

Van: 5.1.2.e
Verzonden: maandag 4 april 2022 14:45
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: Stand van zaken en voorgesteld proces inzake Encryptie
Bijlagen: Bijgesteld Verslag technisch-inhoudelijke werkgroep Encryptie DEF - clean.pdf

Categorieën: Categorie Rood

Van: Secretariaat CSR 5.1.2.e @cybersecurityraad.nl>
Verzonden: maandag 4 april 2022 12:21
Aan: 5.1.2.e @cybersecurityraad.nl>
Onderwerp: Stand van zaken en voorgesteld proces inzake Encryptie

Geachte leden van de raad,

Middels dit bericht breng ik u graag op de hoogte van de stand van zaken rondom de werkzaamheden van de Subcommissie Encryptie.

Aanleiding

Zoals bekend heeft de raad besloten om geen bestaande discussies of onderzoeken aangaande het verzwakken van encryptie te gaan herhalen, maar toegevoegde waarde te bieden door te kijken naar alternatieve oplossingen om rechtmatig toegang te krijgen tot versleutelde communicatie, zodat opsporings- en inlichtingendiensten hiertoe alsnog in staat gesteld worden. Om mogelijke alternatieven in kaart te brengen heeft de subcommissie een technisch-inhoudelijke werkgroep ingesteld, onder leiding van 5.1.2.e. Deze werkgroep heeft zich gebogen over de vraag *'Welke reële alternatieven zijn er om rechtmatige toegang tot end-to-end versleutelde communicatie te krijgen, anders dan verzwakking van encryptie?'*

Eindverslag technisch-inhoudelijke werkgroep

Op vrijdag 25 maart jl. is de Subcommissie Encryptie onder 5.1.2.e 5.1.2.e bijeengekomen om te spreken over het eindverslag van de technisch-inhoudelijke werkgroep. Dit eindverslag vindt u ter informatie bijgevoegd bij deze e-mail.

De werkgroep heeft zich gericht op hacken en de rol van bedrijfslogs, en een zevental aanbevelingen opgesteld.

De subcommissie heeft geconcludeerd dat het eindverslag van de werkgroep volledig is en de aanbevelingen voldoende handvatten bieden voor het opstellen van een adviesbrief aan de betrokken bewindspersonen. Hoewel bij de subcommissie bekend is dat er momenteel verschillende trajecten lopen (een tweetal onderzoeken door het WODC, een EU-questionnaire en een voorstel tot een adviescommissie voor toegang tot versleutelde communicatie), betreffen dit parallelle discussies en kunnen de aanbevelingen van de raad worden opgepakt, onafhankelijk van de uitkomsten van die trajecten.

Voorgestelde aanpak

De subcommissie stelt de volgende aanpak voor:

1. Bureau Secretaris werkt aan een eerste opzet voor de adviesbrief aan de betrokken bewindspersonen;
2. Deze adviesbrief zal na goedkeuring van het concept door de subcommissie middels een consultatieronde per mail worden voorgelegd aan de voltallige raad;
3. Het doel is om de concept adviesbrief tijdens de CSR Vergadering van 16 juni 2022 vast te stellen.
4. Overwogen kan worden om het onderwerp te agenderen tijdens de dialoog met de minister van Justitie & Veiligheid, op 16 juni a.s.

Gevraagde beslissing

Graag verneem ik van u of er nog aanvullende zaken zijn die dienen te worden meegenomen in de adviesbrief. Zo ja, dan ontvang ik deze graag uiterlijk maandag 11 april 2022, vóór 12.00 uur.

Hartelijke groet,



5.1.2.e

.....
CYBER SECURITY RAAD

p/a Nationaal Coördinator Terrorismebestrijding en Veiligheid

Turfmarkt 147 | 2511 DP | Den Haag

Postbus 20011 | 2500 EA | Den Haag | www.Cybersecurityraad.nl

.....
Telefoon: 070 5.1.2.e (secretariaat)

Mobiel: 06 5.1.2.e

E-Mail: 5.1.2.e @cybersecurityraad.nl

E-Mail: 5.1.2.e @cybersecurityraad.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

Verslag bevindingen technisch-inhoudelijk werkgroep Encryptie

Definitief vastgesteld: 25 maart 2022

Inleiding

Het onderstaande is een verslag van een ad hoc werkgroep die samen met leden **5.1.2.e** van de Cyber Security Raad (CSR) in de drie maanden Nov'21 – Jan'22 een aantal maal (online) samengekomen is. Aan deze werkgroep werd (verder) deelgenomen door:

- Twee operationeel specialisten-digitaal vanuit het Team High Tech Crime van de politie;
- Een persoon vanuit de AIVD, met een technische/beleidsmatige achtergrond;
- Een senior adviseur bij het Platform Interceptie Decryptie & Signaalanalyse (PIDS) van het Ministerie van Justitie en Veiligheid;
- Een senior beleidsadviseur bij de Directie Digitale Economie / Directoraat-Generaal Bedrijfsleven en Innovatie, Ministerie van Economische Zaken en Klimaat;
- Een Adviseur Strategie en Beleid, vanuit KPN CISO Office.

De werkgroep werd begeleid door een senior adviseur bij Bureau Secretaris van de CSR.

De vraag/opdracht waarmee de werkgroep aan de slag is gegaan luidt als volgt.

Welke reële alternatieven zijn er om rechtmatige toegang tot end-to-end versleutelde communicatie te krijgen, anders dan verzwakking van encryptie?

De werkgroep had dus nadrukkelijk *niet* de opdracht om te kijken naar mogelijkheden om encryptie te doorbreken, maar juist om alternatieven daarvoor te onderzoeken. De werkgroep heeft in een aantal interne expertsessies in de breedte naar de vraagstelling gekeken en is uitgekomen bij twee belangrijke onderwerpen: (1) **hacken**, door politie en inlichtingendiensten, en (2) **vordering van bedrijfslogs**, d.w.z. van gegevens die bedrijven verzamelen voor hun bedrijfsvoering. Dit verslag gaat, na een korte inleiding, nader in op deze twee onderwerpen en komt dan tot enkele aanbevelingen.

Wanneer in het onderstaande gesproken wordt over interceptie (tappen) van telefoonverkeer en van andere vormen van communicatie is de aanname steeds dat dit slechts plaatsvindt door de daartoe bevoegde instanties (met name: politie en inlichtingen & veiligheidsdiensten) binnen de daarvoor bestaande wettelijke kaders, met de juiste toestemmingen en de verschillende vormen van toezicht. Hetzelfde geldt voor inzet van de hackbevoegdheid. Onder deze bevoegdheid wordt een grote verscheidenheid aan activiteiten uitgevoerd. Deze variëren van het (forensisch) kopiëren van een USB-stick of harde schijf, tot het uitvoeren van een gecompliceerde hack-operatie op grote netwerken. Als er gesproken wordt over de handeling 'hacken' wordt eigenlijk altijd het op afstand binnendringen in computers bedoeld. Die interpretatie wordt hier ook gevolgd.

Het tappen is de afgelopen tientallen jaren internationaal uitgekristalliseerd, zowel technisch, als organisatorisch en juridisch. Deze (publieke) standaardisatie van interfaces en architectuur voor interceptie biedt veel voordelen: enerzijds rechtszekerheid voor burgers en anderzijds professionele duidelijkheid en uitvoerbaarheid voor de opdrachtgevers en uitvoerders. Commercieel beschikbare telecom infrastructuur omvat deze gestandaardiseerde tap functionaliteit.

Met de *end-to-end* (E2E) versleuteling van moderne, populaire *over-the-top* (OTT) berichtendiensten (zoals: Whatsapp, Signal, Telegram) is deze toegankelijkheid en overzichtelijkheid (voorgoed) verdwenen. Omdat een

heldere structuur zoals die voor het tappen van telefoons gefunctioneerd heeft niet bestaat voor OTT-diensten – en op korte en middellange termijn ook niet te verwachten is – is het belangrijk om zicht te hebben op het spectrum aan alternatieven dat voor handen is. Deze notitie heeft een technische focus en bespreekt bijv. niet de juridische alternatieven, zoals verruiming van de mogelijkheden voor online infiltratie. Deze notitie is in korte tijd tot stand gekomen, gebaseerd op zeer beperkt onderzoek, en heeft geen pretentie van volledigheid.

Overigens staat het tappen niet alleen door de beschikbaarheid van deze OTT-diensten onder druk. Ook bij de 5G infrastructuur die nu uitgerold wordt is er nog geen internationale helderheid. Door de versleuteling van signaleringsinformatie bij 5G kan een buitenlandse 5G telefoon in Nederland in beginsel niet getapt worden. Andersom bestaat dit probleem ook. Alleen in het land van herkomst kan de ontsleuteling van de signaleringsgegevens, en daarmee de tap, plaatsvinden. Om nationaal tappen van internationale telefoons wel mogelijk te maken moet in de (honderden) roamingovereenkomsten tussen telecomaانبieders afgesproken worden om deze versleuteling uit te zetten. Aanbieders staan enerzijds onder druk van hun klanten (en van de AVG) om *wel* te versleutelen en anderzijds onder druk van justitiële autoriteiten (in Europa) om *niet* te versleutelen, om internationale taps mogelijk te maken. Deze discussie loopt nog, waarbij Nederland in Europa een actieve rol speelt. Op deze discussie zelf wordt hier niet verder ingegaan.

1. Hacken

Inlichtingen & veiligheidsdiensten hebben sinds de WiV 2002 de wettelijke basis om computers (van targets) te kunnen binnendringen, ofwel rechtstreeks, ofwel indirect. De wet CC III geeft de politie sinds 2019 een vergelijkbare bevoegdheid om op afstand computers binnen te dringen. Bij de inlichtingen & veiligheidsdiensten is hacken een standaard onderdeel van de werkwijze geworden. Bij de politie is het middel nog niet zo ver ingedaald en uitgekristalliseerd (zie het rapport [Verslag toezicht wettelijke hackbevoegdheid politie 2020](#) en een nog te verschijnen rapport van het WODC). De politie heeft te maken met zwaardere beperkingen bij het uitvoeren van hacks, met name op het gebied van de tools en de kwetsbaarheden die ingezet mogen worden.

Bij hacken kan tot op zekere hoogte gebruik gemaakt worden van tools (of scripts) die ofwel aangekocht ofwel zelf opgezet zijn. De markt voor deze tools is omstreden, zie de discussie rond het Israëlische bedrijf NSO, dat nu uitgesloten is in de V.S. Zulke tools zouden hacken makkelijker kunnen maken, maar hebben als nadeel dat ze, op basis van hun uniforme werkwijze, door targets herkend kunnen worden. Ook is de effectiviteit op de langere termijn van deze tools onzeker, omdat de kwetsbaarheden waar ze nu gebruik van maken, op een goed moment onbruikbaar kunnen worden, typisch door een patch.

Hacken is voor een groot deel maatwerk en handwerk. Het middel is niet (internationaal) technisch/organisatorisch/juridisch gestandaardiseerd. De kosten zijn hoog, zowel administratief en operationeel, en de capaciteit is beperkt, waardoor de drempel hoog is. Het is bovendien niet schaalbaar: als je een twee keer zo grote hack-opbrengst wil, heb je twee keer zo veel hackers nodig.

Met hacken zijn de laatste jaren indrukwekkende resultaten behaald, zoals de ontmanteling van verschillende beveiligde communicatienetwerken van criminelen. Juist voor dit soort grote zaken, met een lange adem, is hacken een geschikt middel gebleken. Maar ook daar is de opbrengst vooraf onzeker.

Hacken kan gericht zijn op (hosting) infrastructuur en tegen de daar actieve verdachten/targets. Het hacken van mobiele telefoons is trager van de grond gekomen omdat een daarvoor geschikte uitgangspositie minder vanzelfsprekend voorhanden is. Op dit punt is verbetering voorstelbaar, via een nieuwe wettelijke en technische regeling, waarbij politie en inlichtingen & veiligheidsdiensten een betere uitgangspositie krijgen bij telecomproviders, zodat ze directe toegang hebben tot de verkeersstromen van-en-naar een specifieke telefoon. Daarbij blijft *end-2-end* versleuteling (noodzakelijkerwijs) onaantast, maar is er wel een betere toegang om via een hackoperatie op een specifiek telefoontoestel binnen te dringen.

2. Bedrijfslogs

Omdat OTT-diensten *end-2-end* versleuteld zijn hebben de bedrijven die deze diensten aanbieden zelf geen toegang tot de inhoud van de communicatie. Wel slaan ze met betrekking tot deze communicatie allerlei bedrijfsvoeringsgegevens (logs) op, o.a. voor het kunnen uitvoeren van de dienst, voor fraude-detectie, voor profilering en marketing. Het gaat dan om de identiteit van de betrokkenen, de contacten, tijdstippen, locaties, duur, omvang en aard van de berichten, etc. Ook kunnen deze bedrijven op de toestellen zelf controles uitvoeren, in hun eigen apps, en kunnen ze daar de mogelijkheid bieden tot een (versleutelde) backup van het berichtenverkeer. Wat precies bijgehouden en opgeslagen wordt is in het algemeen niet bekend.

