCTV
**Onderwerp:** RE: advies
**Datum:** dinsdag 19 november 2019 14:46:35
**Bijlagen:** RE Overleg Encryptie en OTT.msg
Gespreksnota tbv minister door DGRR definitief 20191119.docx

10.2.e

---

Is met patricia afgestemd (zie emailbijlage), ze is afgelopen week bijgepraat en ze zal aansluiten bij minister. Gespreksnotitie voor minister heeft Patricia ook al gezien, hierbij de final version die minister dus wilde bespreken.
Gr [redacted]

**Van:** [redacted] BD/NCTV
**Verzonden:** dinsdag 19 november 2019 13:47
**Aan:** [redacted] BD/KS
**Onderwerp:** advies
**Urgentie:** Hoog

[redacted],
Mag ik advies van je hebben voor Patricia. die is uitgenodigd samen met jou om naar de minister te gaan. [redacted]: Encryptie en OTT
**Met vriendelijke groet,**

[redacted]

*Managementassistent van Patricia Zorko (plv. NCTV, Directeur Cyber Security en Statelijke Dreigingen) en Simone Smit (Directeur Contraterrorisme)*

**Ministerie van Justitie en Veiligheid**
**Nationaal Coördinator Terrorismebestrijding en Veiligheid**
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950| 2500 BZ | Den Haag

**T: 070-**[redacted]
**M: 0031 6** [redacted]
[redacted]@nctv.minjenv.nl

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KA; [redacted] BD/PNDV; [redacted] BD/NCSC/SK; [redacted] BD/PACT
**Onderwerp:** RE: Voorbespreking NCTV/NCSC-vertegenwoordiging encryptie
**Datum:** woensdag 4 december 2019 09:29:42

10.2.e

---

Klopt helemaal, dank je. Geen aanvullingen.
Groet,
[redacted]

**Van:** [redacted] BD/KA
**Verzonden:** woensdag 4 december 2019 09:13
**Aan:** [redacted] BD/KS ; [redacted] BD/PNDV ; [redacted] BD/NCSC/SK ; [redacted] BD/PACT
**Onderwerp:** RE: Voorbespreking NCTV/NCSC-vertegenwoordiging encryptie
Beste allemaal, in het bijzonder [redacted] (vanwege niet aanwezig kunnen zijn),

Afgesproken dat:

- Dossiereigenaar in principe [redacted] (gezien historie met dit onderwerp)
- Indien nodig vervangt bijvoorbeeld [redacted]
- Inhoudelijk input vanuit [redacted]

10.2.e

Specifiek voor de 10e: [redacted] afwezig, dus [redacted] gaat naar de sessie samen met [redacted] en [redacted]
Hebben jullie aanvullingen/verbeteringen op bovenstaande?
Gr, [redacted]
-----Oorspronkelijke afspraak-----
**Van:** [redacted] BD/KA
**Verzonden:** woensdag 27 november 2019 13:27
**Aan:** [redacted] BD/KA; [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/NCSC/SK; [redacted] BD/PACT
**Onderwerp:** Voorbespreking NCTV/NCSC-vertegenwoordiging encryptie
**Tijd:** dinsdag 3 december 2019 11:30-12:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
**Locatie:** Statafel op de 7e/zoeken we een zaaltje
Op verzoek van [redacted] verzet naar 11:30, Gr [redacted]
Collega's,
Nav de mail van [redacted], hierbij afspraakverzoek om voor te bespreken hoe we de rolverdelingen het beste kunnen inregelen.

Gr, [redacted]
---
Hoi,
Ivm mijn vertrek naar [redacted] zou ik jullie willen vragen om dit dossier voorlopig even waar te nemen. Mijn functie binnen strategie (incl dit dossier) moet nog worden opgevuld (vacature). Afgelopen vrijdag heeft de minister nav overleg met DGRR en mij toegezegd dat hij openstaat voor andere oplossingen dan de ontsleutelplicht. DGRR zal komend half jaar nemen voor verdere inventarisatie, en met name bij likeminded landen uitvragen naar hun oplossingen. Daarnaast zullen zij de kabinetsstandpunt-partners geinformeerd houden. Daarom stuur ik dit bericht aan jullie door zodat jullie (of een NCTV vertegenwoordiger) kan aansluiten bij dit overleg.
Hartelijke groet, [redacted]