De Nederlandse politie en inlichtingen & veiligheidsdiensten vragen met enige regelmaat gegevens op bij (vaak Amerikaanse) aanbieders van OTT-diensten. Daarbij spelen de verschillen een rol tussen de rechtssystemen van Nederland/Europa en van de V.S., en tussen de daarin gebruikte begrippen en interpretaties. In Nederland wordt gewoonlijk een onderscheid gemaakt tussen identificerende en niet-identificerende gegevens, in lijn met de AVG. In de V.S. is het onderscheid tussen inhoud en meta-data van groter belang. Deze onderscheidingen sluiten niet op elkaar aan. Zo worden locatiegegevens in Nederland als meta-data gezien, maar in de V.S. als inhoud. In de praktijk kunnen account-gegevens (geregistreerd bij het aanmaken van het account) rechtstreeks bij het bedrijf zelf opgevraagd; ze worden dan relatief snel geleverd (in de orde van weken). Andere (gebruiks)gegevens moeten via het Amerikaanse ministerie van Justitie opgevraagd worden. Die procedure duurt langer (in de orde van maanden), waarbij niet altijd alle gegevens geleverd worden. De betrokken bedrijven houden de boot nogal eens af met als verweer dat ze niet weten waar de gevraagde gegevens staan. Het merendeel van de Nederlandse opvragingen betreft daarom accountgegevens.

Onderzoekers bij politie en inlichtingen & veiligheidsdiensten zijn vaak zaak-gedreven, zonder strategisch lange-termijn perspectief. Ze zijn gewend verschillende routes te bewandelen en schakelen makkelijk over van de ene route naar de andere wanneer bepaalde opbrengst tegenvalt. Hierdoor is van gebrekkige levering van bedrijfslogs nooit een fundamentele zaak gemaakt en is er ook nog nooit een juridische procedure gestart om (snellere, uitgebreidere) levering af te dwingen. Ook is, zover bekend, niet geprobeerd om betrokken bedrijven via hun vestigingen in Nederland aan te spreken onder Nederlands recht. Hier ligt ruimte voor verbetering. Ook zou de wettelijke basis voor (internationale) vorderingen versterkt kunnen worden. Daarnaast biedt publiek-private samenwerking bij fraude-bestrijding ruimte voor een meer effectieve aanpak, inclusief hulp aan slachtoffers.

3. Aanbevelingen

1. Probeer de verminderde opbrengst van de traditionele goedgeorganiseerde telefoontaps niet op één enkele wijze op te vangen, maar bekijk het geheel, als spectrum van mogelijke alternatieve middelen.
2. Veranker en stroomlijn het hacken als opsporingsmiddel bij de politie, in lijn met het aanstaande WODC-rapport, maar erken dat hacken een hoge drempel kent, slecht schaalbaar, maatwerk is, vooral geschikt is voor grote zaken, en geen gegarandeerde opbrengst biedt.
3. Bewerkstelling in een Europees kader voor het tappen van 5G verbindingen eenzelfde transparantie, uniformiteit en rechtszekerheid als nu gangbaar is in de telecomwereld.
4. Onderzoek de mogelijkheid van een transparante wettelijke regeling voor versterkte toegang bij telecomproviders, teneinde een betere uitgangspositie te hebben om specifieke mobiele telefoons te kunnen hacken.
5. Dwing aanbieders van online diensten tot nauwere samenwerking en levering van bedrijfsvoeringsgegevens (logs). Dit kan op korte termijn via jurisprudentie en op langere termijn via (internationale) wetgeving.
6. Benader deze vordering van gegevens meer vanuit Nederlands/Europees perspectief, om interpretatiekwedsties onder Amerikaans recht te vermijden. Mogelijke aanknopingspunten zijn hierbij: de

Nederlandse/Europese vestigingen van de betrokken bedrijven en ook de eigen Europese kijk op gegevens, waarbij de zeggenschap bij data-subjecten ligt en niet bij verwerkende organisaties.

7. Organiseer nauwere publiek-private samenwerking met de fraude-afdelingen van deze leveranciers van diensten in de informatiesamenleving. Benadruk hierbij de maatschappelijke zorgplichten die grote ICT-partijen hebben.

Van: 5.1.2.e
Verzonden: dinsdag 24 mei 2022 21:31
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: Akkoord/Aanvulling gevraagd: CONCEPT CSR Adviesbrief encryptie - deadline maandag 31 mei, 10:00 uur
Bijlagen: CONCEPT Adviesbrief_over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie anders dan inperking van encryptie _versie 4.2 geredigeerd.docx; Eindverslag technisch-inhoudelijke werkgroep_reële alternatieven voor encryptie.pdf

Categorieën: Categorie Rood

5.1.2.e ,

Mochten wij input hebben, kunnen jullie dit dan via 5.1.2.e aan 5.1.2.e geven ter verzending?

Gr 5.1.2.e

Van: Secretariaat CSR 5.1.2.e @cybersecurityraad.nl>
Verzonden: dinsdag 24 mei 2022 13:35
Aan: 5.1.2.e @nl.ibm.com' 5.1.2.e @nl.ibm.com>; 5.1.2.e @cs.ru.nl' 5.1.2.e @cs.ru.nl>; 5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @politie.nl; 5.1.2.e @minjenv.nl>; 5.1.2.e @cybersecurityraad.nl>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @cybersecurityraad.nl>
CC: 5.1.2.e @om.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @cybersecurityraad.nl>; Secretariaat CSR 5.1.2.e @cybersecurityraad.nl>; 5.1.2.e @nldigital.nl>; 5.1.2.e @ibm.com>; 5.1.2.e @nl.ibm.com' 5.1.2.e @nl.ibm.com>; 5.1.2.e @cs.vu.nl' 5.1.2.e @cs.vu.nl>; 5.1.2.e @cs.ru.nl' 5.1.2.e @cs.ru.nl>; 5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>; 5.1.2.e @tudelft.nl' 5.1.2.e @tudelft.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minbzk.nl>; 5.1.2.e @minbzk.nl' 5.1.2.e @minbzk.nl>; 5.1.2.e @politie.nl>; 5.1.2.e @politie.nl' 5.1.2.e @politie.nl>; 5.1.2.e @nctv.minjenv.nl>; secretariaat.teamMT 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>; 5.1.2.e @kpn.com>; 5.1.2.e @kpn.com' 5.1.2.e @kpn.com>

Onderwerp: Akkoord/Aanvulling gevraagd: CONCEPT CSR Adviesbrief encryptie - deadline maandag 31 mei, 10:00 uur

Geachte leden van de subcommissie Encryptie,

Bijgevoegd stuur ik u het concept van de CSR Adviesbrief 'over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie', ter akkoord en/of aanvulling. Dit concept is afgestemd met en akkoord bevonden door 5.1.2.e 5.1.2.e 5.1.2.e en 5.1.2.e 5.1.2.e

Vanwege de complexiteit van de thematiek en de verschillende belangen, verzoek ik u om in het geval van wijzigingsvoorstellen daartoe *concrete tekstvoorstellen* aan te leveren.

Graag verneem ik in antwoord op deze e-mail uw akkoord of eventuele wijzigingsvoorstellen vóór maandag 31 mei, 10.00 uur.

Vervolgproces

- Eventuele voorgestelde wijzigingen zullen door Bureau Secretaris (in afstemming met 5.1.2.e [redacted]) worden verwerkt in een nieuw, definitief concept.
- Het definitief concept zal ter akkoord worden rondgestuurd aan de voltallige raad, het streven is dit te doen op 31 mei.
- Indien het haalbaar is om de Adviesbrief op 16 juni as. aan te bieden aan minister Yesilgöz-Zegerius van Justitie en Veiligheid, dan doen we dat. Zo niet, dan zal er gezocht worden naar een goed moment om dat te doen.

Hartelijke groet,



5.1.2.e [redacted]
[redacted]
.....

CYBER SECURITY RAAD
p/a Nationaal Coördinator Terrorismebestrijding en Veiligheid

Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag | www.Cybersecurityraad.nl
.....

Telefoon: 070 5.1.2.e [redacted] (secretariaat)
Mobiel: 06 5.1.2.e [redacted]
E-Mail: 5.1.2.e [redacted]@cybersecurityraad.nl
E-Mail: 5.1.2.e [redacted]@cybersecurityraad.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

Van: 5.1.2.e
Verzonden: woensdag 25 mei 2022 14:06
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Akkoord/Aanvulling gevraagd: CONCEPT CSR Adviesbrief encryptie - deadline maandag 31 mei, 10:00 uur

Categorieën: Categorie Rood

Hi 5.1.2.e

Nee, wat ons betreft ok. De notie van CSR is in lijn met uitkomsten van de technische werkgroep waar ik in zat.

Steun voor brief CSR, zoeken naar alternatieven zonder aan encryptie standpunt te rommelen.

Met vriendelijke groet,

5.1.2.e
Directie Digitale Economie

T: +31-70 - 5.1.2.e
M: +31 6 - 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 24 mei 2022 21:31
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: FW: Akkoord/Aanvulling gevraagd: CONCEPT CSR Adviesbrief encryptie - deadline maandag 31 mei, 10:00 uur

Reeds beoordeeld in dit verzoek

Reeds beoordeeld in dit verzoek

Van: 5.1.2.e
Verzonden: zondag 29 mei 2022 00:57
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Doorst: NRC - aftappen OTT.docx
Bijlagen: NRC - aftappen OTT.docx

Categorieën: Categorie Rood

5.1.2.e

Zie onder en bijgaand. Best een gedetailleerd stuk, waar JenV en EZK niet zo zwart / wit tegenover elkaar staan als wellicht gedacht. Jullie inzichten en evt commentaar of achtergronden ontvang ik graag uiterlijk ma ochtend.

Thx!

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Datum: 27 mei 2022 om 22:40:56 CEST
Aan: 5.1.2.e @minezk.nl>, 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: NRC - aftappen OTT.docx

Beste 5.1.2.e

Bijgaand vertrouwelijk een (concept)artikel dat ik zojuist ontving van NRC Handelsblad. De krant gaat komende week op basis van wob's publiceren. Besprak ik van de week al even met 5.1.2.e De journalist vraagt EZK om maandag mee te lezen en eventueel commentaar of extra achtergrond aan te leveren op deze tekst. Kunnen jullie (en jullie mensen) meekijken? @5.1.2.e je wordt als 5.1.2.e ook genoemd in het artikel.

Hoor graag maandag even, hartelijke groet,

5.1.2.e

Verstuurd vanaf mijn iPhone

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Economische Zaken en Klimaat
Directie Communicatie
Bezuidenhoutseweg 73 | 2594 AC | Den Haag
Postbus 20401 | 2500 EK | Den Haag

.....
T: 06 5.1.2.e
E: 5.1.2.e@minezk.nl
www.rijksoverheid.nl/ezk

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.

Experts van het Ministerie van Justitie & Veiligheid zagen geen heil in het plan van hun voormalige minister Grapperhaus om WhatsApp en Signal af te tappen, blijkt uit interne documenten. Een achterdeurtje bouwen in chatdiensten zorgt voor meer problemen dan oplossingen.

Door onze redacteurs Marc Hijink en Rik Wassens

De Nederlandse overheid ziet geen mogelijkheid om diensten als WhatsApp ‘veilig’ af te luisteren. Het voornemen van het ministerie van Justitie en Veiligheid om mobiele netwerken af te kunnen luisteren en een achterdeur in chatdiensten te bouwen, levert volgen de eigen ambtelijke experts te veel schade op voor de hele maatschappij. Dat is de conclusie van een jarenlange zoektocht, die politiediensten toegang moest geven tot de inhoud van chatberichten.

NRC had inzage in vertrouwelijke discussies tussen experts bij de overheid, Nederlandse en buitenlandse opsporingsdiensten en de ministeries van Economische Zaken en Justitie en Veiligheid. Die documenten verkreeg NRC in het kader van de wet openbaarheid bestuur, na een aanvraag van onderzoekscollectief Lighthouse Reports.

Het ministerie van Economische Zaken en Klimaat (EZK) blokkeerde en vertraagde een wetswijziging van de Telecomwet die chatdiensten aftapbaar te maken. Dat zou WhatsApp weggagen uit Nederland, was de gedachte.

Voor ruim 12 miljoen Nederlanders is WhatsApp een belangrijk communicatiemiddel, die dikwijls telefoongesprekken en mail vervangt. Dat is een probleem bij het bestrijden van misdaad, vinden opsporingsdiensten. Want telefoongesprekken kunnen ze via een tapsysteem afluisteren (dat gebeurt in Nederland 25.000 keer per jaar) en ook e-mail is standaard niet-versleuteld. Bij chatberichten tasten opsporingsdiensten echter in het duister: daar zien alleen de gebruikers de inhoud – ook WhatsApp zelf weet niet wat er gezegd wordt. Datzelfde geldt voor Signal, Facebook Messenger en Apple iMessage.

De wereldwijde opsporingsdiensten worstelen met de opmars van zogeheten end-to-end-encryptie. Vroeger ingewikkeld, maar vrijwel overal gratis beschikbaar. Ook voor criminelen. “Dat is een groot risico voor de openbare veiligheid”, schrijven de zogeheten Five Eyes-landen (VS, Canada, VK, Australië en Nieuw-Zeeland) [in 2020](#).