10.2.e

10.2.e

-----Oorspronkelijke afspraak-----
**Van:** [redacted] BD/DRC/CV <[redacted]@minjenv.nl>
**Verzonden:** dinsdag 26 november 2019 16:12
**Aan:** [redacted] BD/DRC/CV; [redacted]@minbuza.nl); [redacted] [redacted] BD/PNDV; [redacted] BD/DRC/CV; [redacted] BD/DRC/CV; [redacted]

BD/DRC/CV; [redacted]@minezk.nl); [redacted]@minbzk.nl; [redacted] - BD/DGPenV/PPBT; [redacted]

**CC:** [redacted]@minbzk.nl); [redacted] - BD/KS; [redacted]@minezk.nl)

**Onderwerp:** Encryptie

**Tijd:** dinsdag 10 december 2019 09:30-10:30 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.

**Locatie:** Turfmarkt 147 - N22-02 (Vlielandzaal)

Beste collega's,

Naar aanleiding van de uitspraken van Minister Grapperhaus over encryptie in Nieuwsuur op 3 november jl. en de antwoorden op Kamervragen van 15 november jl. zou ik graag met jullie van gedachten wisselen over mogelijke oplossingen voor de uitdagingen die encryptie biedt voor de opsporing en de I&V-diensten. We streven daarvoor naar oplossingen die binnen het Kabinetsstandpunt van 2016 mogelijk zijn.

[redacted] 11.1 10.2.g 10.2.c

Graag hoor ik wie van jullie aanwezig kan zijn ivm de aanmeldingen. Mocht ik iemand anders moeten benaderen, dan hoor ik het ook graag.

Met vriendelijke groet,

[redacted]

Ministerie van Justitie en Veiligheid
Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
M 06-[redacted]
[redacted]@minjenv.nl

10.2.e

**Van:** [redacted] BD/KS
**Aan:** [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/PNDV; [redacted] BD/KBV
**Cc:** [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/KS; [redacted] BD/PNDV
**Onderwerp:** overdrachtsdocument Adviseur (nationaal en internationaal) cybersecurity
**Datum:** woensdag 11 december 2019 11:43:32
**Bijlagen:** Overdracht senior adviseur internationaal cybersecurity december 2019 overdracht[redacted].docx

10.2.e

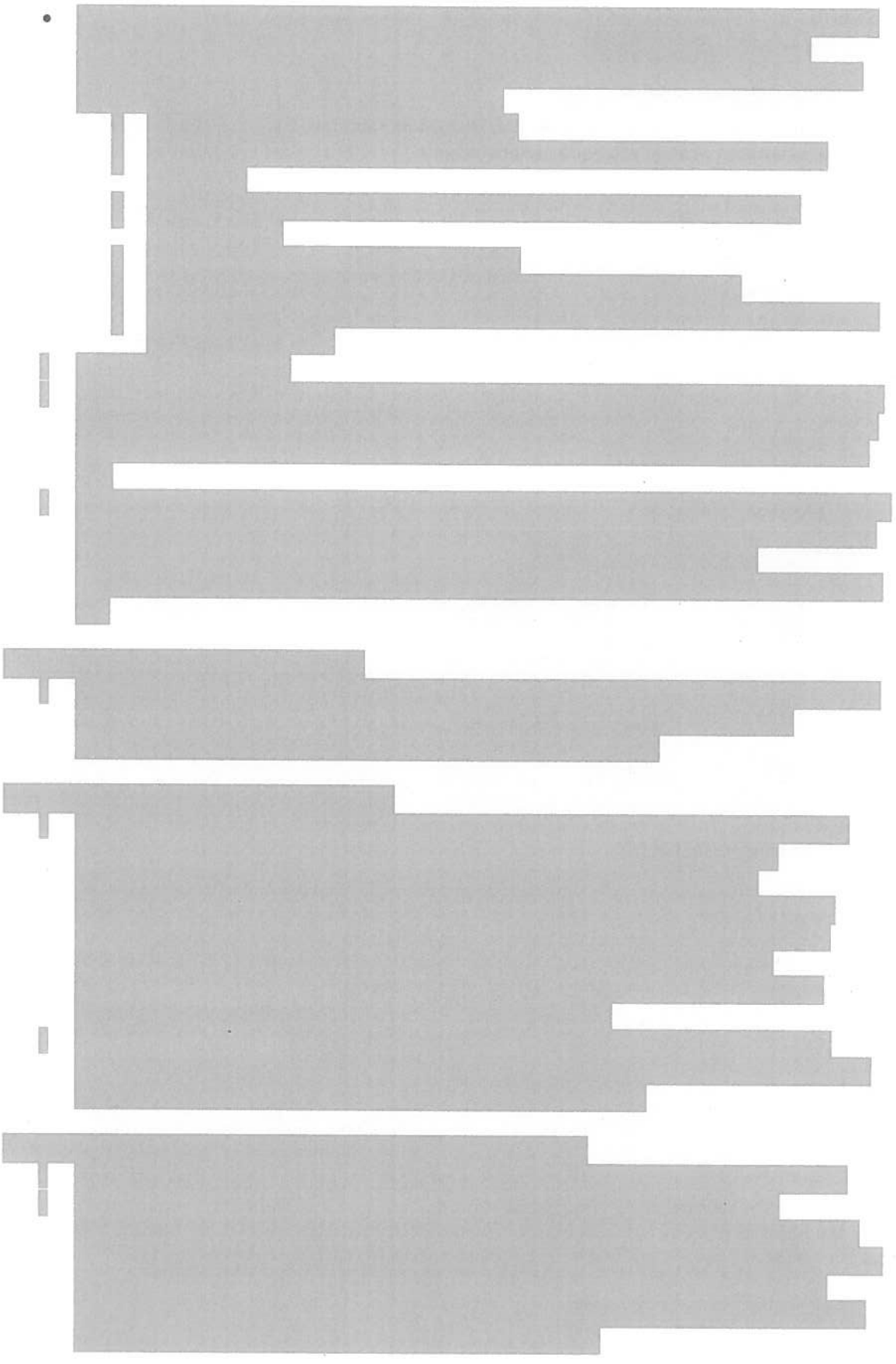
Hoi collega's,
Hierbij (dankzij de politie ;-)) nu toch een uitgebreid overdrachtsdoc. Svp NCTV intern.
Ik heb hem op de K-schijf opgeslagen onder AS/ internationaal/ coördinatie internationaal NCTV.
In groen staan de (voorlopige) dossierhouders/ achtervang genoemd, sommige thema's tot nader order even geposterioriseerd. Acties staan in geel.
Mocht er nog wat wijzigen komende week i'll keep u informed.
Gr [redacted]