Ferd Grapperhaus, de Nederlandse minister van Justitie en Veiligheid, dringt herhaaldelijk aan op onderzoek naar het [omzeilen van versleuteling](#) via een zogenaamd ‘achterdeurtje’. Grapperhaus wijkt af van het Nederlands kabinetsbeleid uit 2016, dat juist geen achterdeurtjes in diensten als WhatsApp wil: “Door een technische ingang in een encryptieproduct te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor criminelen, terroristen en buitenlandse inlichtingendiensten”

Desondanks zet minister Grapperhaus het onderzoek naar een achterdeurtje door. Hij vindt dat noodzakelijk om de stroom aan kinderporno die via Nederland verspreid wordt “af te

knippen”. Het is een onderwerp dat de minister diep heeft geraakt, sinds een bezoek aan het Team Bestrijding Kindermisbruik in Zoetermeer, in 2017.

Maar de Nationaal Coördinator Veiligheid en Terrorisme (NCTV) en het Nationaal Cybersecurity Centrum, beide onderdeel van Grapperhaus’ ministerie, vinden het geen goed idee om de beveiliging van WhatsApp te ondermijnen. Uit de overheidsdocumenten: “NCTV en NCSC zien op basis van hun expertise geen technische oplossingen, die niet communicatie via chatapps over de linie onveiliger maken.”

Met andere woorden: een achterdeurtje levert juist meer problemen op, zoals “spionage, statelijke dreigingen van partijen die interesse hebben in informatie van politici, grote verzamelingen persoonsgegevens en economische veiligheid.”

In geschreven aantekeningen vraagt een ambtenaar zich af: “Hoe voorkomen we dat (weggelakt) de Whatsapps van onze ministers meelesen? En hoe weerhouden we er (weggelakt) ervan om met deze faciliteit hun dissidenten op Nederlandse grondgebied in de gaten te houden?”

De vertraagtactiek van Economische Zaken

Voor de invoering van het 5G-netwerk krijgt Nederland een nieuwe Telecomwet. Het ministerie van Justitie en Veiligheid wil de tapplicht in WhatsApp daarin verwerkt hebben, nog voor de verkiezingen van 2021. Dat leidt tot een felle discussie met het ministerie van Economische Zaken en Klimaat, verantwoordelijk voor de telecomsector.

Economische Zaken eist een “gelijk speelveld”: als telecomoperators zoals KPN, VodafoneZiggo en T-Mobile, aftapbaar moeten zijn, dan zou dat ook voor chatdiensten moeten gelden. Tegelijkertijd wil Economische Zaken van de collega’s van Justitie bevestiging dat de gekozen aanpak niet mag leiden tot een zwakkere encryptie. Dat druist immers in tegen het kabinetsbeleid.”

Justitie reageert boos: “Vlak voor de deadline vertraging op dit fundamentele punt claimen met een niet of amper uitvoerbaar onderzoek is onprofessioneel en onnodig.”

De techsector – “de rijkste en meest geavanceerde bedrijven ter wereld” – moet zelf een oplossing verzinnen om een product te bouwen dat zowel goed beveiligd is als goed aftapbaar, vindt Justitie. “Er moet geen sprake zijn van een omgekeerde bewijslast: dat wij moeten aantonen dat aftapbaarheid veilig kan.”

In het directeurenoverleg verwijt Justitie & Veiligheid dat “Economische Zaken aan slechte en niet-tijdige beleidsvorming heeft gedaan.” “EZK weet dat het Ministerie van Justitie en Veiligheid heeft gekozen voor de aftapbaarheid diensten als WhatsApp en Signal, ook al heeft het spanning met het encryptiestandpunt van het Kabinet. Maar dat stamt uit 2016, en sindsdien is de wereld flink veranderd.”

Voor Economische Zaken spelen andere belangen. Via WhatsApp (2 miljard gebruikers) worden dagelijks 100 miljard berichten verstuurd. Eén achterdeurtje heeft gevolgen voor alle gebruikers – consumenten en bedrijven. Van Tikkie tot toeganskaartje; er bloeit een hele digitale economie op vertrouwelijk dataverkeer via chats. Die wankelt als iemand van buitenaf kan meelesen..

Economische Zaken maakt zich ook zorgen over het ‘vestigingsklimaat’ en wil zeker weten dat Nederland niet als enig Europees land een tapplicht voor appjes instelt. Facebook, eigenaar van WhatsApp, zou Nederland kunnen mijden als een achterdeurtje in de chatdienst verplicht wordt.

“We willen voorkomen dat dienstverleners zich terugtrekken en WhatsApp niet meer beschikbaar is in Nederland”, schrijft de Directoraat-Generaal Bedrijfsleven en Innovatie in oktober 2020 aan de Directie Rechtshandhaving en Criminaliteitsbestrijding van het Ministerie van Veiligheid en Justitie.

Dat argument valt niet in goede aarde. Een beleidsmedewerker van de Rechtshandhaving en Criminaliteitsbestrijding is gefrustreerd: “De discussie had door Economische Zaken veel eerder gevoerd moeten worden en kan nu van een serieuze impact zijn voor de wetgeving en opsporing. (...) Ik baal er wel van.”

Het Ministerie van Justitie en Veiligheid ziet zelf ook dat het niet lukt om voor de verkiezingen in ieder geval “een minimale variant” aan wetgeving erdoor te krijgen. Nadat in januari 2021 het kabinet demissionair is vanwege de Toeslagenaffaire, wordt de aftapplicht door de Tweede Kamer ‘controversieel’ verklaard.

In juni 2021 constateert de Directie Wetgeving en Strafrecht van Justitie en Veiligheid dat een wetsvoorstel pas kansrijk is als er eerst een technische mogelijkheid is uitgewerkt die “zowel sterke beveiliging en encryptie als toegang in specifieke gevallen (...) weet te waarborgen”.

En er zit nog een addertje onder het gras: als providers door het wetsvoorstel extra kosten moeten maken om 5G en chatdiensten aftapbaar te maken, dan moet het ministerie van Justitie en Veiligheid dat betalen. “Daarvoor is nog geen budget beschikbaar.”

EU wil chatberichten scannen

Op Europees niveau wordt nog steeds gezocht naar manieren om de chatdiensten af te tappen zonder daarbij de veiligheid van die systemen aan te tasten. Dat is ook het uitgangspunt van een [nieuwe Europese wet](#) in voorbereiding die techbedrijven verplicht chats te scannen op kinderporno.

Nederlandse experts gingen de afgelopen jaren ook te rade bij de manier waarop opsporingsdiensten in het Verenigd Koninkrijk, Duitsland, Frankrijk en België de versleutelde chatdiensten omgaan. Niemand heeft een oplossing voor een ‘veilige’ achterdeur, blijkt uit de documenten.

En zelfs als er een interceptiemogelijkheid voor chatdiensten zou komen, dan levert dat problemen op buiten de EU, waarschuwt een medewerker van Buitenlandse Zaken die over exportvergunningen gaat. “Het wordt heel lastig om bij voorbaat uit te sluiten dat technische oplossingen alleen voor het Westen ingezet zullen worden. Een vergunning buiten de EU is zeer lastig —in sommige gevallen onmogelijk — te verkrijgen, gezien het risico op mensenrechtenschendingen.”

Het alternatief voor een rechtmatige tap is de ‘onrechtmatige’ variant: hacken met bevoegdheid. Whatsapp houdt bijvoorbeeld wel metadata bij (wie spreekt met wie en wanneer). En er zijn manieren om met zulke verkeersgegevens die de drempel voor infiltratie te verlagen.

Dat worden meer gerichte aanvallen, door middel van hacks op individuele gebruikers. “Dat is arbeidsintensief en daarmee niet goed schaalbaar”, klagen de politiediensten. Bovendien zijn er veel regeltjes die hacken beperken, reden waarom opsporingsambtenaren aandringen op verruiming van hun hackmogelijkheden.

Volgens de lijstjes van WhatsApp en Facebook staat Nederland onderaan in de lijst van landen waar zulke metadata worden opgevraagd.

Hoe gaat het verder?

Ferd Grapperhaus is geen minister van Justitie en Veiligheid meer. Zijn opvolger is Dilan Yeşilgöz-Zegerius (VVD). Bij haar blijft de wens om de encryptie van chatdiensten aftapbaar maken voortleven, schrijft in eind april in een brief bij de publicatie van de Wob-stukken.

“Rechtmatige toegang tot versleutelde communicatie kan ook de veiligheid van de maatschappij en burgers verbeteren. (...). Deze eventuele interceptiebevoegdheid kan worden gebruikt voor de bestrijding van vele soorten criminaliteit.”

Maar hoe kan de minister doorzetten als haar eigen experts ervan overtuigd zijn dat een achterdeur in WhatsApp en andere chatdiensten onmogelijk is zonder schadelijke gevolgen voor de hele samenleving?

In een achtergrondstuk van juni 2021 over tapbare digitale communicatie werpen externe experts van de Cybersecurityraad een principiële vraag op. “Stel, dat dat technisch allemaal lukt en we kunnen een mondiale interceptie-infrastructuur bouwen. Is de mensheid daaraan toe? Welke landen mogen deze tap-infrastructuur voor welke delicten mogen gebruiken? Kunnen taps ingezet worden bij zaken als moord en doodslag en kinderporno, maar niet bij politiek gevoeligere beschuldigingen van terrorisme of staatsondermijnende activiteiten? Wie beheert dat? Mogen [weggelakt] er ook bij? Mag bewijs daaruit leiden tot doodstraffen?”

De aanpak van kinderporno en zware criminaliteit wordt vaak genoemd om chatdiensten tapbaar te maken. Bewijs voor de effectiviteit ontbreekt, volgens het achtergrondstuk van de Cybersecurityraad. Om die reden doet het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie onderzoek naar de impact van encryptie op de opsporing. Dat onderzoek had in april 2022 gereed moeten zijn. De Cybersecurityraad stelt in 2021 al: “Producenten en consumenten van kinderporno zullen WhatsApp zeker niet gebruiken wanneer het tapbaar is. Ze lijken meer gebruik te maken van het dark web.”

Op 16 juni publiceert Cybersecurityraad een officieel advies over de wenselijkheid van het mogen ontsleutelen van chatberichten. Hoogleraar informatiebeveiliging en CSR-lid Bart Jacobs (Radboud Nijmegen Universiteit) wil nog niet op de inhoud vooruitlopen, maar geeft aan dat het advies “het realisme alleen maar zal versterken”.

KADER

Scannen zonder achterdeur

Er zijn ook andere manieren om te controleren of iemand kinderporno in bezit heeft. Apple voerde vorig jaar nieuwe bescherming [tegen kindermisbruik](#) in.

Elke iPhone met besturingssysteem iOS 15 controleert of de gebruikers afbeeldingen met kinderporno uploaden naar opslagdienst iCloud.

Het algoritme kijkt niet naar de daadwerkelijke foto maar naar de hash, een optelsom van alle pixels vertaald in een korte digitale code. Die wordt vergeleken met een database van eerder gevonden verboden afbeeldingen. Als de gebruiker 30 afbeeldingen uploadt die overeenkomen met de verboden database, dan wordt het NCMEC (National Center for Missing & Exploited Children) gewaarschuwd.

WhatsApp werkt ook samen met NCMEC om verspreiding van afbeeldingen van kindermisbruik tegen te gaan. De versleuteling van de chat blijft daarbij intact maar WhatsApp scant wel op bekende foto's en video's van misbruikssituaties en kijkt naar profiel- en groepsfoto's en klachten van gebruikers, [aldus de chatdienst](#). Daarnaast traint WhatsApp software om verdacht gedrag te detecteren dat duidt op het delen van kinderporno.

Van: 5.1.2.e
Verzonden: maandag 30 mei 2022 11:19
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: NRC - aftappen OTT.docx
Bijlagen: 220530 NRC - aftappen OTT 5.1.2.e docx
Categorieën: Categorie Rood

5.1.2.e

Bijgaand een aantal suggesties op de tekst vh artikel vanuit mijn team. 5.1.2.e 5.2.1

Mocht je nog vragen of opmerkingen hebben, weet mij te vinden.

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 30 mei 2022 09:16
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e
 @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: NRC - aftappen OTT.docx

Goedemorgen 5.1.2.e

Dank voor heads up. Heb mijn team er al op gezet.

Na mijn eigen eerste lezing blijf ik vooral steken bij de passage vooraan in het artikel dat EZK heeft geblokkeerd en vertraagd omdat anders Whatsapp zou worden weggejaagd uit NL. Geeft indruk alsof wij er in deze discussie voor de belangen van big tech zaten, terwijl het met name ging om het vertrouwen dat consumenten/gebruikers moeten kunnen hebben in de vertrouwelijkheid en integriteit van hun versleutelde communicatieverkeer, cf kabinetsbeleid 2016. Later in het stuk staat het wel wat genuanceerder.

Verder staat er een steek van JenV richting EZK in dat wij laat in de wedstrijd pas met onze bezwaren kwamen. Mij staat bij dat wij juist verrast werden door de move van JenV, en daarom niet anders konden dan vanaf dat moment onze argumenten en bezwaren in te brengen.

Maar zoals gezegd, mijn team kijkt er nu naar; kom zsm terug met meer nuance/onderbouwing.

5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: vrijdag 27 mei 2022 22:41
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e
 @minezk.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: NRC - aftappen OTT.docx

Beste 5.1.2.e ,

Bijgaand vertrouwelijk een (concept)artikel dat ik zojuist ontving van NRC Handelsblad. De krant gaat komende week op basis van wob's publiceren. Besprak ik van de week al even met 5.1.2.e De journalist vraagt EZK om maandag mee te lezen en eventueel commentaar of extra achtergrond aan te leveren op deze tekst. Kunnen jullie (en jullie mensen) meekijken? 5.1.2.e , je wordt als DG B&I ook genoemd in het artikel.