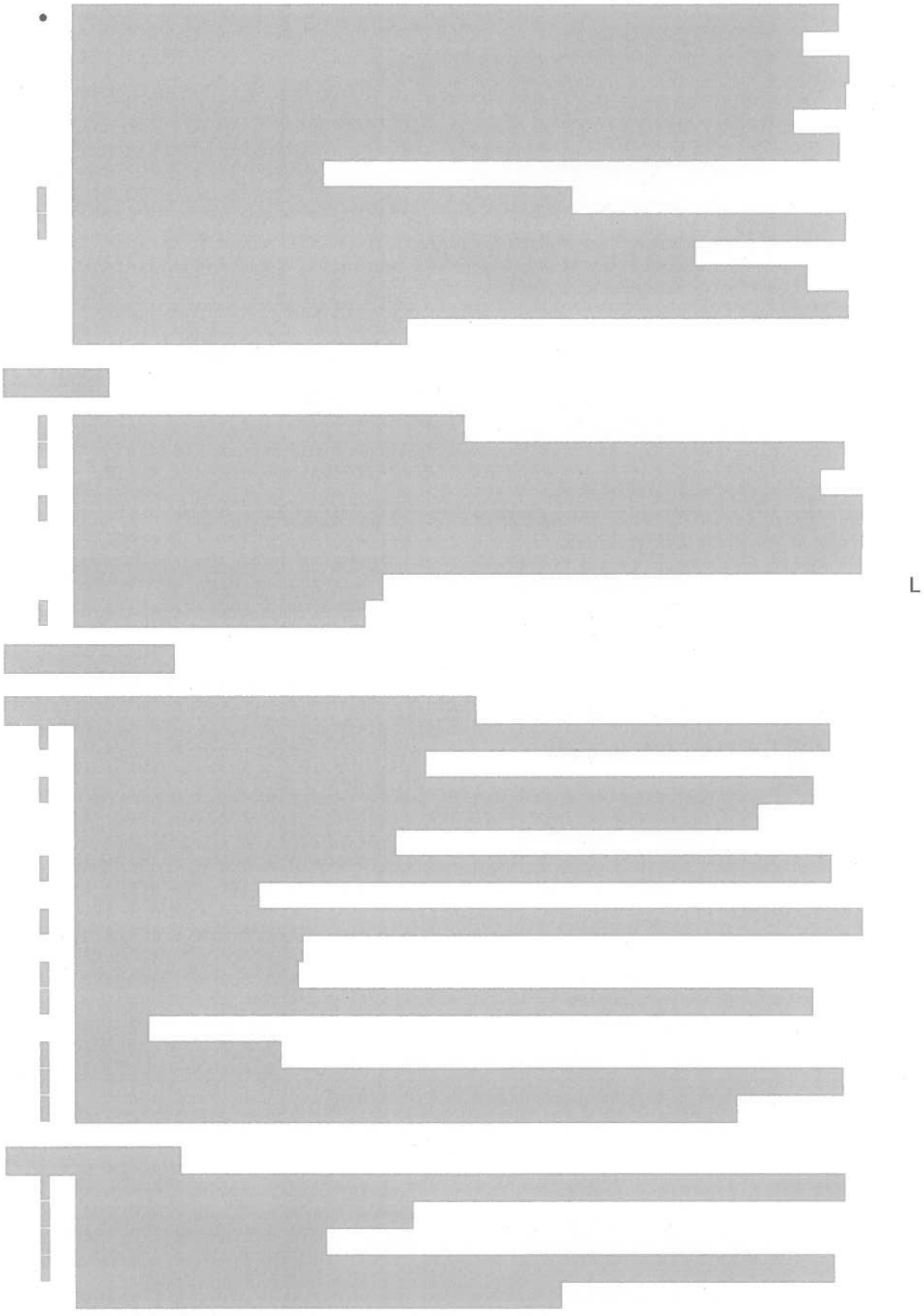
**Overdracht Internationaal adviseur bij Strategie - intern document DEP V**
**December 2019,** 10.2.e