Hoor graag maandag even, hartelijke groet,

5.1.2.e

Verstuurd vanaf mijn iPhone

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Economische Zaken en Klimaat

Directie Communicatie

Bezuidenhoutseweg 73 | 2594 AC | Den Haag

Postbus 20401 | 2500 EK | Den Haag
.....

T: 06 5.1.2.e

E: 5.1.2.e @minezk.nl

www.rijksoverheid.nl/ezk

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: 5.1.2.e
Verzonden: dinsdag 31 mei 2022 10:34
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Aanvullende vraag NRC-artikel / reactie JenV
Categorieën: Categorie Rood

Ha 5.1.2.e

Dank. Er was idd een MCEV voornemen om een wetstraject te starten, maar het kabinetsbesluit 2016 bleef daarbij het vertrekpunt. JenV (mn Grapperhaus zelf) wilde daarop doorpakken met een aanpassing van de Tw die wij teveel vonden doorslaan naar een verzwakking vd vertrouwelijkheid en betrouwbaarheid van de OTT-diensten; we wezen daarbij op het staande kabinetsstandpunt van 2016.

Onze insteek was daarom: inventariseer nu eerst of er (op termijn) mogelijkheden zijn die het mogelijk maken aan aftappen te doen tbv opsporing, ZONDER de veiligheid en betrouwbaarheid van OTT te verzwakken. Daarbij wezen we op de inventarisatie die nationaal en ook Europees liep, waarbij wij sterke voorkeur hebben voor het Europese traject. Immers, dit kan je gezien de interne markt waar dit zich afspeelt niet zomaar nationaal regelen. Wat trouwens an sich nog een extra reden was waarom wij kritisch stonden tegen het voornemen hier als NL met een nationale wet een Alleingang op te doen.

Helpt dit?

5.1.2.e

Van: 5.1.2.e @minezk.nl>

Verzonden: dinsdag 31 mei 2022 10:20

Aan: 5.1.2.e @minezk.nl>

CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>

5.1.2.e @minezk.nl>

5.1.2.e @minezk.nl>

Onderwerp: Aanvullende vraag NRC-artikel / reactie JenV

Beste 5.1.2.e

Een korte vraag nog. JenV gaat ook nog aanvullend reageren op het NRC-stuk. Zie onderstaand. Klopt het gele deel (opdracht MCEV voor een wetstraject, en onze voorkeur voor een inventarisatie)?

CONCEPT ANTWOORD JENV

Een complex dossier als het mogelijk kunnen aftappen van OTT-communicatiediensten vergt een zorgvuldig proces waar gezocht kan worden naar mogelijkheden en waar vervolgens de voor- en nadelen kunnen worden afgewogen op basis van de betrokken belangen. De betrokken belangen zijn al in het kabinetsstandpunt van 2016 over encryptie verwoord, en de verschillende genoemde organisaties zijn een afspiegeling van deze verschillende belangen.

Sinds de raadsresolutie van 24 november 2020 wordt gewacht op de Europese Commissie die in 2022 met een way forward komt. De inventarisatie is dus nog steeds gaande, waarbij we primair inzetten op het Europese traject.

De inventarisatie naar mogelijkheden om OTT-communicatiediensten aftapbaar te maken en de voor- en nadelen daarvan wordt interdepartementaal, ook door EZK en de NCTV, gesteund. Hierbij moet onderscheid worden gemaakt tussen deze inventarisatie van mogelijkheden enerzijds, en het wetstraject in opdracht van de MCEV anderzijds, waarbij EZK de voorkeur had de inventarisatie eerst af te wachten. Voor de inventarisatie worden verschillende experts en bronnen aangeboord, zoals ook het NCSC, vanuit haar expertise op cybersecurity. Logischerwijs wordt er op dergelijke dossiers zowel de voors als tegens (op scherpe wijze) uitgewerkt door de betrokken organisaties op ambtelijk niveau, zodat bij eventuele besluitvorming op ministerieel niveau alle feiten en informatie op een rij staan.

De auteur geeft in zijn artikel al aan kennis te hebben van verschillende van onderstaande documenten, maar voor de volledigheid noem wijs ik op:

-Wob verzoek 1 juli 2020, onder andere: doc nr. 1

-Wob verzoek 28 april 2022, onder andere: doc C004, C006, C012b, C051, C058.

Hartelijke groet,
5.1.2.e

Met vriendelijke groet,

5.1.2.e

Ministerie van Economische Zaken en Klimaat

Directie Communicatie

Bezuidenhoutseweg 73 | 2594 AC | Den Haag

Postbus 20401 | 2500 EK | Den Haag

T: 06 5.1.2.e

E: 5.1.2.e@minezk.nl

www.nrksoverheid.nl/ezk

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: 5.1.2.e
Verzonden: woensdag 29 juni 2022 16:49
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: ter info: Akkoord gevraagd: Definitief concept CSR Adviesbrief over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie anders dan inperking van encryptie

Categorieën: Categorie Rood

Ter info de mail aan de CSR met akkoord van 5.1.2.e

5.1.2.e, willen jullie contact leggen met JenV en DC 5.1.2.e dat dit volgende week eraan komt en dat bij evt woordvoering dat JenV in de lead is?

Alvast dank,

Groeten,

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 29 juni 2022 16:47
Aan: 'Secretariaat CSR' 5.1.2.e @cybersecurityraad.nl>
CC: 5.1.2.e @minezk.nl>
Onderwerp: RE: Akkoord gevraagd: Definitief concept CSR Adviesbrief over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie anders dan inperking van encryptie

Hallo 5.1.2.e

Namens 5.1.2.e akkoord op het advies.

Groeten,

5.1.2.e

5.1.2.e
 Directie Digitale Economie
 Ministerie van Economische Zaken en Klimaat
 5.1.2.e @minezk.nl
 065.1.2.e

Van: Secretariaat CSR 5.1.2.e @cybersecurityraad.nl>
Verzonden: maandag 27 juni 2022 18:27
Aan: 5.1.2.e @cybersecurityraad.nl>; Secretariaat CSR
 5.1.2.e @cybersecurityraad.nl>
Onderwerp: Akkoord gevraagd: Definitief concept CSR Adviesbrief over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie anders dan inperking van encryptie

Geachte leden,

Zoals besproken tijdens de CSR Vergadering van 16 juni jl. stuur ik u hierbij een aangepaste versie van de CSR Adviesbrief over reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie anders dan inperking van encryptie. De wijzigingen in de brief zijn met track changes aangebracht. Graag verneem ik uiterlijk vrijdag 1 juli a.s. of u akkoord bent met deze versie. Bureau Secretaris zal daarna de nodige voorbereidingen treffen om het advies in de week van 4 juli in eerste instantie schriftelijk aan te bieden aan de bewindspersonen en daags erna ook publiceren op de website van de raad en op LinkedIn en Twitter. Ik hou u uiteraard op de hoogte van de ontwikkelingen.

Met hartelijke groet,

5.1.2.e



5.1.2.e

Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag

Ministry of Justice and Security
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands
P.O. Box 20011 | 2500 EA | The Hague | The Netherlands

T +31 70 5.1.2.e (secretariaat/secretary)

M +31 6 5.1.2.e

5.1.2.e [@cybersecurityraad.nl](mailto:5.1.2.e@cybersecurityraad.nl)
<https://www.cybersecurityraad.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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:46
Aan: 5.1.2.e
Onderwerp: FW: concept nota ACEV OTT
Bijlagen: 310125 Nota ACEV februari 2021 def.docx

Van: 5.1.2.e @minjenv.nl>
Verzonden: zondag 31 januari 2021 22:09
Aan: 5.1.2.e @minezk.nl>
Onderwerp: RE: concept nota ACEV OTT

Dag 5.1.2.e

Zie bijgaand een aangepaste versie van mijn kant. Wijzigingen die ik heb gemaakt betreffen:

- Ik heb de aanleiding voor de vervolgopties naar boven gehaald en onder de vervolgopties vind je ons beider standpunten.
- Ik heb in de nota nu aangegeven dat vanuit EZK bezwaren zijn gerezen voor de omzetting van het besluit van de MCEV en waarom.
- De vervolgopties heb ik nu neutraal geformuleerd, evt voors en tegens komen in onze afzonderlijke standpunten naar voren.
- Verder hebben we evenals jullie de onderbouwing van waarom we hier staan voor deze keuze en die van belang is in ons standpunt uitgebreider geschetst.
- In jullie standpunt heb ik natuurlijk niets gewijzigd, wel wil ik je de suggestie meegeven om te kijken of je het standpunt van de IenV diensten over verbeterde beveiliging van SMS-diensten zo wil opnemen. Het is inhoudelijk namelijk niet juist, de diensten willen beter beveiliging, niet dat ze niet meer aftapbaar zijn. Daarmee raakt dat punt aan de kern van onze discussie: er moet goede beveiliging zijn, maar ook toegang. Zoals nu KPN en andere telco's het hebben ingericht.

Mocht je nog vragen hebben dan hebben we nog contact.

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: woensdag 27 januari 2021 15:05
Aan: 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
Onderwerp: concept nota ACEV OTT

Beste 5.1.2.e

Bijgaand onze aanzet tot een gezamenlijke notitie inzake het aftappen van OTT's. Wij hebben meer helder de EZK visie erin verwerkt, waaronder de gevolgen voor encryptie. Graag hoor ik of je hierin kunt vinden,

Groet,

5.1.2.e

Ministerie van Economische Zaken

Bezuidenhoutseweg 73 | 2594 AC | Den Haag

Postbus 20401 | 2500 EK | Den Haag

.....
T: +31 65.1.2.e
.....

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, 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.
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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:47
Aan: 5.1.2.e
Onderwerp: FW: Brief OTT briefing
Bijlagen: Brief OTT briefing.docx

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 08:39
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minezk.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Brief OTT briefing

Dag 5.1.2.e

Zie bijgaan de versie die nu bij de SG/minister ligt. Verzoek is dus of deze mede namens de stas deze ochtend naar buiten kan. 5.1.2.e heeft gisteren al contact gehad met 5.1.2.e over deze brief.

Dank al vast en groet,

5.1.2.e

Regards,

5.1.2.e

Head of Organised Crime Unit

.....
Law Enforcement Department

Turfmarkt 147 | 2511 DP The Hague | The Netherlands
 P.O. Box 20301 | 2500 EH The Hague

.....
 M: +31 6 5.1.2.e

Secr: +31 70 5.1.2.e

5.1.2.e @minjenv.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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:47
Aan: 5.1.2.e
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon
Bijlagen: Aftapbaarheid OTT-diensten versie 2 schoon.docx; Brief OTT briefing 5.1.2.e.docx

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 12:15
Aan: 5.1.2.e @minezk.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Ha 5.1.2.e

Zie bijgaan de versie die wij nu bij de minister hebben voorgelegd.

Groet, 5.1.2.e

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 12:14
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e

Hierbij de nieuwe versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
 5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:12
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>
CC: 5.1.2.e @minjenv.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Excuus voor spam. Laatste versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e [@minvenj.nl](mailto:5.1.2.e@minvenj.nl)

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:07
Aan: 5.1.2.e [@minjenv.nl](mailto:5.1.2.e@minjenv.nl)>
Onderwerp: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e

Hierbij de brief.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e [@minvenj.nl](mailto:5.1.2.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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:47
Aan: 5.1.2.e)
Onderwerp: FW: Aftapbaarheid OTT-diensten poging 4
Bijlagen: Aftapbaarheid OTT-diensten versie 4.docx; Aftapbaarheid OTT-diensten versie 3 en 4 TC.docx

Urgentie: Hoog

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 16:03
Aan: 5.1.2.e @minezk.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten poging 4
Urgentie: Hoog

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 15:38
Aan: 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aftapbaarheid OTT-diensten poging 4
Urgentie: Hoog

Hallo 5.1.2.e

Hierbij de versie zoals geaccordeerd door de minister. Tov versie 3 enkele nuance verschillen, deze heb ik inzichtelijk gemaakt in bijgevoegde TC versie.

Nogmaals excuses voor de verschillende versies. De spoed is bij je bekend, zou je kunnen laten weten wanneer de SEZK er naar kan kijken en met welk advies jullie de brief voorleggen?

Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
 5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 14:21
Aan: 5.1.2.e @minezk.nl>
Onderwerp: FW: Aftapbaarheid OTT-diensten poging 3

Hallo 5.1.2.e

Hierbij de nieuwe versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 14:17
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e
@minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e
@nctv.minjenv.nl>; 5.1.2.e
@nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>;
5.1.2.e @nctv.minjenv.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e
@minjenv.nl>
Onderwerp: Aftapbaarheid OTT-diensten poging 3

Nav overleg met de minister de derde versie.

Met vriendelijke groet,

5.1.2.e

M 06 5.1.2.e
5.1.2.e @minvenj.nl

Van: 5.1.2.e
Verzonden: donderdag 11 maart 2021 12:12
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e
@minjenv.nl>; 5.1.2.e @minjenv.nl>; 5.1.2.e
@nctv.minjenv.nl>; 5.1.2.e
@nctv.minjenv.nl>; 5.1.2.e @minjenv.nl>

CC: 5.1.2.e [redacted]@minjenv.nl>

Onderwerp: FW: Aftapbaarheid OTT-diensten versie 2 schoon

Excuus voor spam. Laatste versie.