**1. KLUIS stukken (hardcopies)**

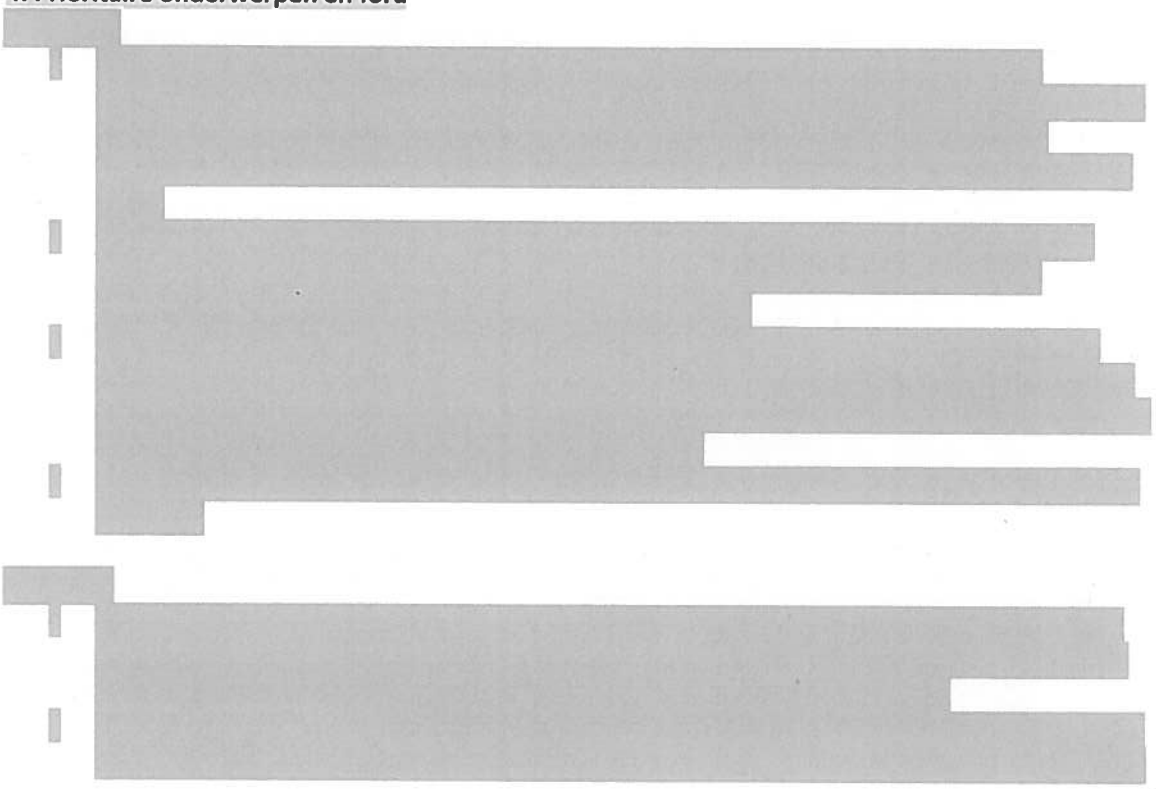
I.k.v. een "goede archivering" ;-), in de KES-kluis op de kamer van ( zitten een aantal hardcopy stukken over de volgende onderwerpen: 10.2.e 10.1.b

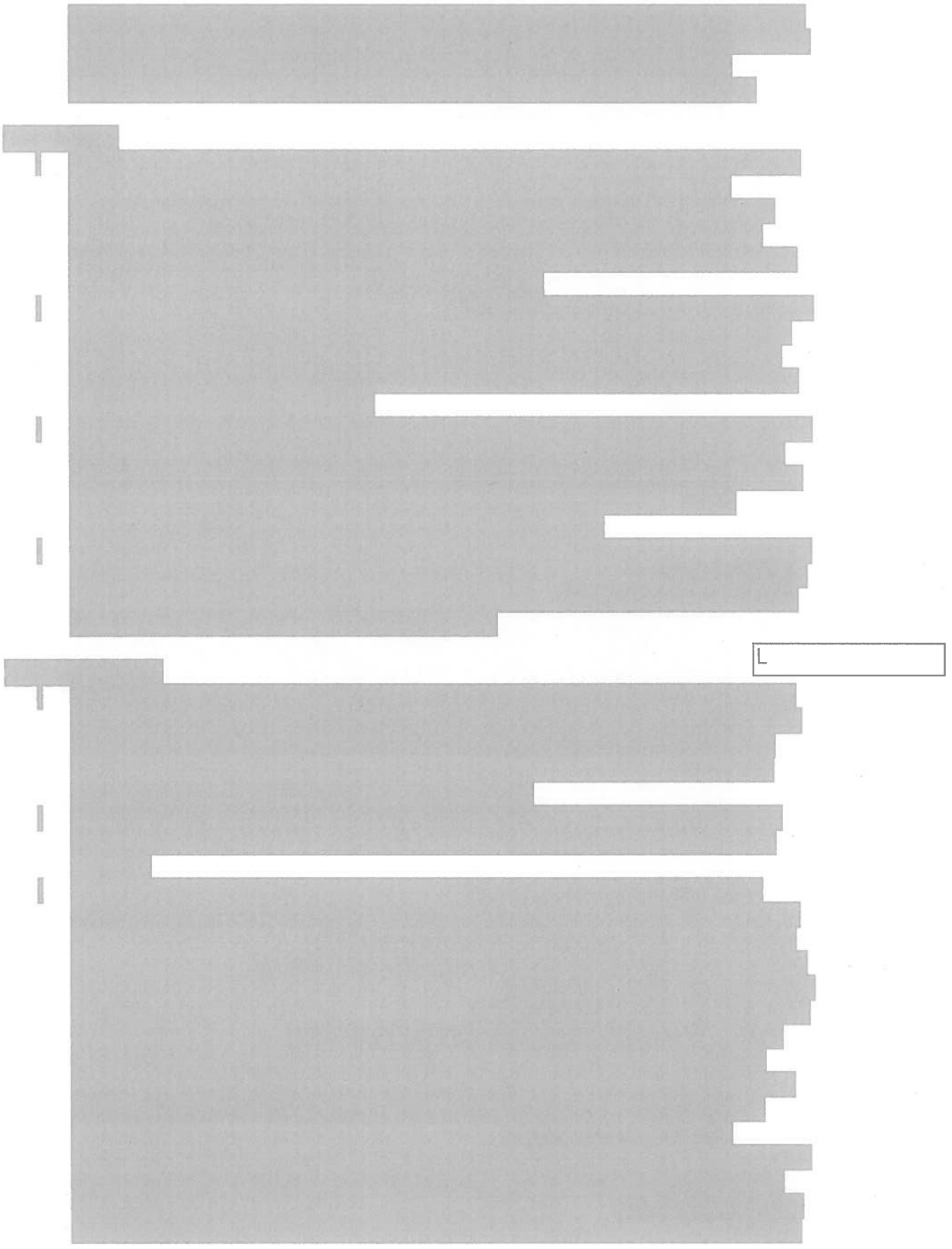
- 
- **@ encryptie:** L
- **@ encryptie:**
- L
- **@ encryptie:** 10.2.e **/ opvolger :** Verder staat op rubri nog documentatie over encryptie, L