Met vriendelijke groet,

5.1.2.e [redacted]

M 06 5.1.2.e [redacted]
5.1.2.e @minvenj.nl

Van: 5.1.2.e [redacted]

Verzonden: donderdag 11 maart 2021 12:07

Aan: 5.1.2.e [redacted]@minjenv.nl>

Onderwerp: Aftapbaarheid OTT-diensten versie 2 schoon

Hallo 5.1.2.e [redacted]

Hierbij de brief.

Met vriendelijke groet,

5.1.2.e [redacted]

M 06 5.1.2.e [redacted]
5.1.2.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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:47
Aan: 5.1.2.e
Onderwerp: FW: Aftapbaarheid OTT-diensten versie 4
Bijlagen: Aftapbaarheid OTT-diensten versie 4.docx

Van: 5.1.2.e @minjenv.nl>
Verzonden: donderdag 11 maart 2021 18:34
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e @minezk.nl>
CC: 5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl>
Onderwerp: Aftapbaarheid OTT-diensten versie 4

Heren,

Hierbij de def versie, voor hacks hebben we de officiële term binnendringen in geautomatiseerd werk gebruikt.

Groet en dank,

5.1.2.e

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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:49
Aan: 5.1.2.e
Onderwerp: FW: Brief

Van: 5.1.2.e @minjenv.nl>
Verzonden: woensdag 17 maart 2021 10:00
Aan: 5.1.2.e @minezk.nl>; 5.1.2.e
@minezk.nl>
Onderwerp: RE: Brief

Ha 5.1.2.e

Dat lijkt me een goed idee, mijn collega 5.1.2.e sluit dan ook aan.

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 maart 2021 22:47
Aan: 5.1.2.e @minjenv.nl>; 5.1.2.e
@minezk.nl>
Onderwerp: RE: Brief

Dag 5.1.2.e

Lijkt me goed als we binnenkort afspreken hoe nu verder. Ik had 5.1.2.e benaderd maar kreeg nog geen reactie. Zouden jullie tijd hebben voor een afspraak, bv do middag?

Hoor graag, dan plannen we wat in.

Groet!

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 12 maart 2021 11:03
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Brief

Ha 5.1.2.e

Bijgaande brief is naar de kamer gestuurd, is dus de versie geworden van voor de afstemming.

Laten we begin volgende week even met elkaar bekijken hoe verder te gaa.

Groet, 5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

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

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, 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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:50
Aan: 5.1.2.e
Onderwerp: FW: Aanbiedingsform MCEV
Bijlagen: Aanbieding MCEV OTT feb 2021.pdf

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 16 februari 2021 12:17
Aan: 5.1.2.e @minezk.nl>
Onderwerp: Aanbiedingsform MCEV

Let op, in de bijlage van deze e-mail, verzonden door 5.1.2.e @minjenv.nl, is een macro aangetroffen. Macro's kunnen misbruikt worden om malware op uw systeem te installeren. Open de bijlage alleen als de e-mail afkomstig is van een door u vertrouwde afzender.

Indien dit niet het geval is dient u deze e-mail direct te verwijderen zonder de bijlage te openen.

DICTU Servicedesk

Dag 5.1.2.e

Voor de MCEV van volgende week moet nog een aanbiedingsformulier opgesteld worden, zie bijgaand. Tevens wordt de nota en het verslag van ACEV er bij aangeboden. Ben jij akkoord met bijgaande formulering. Deze moet uiterlijk vandaag bij AZ. Dank al vast voor je reactie.

Groet, 5.1.2.e

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

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:50
Aan: 5.1.2.e
Onderwerp: FW: Aanbiedingsform MCEV

Van: 5.1.2.e @minjenv.nl>
Verzonden: dinsdag 16 februari 2021 16:41
Aan: 5.1.2.e @minezk.nl>
Onderwerp: RE: Aanbiedingsform MCEV

Dag 5.1.2.e

Eens met je dat we discussies niet opnieuw gaan doen. Ik wil wel scherp hebben waarom we dit gesprek nu op de MCEV voeren en bijgaande zin haal ik uit de nota: EZK voorziet ondanks eerdere besluitvorming en debat hierover toch risico's ten aanzien van veilige encryptie als OTT-diensten aftapbaar worden.

Wat mij betreft zetten we die overeengekomen zin dan ook terugkomen in het aanbiedingsformulier, want volgens mij geeft deze het correct weer (anders waren we m ook niet overeen gekomen ;-).

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>
Verzonden: dinsdag 16 februari 2021 15:21
Aan: 5.1.2.e @minjenv.nl>
Onderwerp: RE: Aanbiedingsform MCEV

5.1.2.e

De reden voor mijn tekstvoorstel was dat ik uit de semantiek zou willen blijven en een eerdere discussie niet over wil doen.

Wij hebben eerder, om goede redenen, bezwaar gemaakt tegen de zin die nu weer wordt voorgesteld. Daar zijn we toen in de herkansing goed uitgekomen, met de overeengekomen passage in de nota, die een goede discussie in de ACEV heeft gefaciliteerd. Laten we het daarom houden bij de agreed language en die ook weer op te nemen in dit aanbiedingsformulier.

Groet,

5.1.2.e

Verzonden vanuit [Mail](#) voor Windows 10

Van: 5.1.2.e
Verzonden: dinsdag 16 februari 2021 14:12
Aan: 5.1.2.e
Onderwerp: RE: Aanbiedingsform MCEV

Ha 5.1.2.e

Naar mijn idee moet wel helder zijn dat de nota er nu ligt omdat er een wijziging is van de eerder ingezette koers, dus een heroverweging van jullie kant op het eerder genomen besluit. Daar ben je het wel mee eens toch?

Groet, 5.1.2.e

Van: 5.1.2.e @minezk.nl>

Verzonden: dinsdag 16 februari 2021 13:31

Aan: 5.1.2.e @minjenv.nl>

Onderwerp: RE: Aanbiedingsform MCEV

Ha 5.1.2.e

Ik heb bezwaren tegen de volgende zin: "Dit laatste onderdeel van het MCEV besluit wordt door EZK niet meer gesteund. De Minister van Justitie en Veiligheid wil deze impasse en hoe hiermee om te gaan bespreken in de MCEV."

Daarom het volgende tekstvoorstel: ..

"Bijgesloten nota is door JenV en EZK opgesteld en besproken in de ACEV van 11 februari 2021. Het verslag van die bespreking is tevens toegevoegd.

Doel van de nota is u te informeren over de dilemma's die ten grondslag liggen aan de vraag hoe zorgvuldig invulling gegeven kan worden aan het MCEV-besluit van mei 2020 om Over-The-Top-communicatiediensten (OTT) net als telecommunicatiediensten wettelijk te verplichten om hun communicatiedienst, in het bijzonder met betrekking tot encryptie, zodanig in te richten dat communicatie daarover afgetapt kan worden ten behoeve van de opsporing of nationale veiligheid. Vervolgens is het doel dat u, na kennisname over de gevolgen en risico's, een keuze maakt uit de **in de nota** geschetste opties."

Groet,

5.1.2.e

Groet,

5.1.2.e

Verzonden vanuit [Mail](#) voor Windows 10

Van: 5.1.2.e

Verzonden: dinsdag 16 februari 2021 12:17

Aan: 5.1.2.e

Onderwerp: Aanbiedingsform MCEV

Let op, in de bijlage van deze e-mail, verzonden door 5.1.2.e @minjenv.nl, is een macro

aangetroffen. Macro's kunnen misbruikt worden om malware op uw systeem te installeren. Open de bijlage alleen als de e-mail afkomstig is van een door u vertrouwde afzender.

Indien dit niet het geval is dient u deze e-mail direct te verwijderen zonder de bijlage te openen.

DICTU Servicedesk

Dag 5.1.2.e

Voor de MCEV van volgende week moet nog een aanbiedingsformulier opgesteld worden, zie bijgaand. Tevens wordt de nota en het verslag van ACEV er bij aangeboden. Ben jij akkoord met bijgaande formulering. Deze moet uiterlijk vandaag bij AZ. Dank al vast voor je reactie.

Groet, 5.1.2.e

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

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, 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: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 10:51
Aan: 5.1.2.e
Onderwerp: FW: Tekst Beleidsnota MCEV mei 2020
Bijlagen: 1 Beleidsnota 5G en de opsporing MCEV.docx

Van: 5.1.2.e @minjenv.nl>
Verzonden: woensdag 13 januari 2021 10:25
Aan: 5.1.2.e @minezk.nl>
Onderwerp: Tekst Beleidsnota MCEV mei 2020

Dag 5.1.2.e

Ik heb in bijgaande nota nog geel gearceerd mbt het besluit van de MCEV. JenV interpreteert deze als volgt:

In lijn met de implementatiewetgeving van het Europees wetboek voor elektronische communicatie, de Telecomcode, wordt ook in hoofdstuk 13 van de Telecommunicatiewet het begrip 'elektronische communicatiedienst' gehanteerd. Dit begrip omhelst diverse soorten diensten, waaronder 'nummeronafhankelijke interpersoonlijke communicatiediensten (zogenaamde Over The Top diensten (OTT) zoals WhatsApp en Signal), die nu geen medewerkings- en aftapbaarheidsverplichting kennen in hoofdstuk 13.

Kortom we brengen OTT-diensten onder de aftapverplichting.

worden de mogelijkheden verkend om nummeronafhankelijke interpersoonlijke communicatiediensten mee te nemen in het wijzigingstraject van 5G. Tenzij dit leidt tot vertraging van de invoering van de benodigde wet- en regelgeving van de functionele eisen.^[1]

De verkenning ziet dus niet toe op het punt of OTT onder de aftapverplichting moet komen maar op het feit of dit 5G gaat vertragen. De werkgroep heeft dit verkend en besproken en het leidt vooralsnog niet tot een vertraging die onacceptabel is.

Groet, 5.1.2.e

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

^[1] Besloten netwerken hoeven in beginsel niet bij voorbaat te investeren in een aftapfaciliteit of een ontheffing daarvoor aan te vragen. Op dit moment ziet deze eis op aanbieders die nu als 'openbaar telecommunicatienetwerk of openbare telecommunicatiedienst' kunnen worden aangewezen, maar onder 5G niet meer of aanbieders die soortgelijke diensten gaan aanbieden onder 5G. Pas bij een regulier verzoek zullen voorzieningen moeten worden getroffen of worden verzocht om een ontheffing.

Van: 5.1.2.e
Verzonden: donderdag 18 augustus 2022 11:07
Aan: 5.1.2.e
Onderwerp: FW: ACEV nota OTT en %G
Bijlagen: Nota ACEV 14 januari 2021_def.docx

Van: 5.1.2.e @minjenv.nl>

Verzonden: donderdag 7 januari 2021 14:45

Aan: 5.1.2.e @minezk.nl>; 5.1.2.e
@ind.nl>

CC: 5.1.2.e @minjenv.nl>; 5.1.2.e
@minjenv.nl>

Onderwerp: ACEV nota OTT en %G

Beste 5.1.2.e en 5.1.2.e

Conform bespreking tussen jou en 5.1.2.e heb ik de nota voor de ACEV nog iets aangevuld en de relatie met het kabinetsstandpunt encryptie aangegeven.

Groet,

5.1.2.e

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

Behoud effectiviteit van interceptie en sterke encryptie

Ingediend door de ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat

Probleemstelling

- Interceptie (aftappen) van communicatie van subjecten en verdachten is een onmisbaar instrument voor de opsporingsdiensten en inlichtingen- en veiligheidsdiensten (hierna: I&V-diensten): om zicht te krijgen op een (statelijke) dreiging en voor inzage in digitale sporen, vergaring van bewijs en identificatie van daders, mededaders en slachtoffers.
- Over The Top-communicatiediensten (hierna: OTT-communicatiediensten) zoals WhatsApp, Signal, e.d. zijn steeds meer het standaard communicatiemiddel geworden ten koste van de spraak- en SMS-diensten van aanbieders van (klassieke) telecommunicatiediensten, zoals KPN, T-mobile, e.d. Dat geldt ook voor criminelen – bijvoorbeeld fraudeurs, witwassers, pedofielen die kinderen *groomen* op die diensten, inbrekers, plegers van gewelds- en levensdelicten etc. - en personen die een dreiging voor de nationale veiligheid vormen.
- De meeste aanbieders van OTT-communicatiediensten zijn hun dienst sinds een jaar of zes gaan versleutelen met end-to-end-encryptie. Daartoe hebben zij verschillende redenen, zoals dat de veiligheid van digitale communicatie op deze wijze sterk en goed beschermd is en de privacy van gebruikers, namelijk burgers, bedrijfsleven en de overheid te waarborgen.
- De consequentie hiervan is dat de onversleutelde inhoud van de communicatie van een voor het onderzoek relevant subject of verdachte niet via een tap kan worden verkregen. Deze OTT-communicatiediensten kunnen vanwege de door de OTT's beschikbaar gestelde versleutelingstechniek namelijk niet aan een rechtmatige vordering, bijvoorbeeld door een rechter-commissaris, van de onversleutelde inhoudelijke communicatie voldoen. Dit ongeacht de ernst van de dreiging of het misdrijf.
- Naast deze voor het brede publiek vrij toegankelijke OTT-communicatiediensten (Whatsapp, Facebook Messenger, Signal etc.), is uit recente strafrechtelijke onderzoeken gebleken dat er bij internationale en georganiseerde zware criminaliteit óók gebruik wordt gemaakt van betaalde versleutelde communicatiediensten, veelal in combinatie met specifiek geprepareerde telefoons, die niet bij het algemene publiek in gebruik zijn (voorbeelden hiervan zijn skyECC en Encrochat). Problematisch blijft naar verwachting dat de genoemde (online) minder breed beschikbare betaalde cryptodiensten zich niet zullen voegen naar wet- en regelgeving.
- De aanbieders van breed toegankelijke OTT-communicatiediensten zijn, evenals aanbieders van de minder breed beschikbare betaalde cryptodiensten zoals Encrochat, in tegenstelling tot de (klassieke) telecommunicatiediensten niet wettelijk (Telecommunicatiewet) verplicht om hun dienst zodanig in te richten dat de ontsleutelde inhoud van de communicatie van een subject of verdachte daarover via een tap kan worden verkregen. Aanbieders van telecommunicatiediensten en-netwerken zijn onder de huidige wetgeving verplicht om de communicatie bij een rechtmatige vordering van de door hen aangebrachte versleuteling te ontdoen.
- Dit heeft een steeds grotere negatieve impact op de slagkracht van de opsporingsdiensten, I&V-diensten en op de strafrechtelijke vervolging van verdachten.
- Het verkrijgen van rechtmatige toegang tot de inhoudelijke communicatie van verdachten en subjecten via interceptie vergt dat de wijze van beveiliging en implementatie van versleuteling door aanbieders van OTT-communicatiediensten daartoe in specifieke gevallen mogelijkheden biedt. Voor end-to-end versleuteling kan dit waarschijnlijk een verzwakking ten opzichte van de huidige implementatie betekenen. Hierdoor wordt het belang om gedegen onderzoek naar een haalbare oplossing te doen nogmaals benadrukt.
- Experts verschillen van mening over de vraag of een dergelijke aanpassing van de aard en implementatie van beveiliging - ten behoeve van rechtmatige toegang tot de communicatie van een subject of verdachte voor de opsporings- en I&V-diensten - op een veilige manier te realiseren is.
- Behoud van goede encryptie is van essentieel belang voor beveiliging van de communicatie en het waarborgen van fundamentele rechten, zoals privacy, bescherming van bedrijfs- en staatsgeheimen en vrijheid van meningsuiting (inclusief persvrijheid).
- Veel cybersecurityexperts geven aan dat indien OTT-communicatiediensten in rechtmatige toegang tot inhoudelijke communicatie voorzien, daarmee ook het risico op toegang door (kwaadwillende) derden – het bedrijf zelf, criminelen en statelijke actoren – te veel wordt vergroot; omdat dit zou leiden tot een afzwakking van encryptie. Wanneer het risico van

misbruik te groot wordt, zal dit volgens de tele- en OTT-communicatiediensten, cybersecuritywetenschappers en -experts en verschillende NGO's en belangenorganisaties negatieve gevolgen hebben voor goedwillende afnemers van deze diensten (bedrijven en consumenten) en het vertrouwen in de digitale dienstverlening en -economie.

- In aanvulling hierop speelt nog de vraag, omdat de OTT-communicatiediensten veelal internationaal hun diensten aanbieden, welke indirecte gevolgen een eventuele wettelijke regeling hier heeft voor de bescherming van fundamentele rechten en veiligheid van burgers in niet democratische derde landen. Risico's voor ongewenst gebruik en misbruik van mogelijkheden voor toegang tot communicatie die dankzij wetgeving hier voor ondemocratische regimes worden gecreëerd moeten gemitigeerd worden.
- Er is kortom sprake van een dilemma met grote belangen die gewaarborgd en in evenwicht gebracht moeten worden: veiligheid door encryptie en veiligheid door interceptie. Dit is ook in het Kabinetstandpunt van 2016 over encryptie verwoord.
- Verantwoorde, duurzame en proportionele toegang tot communicatie is voor opsporings- en I&V-diensten én de samenleving van groot belang. De vraag is: (hoe) kan dit bestendig technisch en/of functioneel, worden gerealiseerd zonder grote veiligheidsrisico's door onrechtmatige toegang van kwaadwillende derden te creëren?

Huidige stand van zaken

- De interceptiebevoegdheid is met rechtswaarborgen omkleed en opgenomen in het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten en is zowel van toepassing op traditionele telecommunicatiediensten als op OTT-communicatiediensten.
- Vanwege het hierboven beschreven dilemma rondom encryptie zijn de in hoofdstuk 13 van de Telecommunicatiewet opgenomen inrichtings- en medewerkingsvereisten – ten behoeve van de effectieve tenuitvoerlegging van de wettelijke tapbevoegdheid van de opsporings- en I&V-diensten – niet van toepassing op OTT-communicatiediensten. Ook het feit dat OTT-communicatiediensten gebruik maken van open internationale netwerken en dus zelf beveiliging moeten toepassen speelt daarbij een rol.
- Andere bestaande bevoegdheden zoals de inzet van de 'hackbevoegdheid' (CCIII en WIV) en verzamelen en analyseren van meta-data zijn niet afdoende om het toenemende verlies aan effectiviteit bij de interceptiebevoegdheid op te vangen:
 - o de inzet van de 'hackbevoegdheid' is een bijzonder opsporingsmiddel dat kan worden ingezet als lichtere bevoegdheden niet toereikend zijn. Echter, de strafvorderlijke en (politiek) gestelde voorwaarden voordat een inzet kan worden overwogen zijn hoog, het wettelijk kader kent strikte voorwaarden, vraagt hoogwaardige expertise, het is arbeidsintensief en daarmee niet goed schaalbaar. Het slagen van een inzet is afhankelijk van bestaande zwakheden in de beveiliging van de communicatiedienst of bij de gebruiker. Een duurzame oplossing voor het effectueren van de huidige interceptiebevoegdheden is gebaat bij samenwerking met de OTT-diensten. In het bijzonder waar het om mondiale diensten gaat. De effectiviteit van de wet CCIII wordt op dit moment geëvalueerd, een rapport wordt in 2022 verwacht.
 - o De beschikbaarheid en gebruik van metadata wordt sterk teruggedrongen met recente uitspraken van het Hof van Justitie van de Europese Unie (HvJ-EU), zie onder andere het *Tele2 Sverige* arrest uit 2015 en recente uitspraken als *La Quadrature du Net*. Ook de AVG en de aanstaande e-privacy-verordening nopen communicatiediensten om metadata zo min en kort als mogelijk te bewaren.
- De behoefte aan een oplossing ten behoeve van de opsporing en nationale veiligheid is groot. Zowel in EU verband (zie raadsverklaring van december 2020 over encryptie) als mondiaal is de dringende noodzaak geuit aan een oplossing waarin zowel veiligheid van communicatie door encryptie als rechtmatige toegang ten behoeve van de opsporing en nationale veiligheid wordt gerealiseerd. Ook heeft het vorige Kabinet in de MCEV van mei 2020 besloten dat OTT-communicatiediensten in beginsel net als telecommunicatiediensten aan de verplichtingen - waaronder aftapbaarheid - van hoofdstuk 13 van de Telecommunicatiewet zouden moeten voldoen.

Beleidsoptie

Nader onderzoek is nodig om goed geïnformeerde besluitvorming over bovenstaand dilemma mogelijk te maken. Het gaat daarbij om de vraag of en, zo ja, welke proportionele oplossing - met voldoende waarborgen voor de beveiliging van de communicatie t.b.v. de bescherming van fundamentele rechten, alsook rechtmatige toegang in specifieke gevallen - mogelijk is. Politieke

steun voor dit onderzoek is nodig, omdat er op dit moment zowel politiek, maatschappelijk als ambtelijk grote tegenstellingen bestaan over de vraag of en, zo ja, op welke wijze oplossingen voor het vraagstuk gevonden moeten worden.

Als de politieke steun en richting, evenals de nodige financiële middelen, gegeven worden, dan zijn i.i.g. twee trajecten gewenst:

1. Het blijven steunen en politiek aanjagen van de verkenning van mogelijke technische oplossingen door de Europese Commissie, waartoe is opgeroepen in een raadsverklaring in december 2020. Temeer omdat dit een grensoverschrijdend vraagstuk is en een Europese oplossing effectief kan zijn waar het wereldwijd opererende (OTT) spelers betreft.
2. Opzetten van onderzoek op nationaal niveau om mogelijke (technische) oplossingen binnen de gestelde kaders: sterke encryptie en beveiliging ter bescherming van fundamentele rechten en rechtmatige toegang tot communicatie in specifieke gevallen. De toerusting en bevoegdheden van opsporings- en I&V-diensten zijn bij uitstek een nationaal domein. Voor de verkenning is onderzoeksbudget en inzet van de opsporings- en I&V-diensten evenals experts vanuit het bedrijfsleven en wetenschap nodig. Ook het maatschappelijk middenveld moet daarbij worden betrokken.

Op basis van de mogelijk gevonden (technische) oplossingen, waarbij de inzet is dat die op breed draagvlak kunnen rekenen vanuit hogergenoemde stakeholders, kan een voldragen juridische en politiek-bestuurlijke weging over de proportionaliteit en wenselijkheid daarvan plaats vinden - in het licht van de in de probleemstelling benoemde belangen en risico's - en eventueel tot wetgeving besloten worden. Zoals gebruikelijk worden bij de besluitvorming ook reeds beschikbare mogelijkheden voor toegang tot bewijs meegenomen of alternatieve (toekomstige) mogelijkheden.

Van onomkeerbare stappen is in dit voorstel dan ook geen sprake. Het onderzoek moet bijdragen aan geïnformeerde besluitvorming. Daarbij blijft de conclusie mogelijk - zoals in het Kabinetsstandpunt encryptie uit 2016 is geconcludeerd - dat op er nog steeds geen zicht is op mogelijkheden om in algemene zin, bijvoorbeeld via wettelijke functionele eisen en standaarden, rechtmatige toegang tot inhoud van communicatie van subjecten en verdachten via OTT-communicatiediensten te krijgen zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Dan zal weloverwogen het verlies van effectiviteit van de bevoegdheid om communicatie van verdachten en subjecten af te luisteren en gevolgen daarvan voor de opsporing- en nationale veiligheid geaccepteerd moeten worden.

Alternatief

Een alternatief voor de ambtelijke gecoördineerde uitwerking is de instelling van een onafhankelijke adviescommissie - met wetenschappers en experts op het terrein van opsporing, openbare orde, slachtofferrechten, strafrecht, mensenrechten, persvrijheid, cybersecurity en communicatietechnologie - die gevraagd kan worden om de mogelijke praktische oplossingen en consequenties voor het vraagstuk uit te werken in concrete voorstellen en de regering daarover te adviseren.

Benodigde uitwerking wet- en regelgeving

Afhankelijk van de uitkomsten van de (technische) verkenning en politieke besluitvorming daarover.

Financiële consequenties

De genoemde bedragen betreffen enkel zeer grove inschatting van de benodigde middelen voor het voorgestelde technisch innovatietraject. De daadwerkelijke kosten kunnen dus lager of hoger uitvallen, omdat de gewenste onderzoeksopzet en scope - in verband met het nodige draagvlak en medewerking daarvoor van zowel publieke als private partijen - nog moet worden uitgewerkt en omdat de kosten voor technisch onderzoek relatief hoog en variabel kunnen zijn. Deze uitwerking en daarmee een nauwkeurigere raming van de kosten, kan pas plaats vinden als er politieke opdracht is om bovenstaand onderzoek uit te laten voeren.

Voor de verkenning van en het onderzoek naar technische mogelijkheden door opsporings- en I&V-diensten, bedrijven en wetenschap is een grof geraamd onderzoeksbudget van circa € 8 mln. (beperkte variant) à € 10 mln. (uitgebreide variant) eenmalig in gelijke delen verdeeld over 4 jaren nodig. Een zeer beperkte variant - voornamelijk bepaling requirements en literatuurstudie, maar zonder technische uitwerking en proof-of-concept - wordt geraamd op circa € 2 mln. eenmalig verdeeld over 2 jaren.

Consequenties voor de keten

Afhankelijk van de uitkomsten, nu nog niet bekend. Mocht beleids- en wetswijziging te zijner tijd op basis van de uitkomsten van bovenstaand onderzoek overwogen worden, dan geldt net zoals voor alle wetswijzigingen dat deze uitvoerbaar en handhaafbaar moet zijn.

Betrokken partners

Ministerie van Justitie en Veiligheid, Ministerie van Defensie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het Ministerie van Buitenlandse Zaken, Ministerie van Economische Zaken en Klimaat, Openbaar Ministerie, Politie, Agentschap Telecom, Nationaal Coördinator Terrorismebestrijding en Veiligheid (waaronder NCSC), Algemene Inlichtingen en Veiligheidsdienst, Militaire Inlichtingen en Veiligheidsdienst, Bijzondere Opsporingsdiensten (FIOD, ISZW-IOD, IL&T-IOD en NVWA-IOD) en het Nederlands Forensische Instituut (NFI).