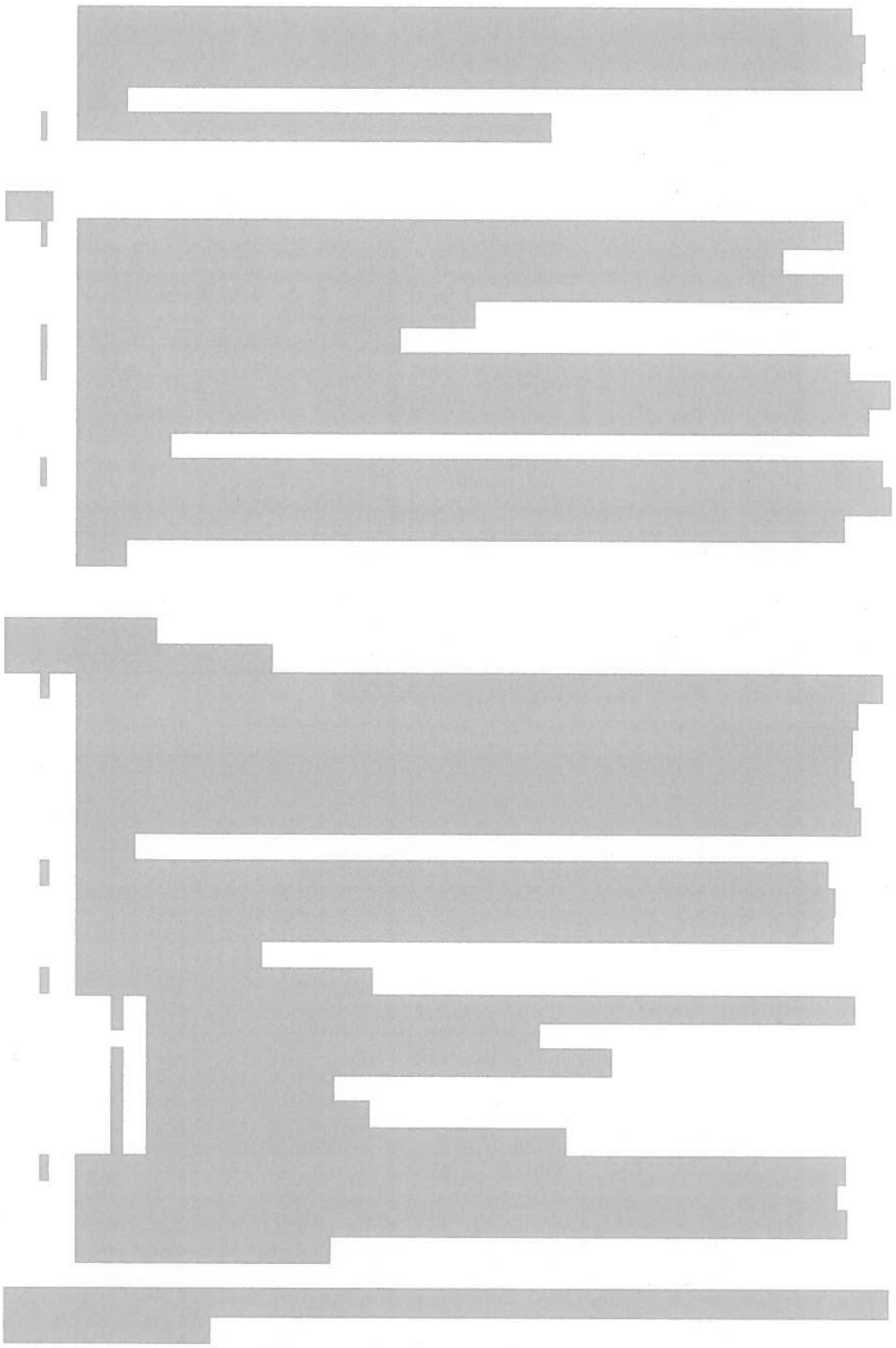




## 4. Prioritaire onderwerpen en fora







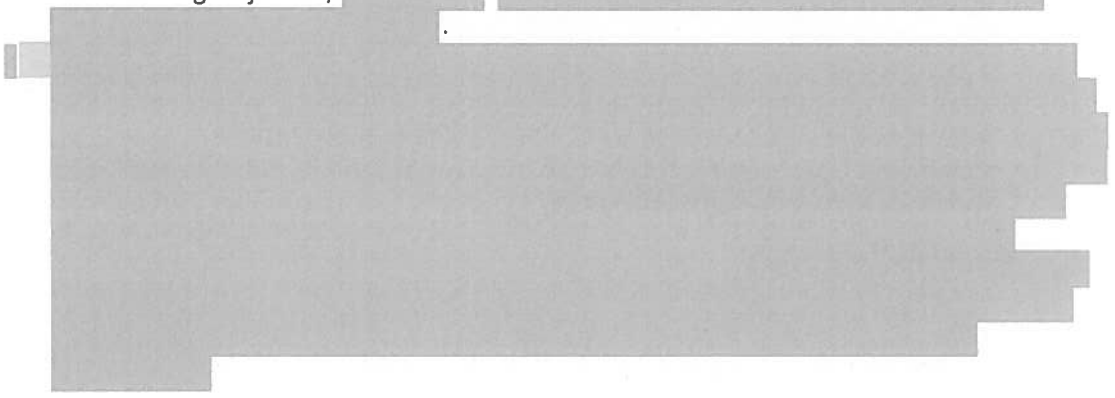
- [redacted]

L

**6. Encryptie**

**Kabinetsstandpunt encryptie -** [redacted] 10.2.e

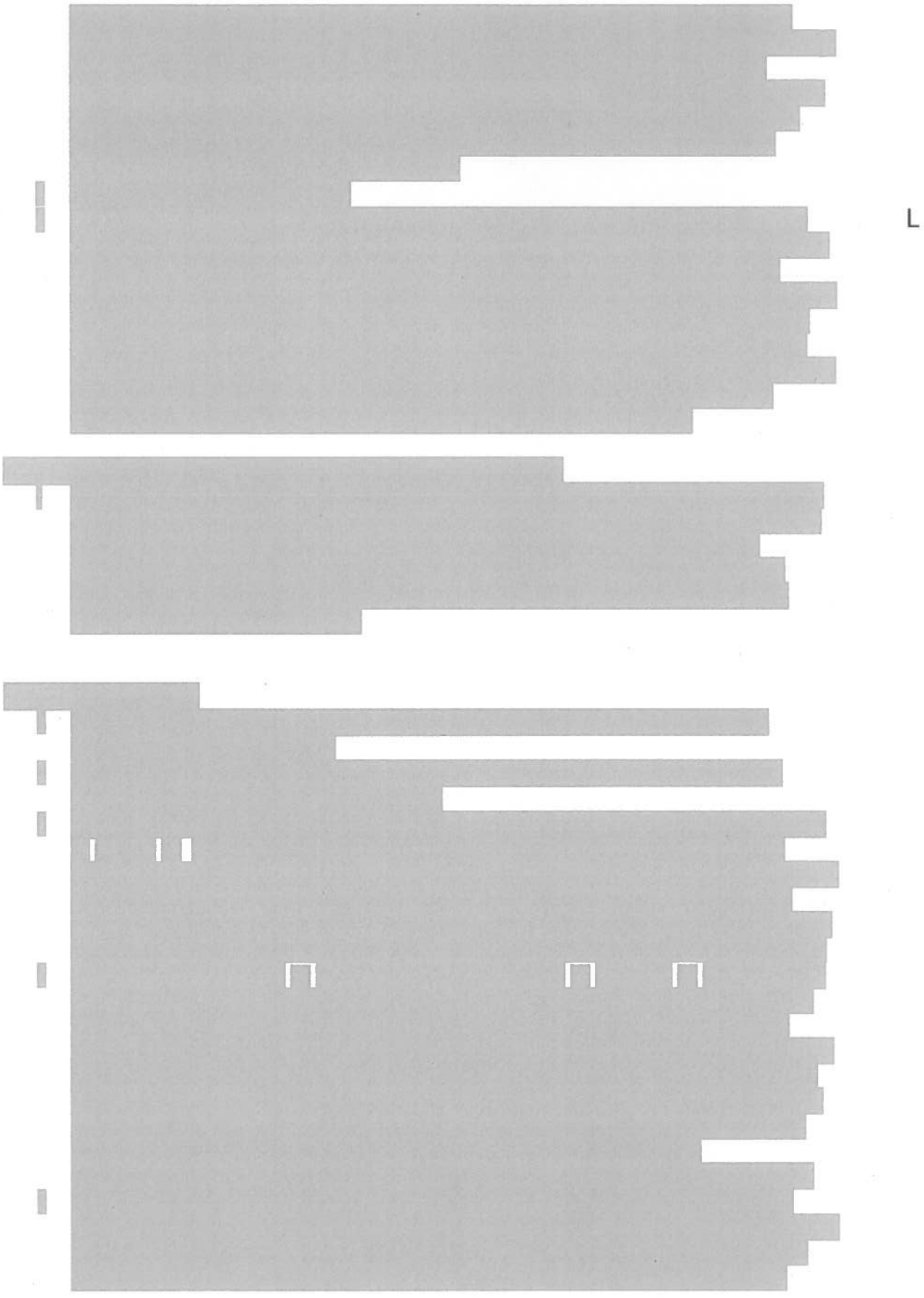
- Kabinetsstandpunt nav TK-motie op 4 januari 2016 o.l.v. NCTV tot stand gekomen (BZ, DEF, BZK, POL, OM, DGRR) en door JenV en EZK ondertekend. N.a.v. opsporingsproblematiek voor de politie rondom versleuteld verkeer en data, heeft Minister in nieuwsuur uitspraken gedaan die door TK/Verhoeven als afwijking van het kabinetsstandpunt worden beschouwd. Actueel omdat Minister naar VS gaat en VS samen met AUS en VK een oproep aan Facebook hebben gedaan om Messenger niet zomaar end-to-end te versleutelen.
- Dossier belegd bij DGRR/ [redacted]