Factsheet Encryptie

Algemeen

- Encryptie, ofwel versleuteling, is een essentieel middel voor bedrijven en overheden om aangeboden communicatie te beveiligen.
- Aanbieders van Over-The-Top diensten, diensten die via open netwerken worden aangeboden, passen end-to-end encryptie toe. Hiermee wordt persoonlijke informatie van de gebruikers van dergelijke diensten beschermd en vertrouwelijkheid cf. het Europese wettelijke kader geborgd.
- End-to-end encryptie betekent dat de inhoud van communicatie van de afzender aan de ontvanger adequaat versleuteld is. Het doel van adequate encryptie is dat zowel de aanbieder van een online dienst als een derde geen sleutel en dus geen toegang hebben om de communicatie van de betrokkene in te zien. De communicatie tussen verzender en aanbieder van de communicatieboodschap is niet in te zien door derden.
- End-to-end encryptie is een belangrijke technologie die gegarandeerde bescherming biedt tegen misbruik door derden en is van wezenlijk belang voor het versterken van de cyberveiligheid.
- JenV verkent in hoeverre het mogelijk is om toch OTT-diensten af te kunnen tappen. De aanbieders van OTT-diensten zouden dan de communicatie bijvoorbeeld kunnen ontsleutelen door middel van 'backdoors'. Met backdoors of andere kwetsbaarheden wordt de encryptie per definitie afgezwakt en voor derden toegankelijk. Een dergelijke bepaling zou dan in optiek van JenV in de Telecommunicatiewet moeten worden opgenomen (hoofdstuk 13). EZK is politiek en beleidsmatig verantwoordelijk voor de Telecommunicatiewet.
- Cybersecuritydeskundigen (wetenschap, experts) stellen dat wanneer er toch sleutels worden ingebouwd (zogenaamde 'backdoors') dat de risico's van misbruik van de communicatie door derden (criminele organisaties, spionagediensten) aanzienlijk vergroot worden. Deze ontwikkeling is onacceptabel omdat hiermee het systeem – digitale infrastructuur en online diensten – onveilig wordt. Dit wordt ook onderkend door de Nederlandse overheid, zie het kabinetsstandpunt over encryptie.
- De beschikbaarheid en de toepassing van hoogwaardige encryptie is essentieel voor de bescherming van onze digitale infrastructuur en communicatie, en daarmee niet alleen belangrijk voor onze democratische vrijheid, maar ook van groot belang voor innovatie en economische groei.
- 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. De introductie van *backdoors* verzwakt het vertrouwen van afnemers in de digitalisering en daarmee de digitale economie.
- Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigingsklimaat. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de groeipotentie van de economie, die vooral zit in de digitale economie.

Kabinetsstandpunt encryptie

- J&V, BZ, BZKzk en EZK hebben in 2016 het kabinetsstandpunt over encryptie geformuleerd en naar de Kamer gestuurd. Het kabinetsstandpunt geeft aan dat versleuteling (encryptie) gebruikt wordt om het vertrouwelijke karakter en de integriteit van communicatie en data te waarborgen. Encryptie is dan ook een belangrijke technologie om de cyberveiligheid te waarborgen.
- Verder wordt benadrukt dat encryptie het vertrouwen in digitale communicatie bevordert en digitale innovatie aanjaagt. Dit is zeker van belang gezien de toenemende economische spionage bij Nederlandse bedrijven.
- Tegelijkertijd erkent het kabinet dat encryptie een belemmering vormt voor het verkrijgen van voor opsporings-, inlichtingen- en veiligheidsdiensten noodzakelijke informatie wanneer terroristen hiervan gebruikmaken.

- Het kabinet concludeert echter dat het beleidsmatig opleggen van beperkingen aan encryptie of het inbouwen van achterdeurtjes in encryptieproducten om diensten toegang te geven tot informatie onwenselijk is. Dit introduceert *kwetsbaarheden* die ook door kwaadwillende kunnen worden gebruikt. Ook is dit *niet effectief* gezien het feit dat kwaadwillenden makkelijk via andere wegen aan sterke encryptieproducten kunnen komen.

Wat is er de afgelopen tijd gebeurd?

Nationaal

- JenV is voornemens te verkennen in hoeverre het mogelijk is om OTT-diensten af te tappen. JenV heeft 11 maart jl. hiertoe een brief aan de Kamer gestuurd waarin is aangekondigd dat JenV het gesprek zal aangaan met stakeholders (cybersecurity-experts, bedrijfsleven, wetenschap en maatschappelijk middenveld) inzake het aftappen van OTT-dienstverleners.
- Deze brief is verzonden naar aanleiding van mediaberichtgeving en maatschappelijke weerstand omtrent dit dossier. Zo werd in diverse mediaberichten gewezen op het gebrek aan kennis en expertise op encryptiedossier en de negatieve gevolgen van het afzwakken van end-to-end encryptie ten behoeve van het aftappen van OTT-diensten.
- Naar aanleiding daarvan hebben JenV en EZK plannen gemaakt voor het starten van een gezamenlijk traject met stakeholders.
- In een eerste politiek stakeholdersoverleg heeft de minister van JenV meegegeven dat in individuele gevallen er toch rechtmatige toegang tot communicatie gerealiseerd moeten worden. Stakeholders hebben aangegeven dat deze discussie op internationaal/mondiaal niveau gevoerd moet worden en zich zou moeten toespitsen op het verbeteren van de toegang tot inhoud (bevoegdheden & innovatieve methoden) en niet op beschermingstechniek (encryptie). Door middel van ambtelijke sessies (7 en 8 juli 2021) is er follow-up gegeven aan dit overleg. Gedurende de sessies hebben stakeholders gewezen op de veiligheidsrisico's van het afzwakken van encryptie en ervoor gepleit dat alternatieve opties meegewogen worden.

Europa

- De lidstaten hebben in een EU-raadsverklaring van 14 december jl. aan de Europese Commissie gevraagd om samen met internetdienstverleners en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs zonder daarbij de encryptie af te zwakken.
- De eerste stappen zijn hierin gezet. De Europese Commissie heeft een questionnaire uitgezet waar de lidstaten op hebben kunnen reageren. JenV heeft samen met EZK de beantwoording verzorgd.

Wat gaat er de komende tijd gebeuren?

Nationaal

- Gelet op de demissionaire-status van het kabinet worden er voorlopig nog geen vervolgstappen ondernomen. JenV heeft in samenwerking met EZK een formatiefiche ontwikkeld inzake het aftappen van OTT-dienstverleners.
- In het fiche wordt voorgesteld dat indien het nieuwe kabinet follow-up wil geven aan dit traject inzake het aftappen van OTT-diensten, het onderzoek voortgezet moet worden naar de mogelijke innovatieve (technische) oplossingen binnen de gestelde kaders - sterke encryptie en beveiliging ter bescherming van fundamentele rechten en rechtmatige toegang tot communicatie in specifieke gevallen. Dit betreft dan ook een breed stakeholdertraject. EZK heeft ervoor gepleit dat hierbij ook alternatieve opties m.b.t. bevoegdheden en methoden worden meegenomen.
- Verder wordt voorgesteld om een formele onafhankelijke adviescommissie in te stellen met wetenschappers en experts op het terrein van opsporing, nationale veiligheid, openbare orde, slachtofferrechten, strafrecht, mensenrechten (waaronder een civil society component), persvrijheid, cybersecurity en communicatietechnologie.
- De Cybersecurity Raad heeft een onafhankelijke subcommissie ingesteld welke onderzoek zal doen naar alternatieve middelen tot toegang tot inhoud van OTT-communicatiediensten. Dit onderzoek wordt sterk toegejuicht door EZK.

Europa

- Het blijven steunen en politiek aanjagen van de verkenning van mogelijke technische oplossingen door de Europese Commissie, waartoe is opgeroepen in een raadsverklaring in december 2020. Temeer omdat dit een grensoverschrijdend vraagstuk is en een Europese oplossing effectief kan zijn waar het wereldwijd opererende (OTT) spelers betreft.

Verwachte politieke punten tijdens het AO

- Encryptie is een gevoelig dossier binnen de Kamer. Een meerderheid in de Kamer hecht veel waarde aan sterke encryptie, privacy en borging van betrouwbaarheid van communicatiesystemen en heeft november jl. nog een motie aangenomen welke het belang van sterke encryptie voor communicatie tussen burgers onderschrijft (motie Baudet).

Q&A 1 van 4: Encryptie**Vraag:**

Deelt u de mening dat sterke encryptie cruciaal is voor onze voor digitale samenleving?

Antwoord:

- In dit tijdperk van verdergaande digitalisering dient de digitale omgeving veilig en betrouwbaar te zijn voor burgers, bedrijven en ook overheden. Dit betekent dat burgers en bedrijven op een veilige manier willen en moeten kunnen communiceren.
- Om het vertrouwelijke karakter van hun diensten te waarborgen passen steeds meer communicatiedienstverleners, zoals de aanbieders van Over-The-Top diensten, sterke encryptie toe zoals end-to-end encryptie.
- Sterke encryptie zoals end-to-end encryptie betekent dat de inhoud van communicatie van de afzender aan de ontvanger versleuteld is en de aanbieder van de online dienst geen sleutel heeft om de communicatie in te zien. Hiermee wordt het vertrouwelijke karakter gewaarborgd.
- Sterke encryptie, zoals end-to-end encryptie, is dan ook cruciaal voor onze digitale samenleving en beschermt onze maatschappij dan ook tegen derden met kwaadwillende doeleinden zoals cybercriminelen.
- Verdere besluitvorming is aan een volgend kabinet.

Q&A 2 van 4: Encryptie

Vraag:

Deelt u de mening dat 'end-to-end versleuteling' van gegevens nodig is om burgers en bedrijven veilig te laten communiceren via internet, WhatsApp of andere vergelijkbare diensten?

Antwoord:

- De mening van het kabinet over versleuteling is weergegeven in het kabinetsstandpunt van 4 januari 2016. Dit standpunt is sindsdien niet veranderd. Bovendien heeft de Kamer onlangs ingestemd met motie Baudet waarin de regering wordt opgeroepen niet akkoord te gaan met enig voorstel om versleuteling van berichtgeving te verbieden. Deze motie is complementair aan het kabinetsstandpunt inzake encryptie.
- Sterke encryptie heeft tot doel om de vertrouwelijkheid van communicatie te beschermen en daarmee de cyberveiligheid te versterken. Iets wat extra gewenst is nu de statelijke dreigingen toenemen en wat recent heeft geleid tot het opleggen van extra beveiligingsmaatregelen aan mobiele netwerkkoperators om o.a. hun berichtenverkeer extra te beveiligen.
- Het is dan ook niet wenselijk om sterke encryptie in algemene af te gaan zwakken. Dit schaadt het vertrouwen van afnemers in de digitalisering en daarmee de digitale economie. Het vergroot immers het risico op misbruik van kwaadwillende derden
- Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigingsklimaat. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de groeipotentie van de economie, die vooral zit in de digitale economie.
- Overigens is een sterke encryptie ook een speerpunt van overheidsdiensten. Een goede beveiliging (via encryptie) van tussen overheid en bedrijfsleven/burgers gewisselde gegevens is hiervoor een randvoorwaarde.
- Verdere besluitvorming is aan een volgend kabinet.

Q&A 3 van 4: Encryptie

Vraag:

Moeten OTT dienstverleners (Whasapp etc) end-to-end encryptie verzwakken ?

Antwoord:

- Aanbieders van Over-The-Top diensten zoals Whatsapp passen onder meer end-to-end encryptie toe. Hiermee wordt persoonlijke en vertrouwelijke informatie beschermd van de gebruikers van dergelijke diensten.
- Het toepassen van sterke encryptie w.o. end-to-end encryptie betekent dat de sleutel om te decrypten (ontsleutelen) niet bij de aanbieder van de dienst of bij een derde partij aanwezig is. Elke keer dat gebruikers communiceren, wordt het bericht versleuteld met hun eigen sleutels die verder niemand heeft. Daar kan verder niemand bij. Sleutels beschikbaar stellen aan derden zou de facto tot gevolg hebben dat het sterke karakter van encryptie teniet wordt gedaan omdat een of meerdere (kwaadwillende) partijen over de sleutel (kunnen) beschikken.
- De communicatie is dan ook niet in te zien door derden. End-to-end encryptie is dan ook een belangrijke technologie die bescherming biedt tegen misbruik van derden en bijdraagt aan het versterken van de cyberveiligheid.
- Het verzwakken van deze sterke encryptie zou ertoe leiden dat het beveiligings- en beschermingsniveau van alle afnemers dergelijke chatdiensten afzwakt.
- Verdere besluitvorming is aan een volgend kabinet.