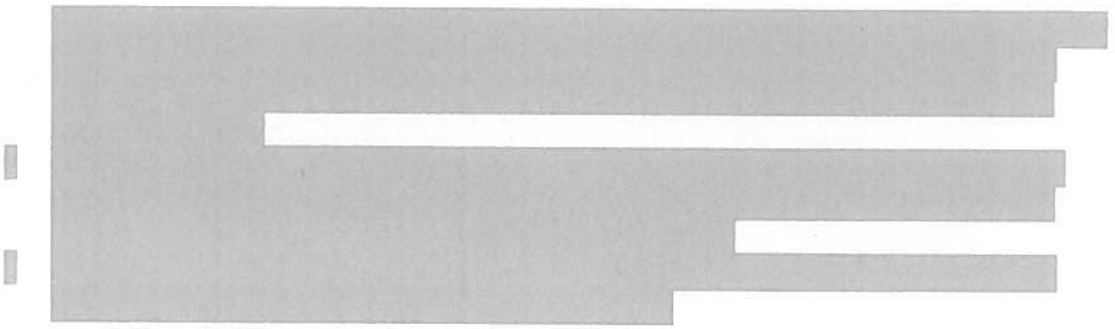


11.1

10.2.e
L

[redacted]





20200107

**Van:** [redacted] - BD/PNDV
**Aan:** [redacted] - BD/KA; [redacted] - BD/KS; [redacted] - BD/PACT; [redacted] - BD/NCSC/SK
**Onderwerp:** FW: Dossiernotitie [redacted] -Grapperhaus 16 januari
**Datum:** dinsdag 7 januari 2020 17:47:58
**Bijlagen:** Dossiernotitie bezoek [redacted] aan MinJenV 16jan2020.doc

10.2.e

10.2.a

Allen,
Volgende week donderdag spreekt de minister met [redacted] onder meer over lawful interception en encryptie. Daarvoor heeft DGRR bijgevoegde annotatie gemaakt. Doel is dat het allemaal wat hoog over blijft. Dat lukt met deze annotatie aardig, dus wat mij betreft geen aanvullingen. Als jullie hele gekke dingen zien, laat het zsm, maar op zijn laatst voor morgen (woensdag) 10.00 uur weten.
Vanuit de NCTV zal ik bij het gesprek aanschuiven.
Groet,
[redacted]

10.2.e
10.2.a

**Van:** [redacted] - BD/DRC/CV
**Verzonden:** dinsdag 7 januari 2020 16:37
**Aan:** [redacted] - BD/DEIA/IBP ; [redacted] - BD/PNDV ; [redacted] - BD/PNDV ; [redacted] - BD/DRC/CV ; [redacted] BD/DRC/CV ; [redacted] - BD/DEIA/IBP
**Onderwerp:** Dossiernotitie [redacted] -Grapperhaus 16 januari
Beste collega's, bij deze de dossiernotitie voor het gesprek tussen de minister en [redacted].
Let op: ik heb er in gezet dat deze is afgestemd met de NCTV en DEIA. Gezien de korte deadline stel ik voor dat eenieder deze doorleest en wijzigingen in tracks direct aan DEIA doorgeeft, in cc aan de rest. Dan kunnen we allemaal meekijken en snel reageren, mocht dat nodig zijn.
BVD,
[redacted]

10.2.e

10.2.a