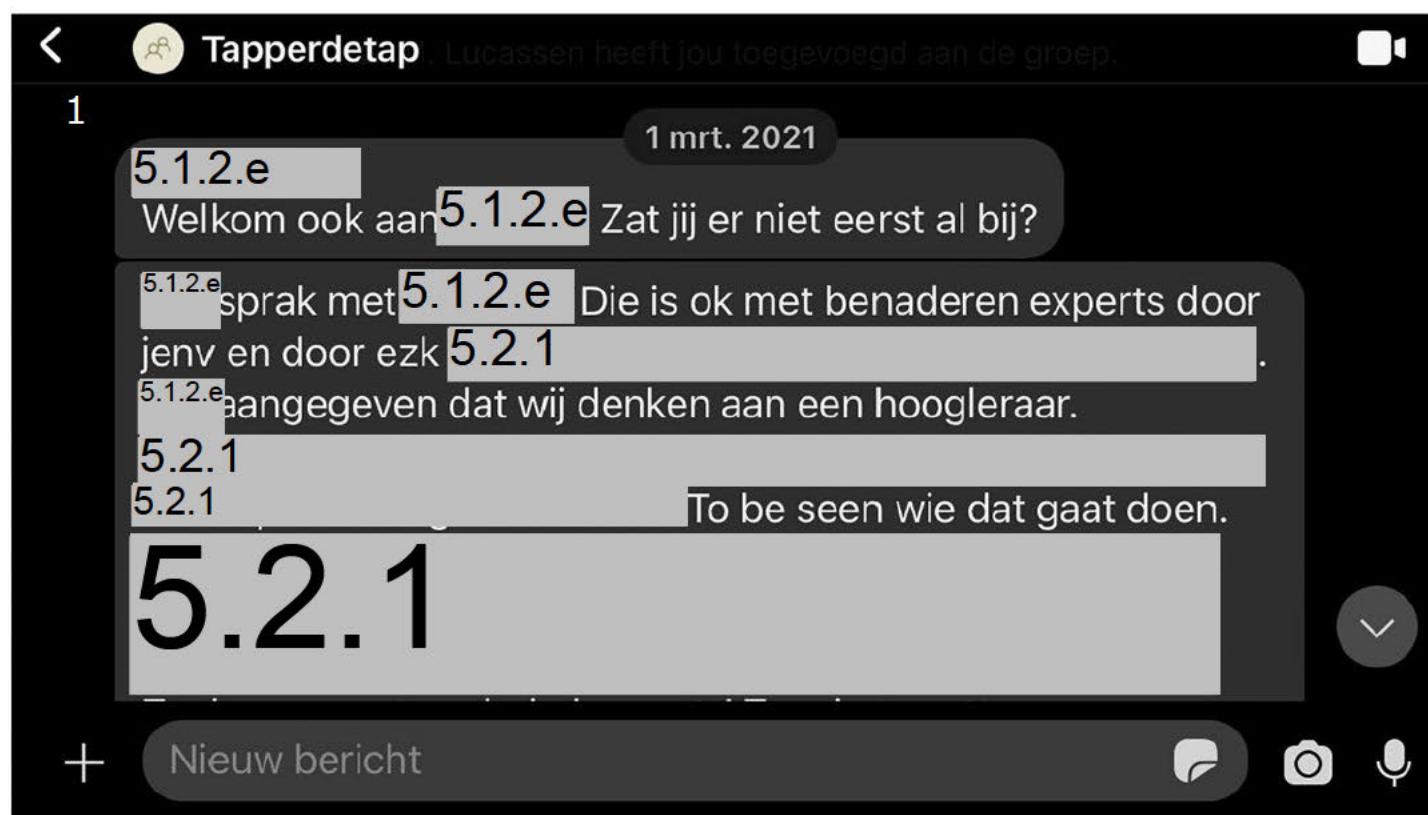
Q&A 4 van 4: Encryptie

Vraag:

Welke nationale en internationale trajecten lopen er momenteel m.b.t. effectieve opsporing met behoud van encryptie ?

Antwoord:

- Het Ministerie van JenV verkent in samenwerking met het Ministerie van EZK in hoeverre het mogelijk om toegang tot digitale inhoud te verkrijgen via de interceptie-bevoegdheden met behoud van sterke encryptie. Dit nationale traject wordt uitgevoerd samen met stakeholders: cybersecurity-deskundigen, bedrijfsleven, wetenschappers en het maatschappelijk middenveld.
- Het nationaal traject bevindt zich de verkennende fase en zal na de vorming van een nieuw kabinet een vervolg krijgen.
- Daarnaast is ook de Europese Commissie een inventarisatie gestart naar de mogelijkheden om technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs zonder daarbij de encryptie af te zwakken. De eerste stappen hierin zijn inmiddels gezet.
- Tot slot wil ik Uw Kamer meegeven dat de Cybersecurity Raad een onafhankelijk onderzoek is gestart naar alternatieve mogelijkheden (dan interceptie) tot toegang tot communicatie van chat-diensten, welke encryptie ongemoeid laten. Ik kijk met veel belangstelling uit naar de uitkomsten hiervan.



5.1.2.e



Tapperdetap

18:06



2

5.1.2.e

1 mrt. 2021

Is wel goed dat onze 5.1.2.e tijdig weet wat voorstel is dat wordt gepresenteerd door expert JenV om daar op te kunnen reflecteren

18:09

5.1.2.e

5.1.2.e

5.1.2.e

Is wel goed dat onze 5.1.2.e tijdig weet wat voorstel is dat wordt gepresenteerd door expert JenV om daar op te kunnen reflecteren

5.1.2.e

5.2.1

18:26



Nieuw bericht





Tapperdetap



3

5.1.2.e

2 mrt. 2021

Vanmiddag 1500 spreek ik met AZ 5.1.2.e en JenV 5.1.2.e

Zit beetje te dubben of we 5.1.2.e alvast kunnen gaan polsen. 5.1.2.e heeft 5.1.2.e gezegd dat we aan een hoogleraar denken en dat werd niet meteen categorisch afgewezen.

5.2.1

5.1.2.e

5.2.1

Wat jullie?

08:52

5.1.2.e

Ik zou hem al polsen. Is kortdag en als wij als belangrijke stakeholder dit willen en met neutrale en gerepresenteerd



Nieuw bericht







Tapperdetap

09:32



5

5.1.2.e

06

5.1.2.e

5.2.1

5.1.2.e

5.2.1

Hij weet via

5.1.2.e

dat we hem willen bellen

09:57

5.1.2.e

Inmiddels ben ik door

5.1.2.e

benaderd. Kent de

materie en kent ook law. Zij nummer is

+31 6

5.1.2.e

12:50



5.1.2.e

van ncsc heeft me zojuist tel benaderd. Hij had geluiden

opgevangen - informeel, nog ver onder de radar - dat nctv

ncsc zou hebben gevraagd om op directeuren niveau dus

5.1.2.e

tijdens mcev expert meeting te laten spreken. Welk geluid



Nieuw bericht





Tapperdetap



matene en kent ook law. Zij nummer is +31 6 5.1.2.e

2 mrt. 2021

12:50

6

5.1.2.e van ncsc heeft me zojuist tel benaderd. Hij had geluiden opgevangen - informeel, nog ver onder de radar - dat nctv ncsc zou hebben gevraagd om op directeuren niveau dus 5.1.2.e tijdens mcev expert meeting te laten spreken. 5.2.1

5.2.1

5.1.2.e

Thx 5.1.2.e heeft met 5.1.2.e gesproken die is bereid het te doen



Nieuw bericht





Tapperdetap



7

wetenschapper te kiezen

2 mrt. 2021

14:05



5.1.2.e

Thx. 5.1.2.e heeft met 5.1.2.e gesproken, die is bereid het te doen. Wil graag meer info over hoe en wat, kunnen we hem bieden maar eerst even gesprek met Az en JenV zodadelijk.

14:07

OK mooi

15:51



5.1.2.e

Zijn jullie belbaar?



Nieuw bericht







Tapperdetap

De groepsooproep is beëindigd - 2 mrt. 2021 16:05



9

5.1.2.e

2 mrt. 2021

Ik heb geen geluid

5.1.2.e

Kan FaceTime?

16:07

5.1.2.e

Meteen maar met 5.1.2.e van AZ gesproken. Zij is het helemaal eens met wat de kern van de discussie moet zijn: heeft dezelfde vraag gehoord als 5.1.2.e 5.2.1

5.2.1

Ze gaat een voorstel maken inclusief vraagstelling, strakke rolverdeling en tijdslots; komt morgenochtend mijn kant op. Let's take it from there.

17:25



Nieuw bericht







Tapperdetap

11

5.1.2.e

3 mrt. 2021

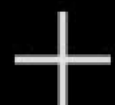
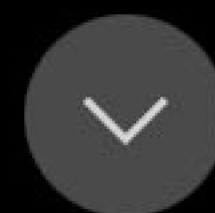
5.2.1

5.1.2.e

5.2.1

5.1.2.e

Goed gesprek gehad met 5.1.2.e ruim 40 minuten. Opzet presentatie doorgelopen en het verloop van zo'n vergadering besproken. Hij kan goed uit de voeten met de opzet, zowel qua volgorde sprekers (eens met ons om na 5.1.2.e te gaan) als



Nieuw bericht





Tapperdetap

5.2.1



5.2.1

12

3 mrt. 2021

PS Ik ga vanavond nog even in de weer met de mail van AZ (eerst ff eten en kids naar bed). Mail die eerst aan jullie voor commentaar voordat ik hem met 5.1.2.e en 5.1.2.e deel.

18:12

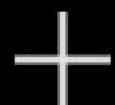
5.1.2.e

Dank voor update 5.1.2.e en klinkt goed. Ik had het met 5.1.2.e erover om alvast nota voor stas voor te bereiden. Met vragen die zij kan stellen

19:04

5.1.2.e dat is mooi, fijn te horen dat hij eens is met volgorde

5.1.2.e en subvragen. Het laatste Mbt alternatieven op EU



Nieuw bericht





3 mrt. 2021

5.1.2.e dat is mooi, fijn te horen dat hij eens is met volgorde na 5.1.2.e en subvragen. Het laatste Mbt alternatieven op EU level vind ik heel interessant.

19:11

5.1.2.e

5.1.2.e

Goed gesprek gehad met 5.1.2.e ruim 40 minuten. Opzet presentatie doorgelopen en het verloop van zo'n vergadering besp...

Ah mooi zeg.

19:51



Nieuw bericht





14

5.1.2.e

3 mrt. 2021

5.1.2.e

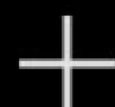
Dank voor update 5.1.2.e en klinkt goed. Ik had het met 5.1.2.e
erover om alvast nota voor stas voor te bereiden. Met vragen die zij...

Goed plan. 5.2.1

5.2.1

21:11

Heb voorstel voor wat ik aan AZ en JenV wil sturen net gemaild.
Als nog lukt dan zou het fijn zijn als er nog iemand kan
meelezen voor ik het verstuur. NB heb morgen 09.00 al overleg



Nieuw bericht





21:57

3 mrt. 2021

5.1.2.e

Synchronisatie mail werkt niet, dus kan niet meelezen via mail

22:11

5.1.2.e

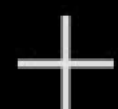
Aiii... ik heb ook last maar als ik op de cloud inlog lukt het me wel.

22:12

5.1.2.e anders even cash legen op pc

22:13

5.1.2.e



Nieuw bericht





Tapperdetap



5.1.2.e

5.1.2.e lukt, reageer per mail

3 mrt. 2021

16

Cache legen bedoelde ik. iPhone toetsenbord vervangt zelf getypte woorden.

22:16



4 mrt. 2021



Overheid werkt aan plan voor afzwakken encryptie: 'Taak v...

De overheid werkt nog steeds aan plannen om de beveiliging van chatberichten af te



Nieuw bericht





17

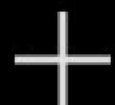
5.1.2.e

3 mrt. 2021

Goed gesprek gehad met 5.1.2.e ruim 40 minuten. Opzet presentatie doorgelopen en het verloop van zo'n vergadering besproken. Hij kan goed uit de voeten met de opzet, zowel qua volgorde sprekers (eens met ons om na 5.1.2.e te gaan) als qua subvragen (wat betekent tappen voor E2E encryptie, wat zijn de consequenties, zijn er alternatieven). Belangrijk: Hij heeft serieuze ideeën voor alternatieven, waarbij geldt dat die echt alleen op EU niveau gerealiseerd kunnen worden 5.2.1

5.2.1

PS Ik ga vanavond nog even in de weer met de mail van AZ



Nieuw bericht



5.1.2.e



Tapperdetap

07:50



18

5.1.2.e

4 mrt. 2021

Hmmm

Hoe komen er aan?

5.1.2.e

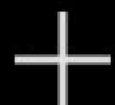
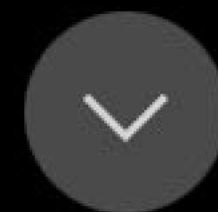
Het veld? 07:55

5.1.2.e

Illustreert maar weer de controverse van dit onderwerp. Staat veel info in, ook over onze positiewisseling (?). Dus goed geïnformeerd.

5.2.1

5.2.1



Nieuw bericht



5.1.2.e



19

W 4 mrt. 2021 men ze aan al die info?

09:01 

5.1.2.e

5.2.1

5.1.2.e

5.1.2.e

5.2.1

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



5.1.2.e

09:09

4 mrt. 2021

20

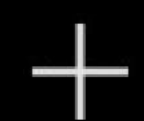
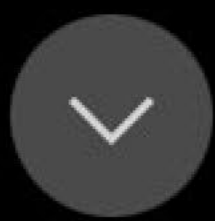
5.2.1 09:10

5.1.2.e
5.2.1

Verder: zie mailbox voor comentaar 5.1.2.e 5.2.1
5.2.1

5.1.2.e

5.1.2.e



Nieuw bericht





Tapperdetap



5.1.2.e

5.1.2.e

Ik stuur wat comments

09:

4 mrt. 2021

21

5.1.2.e

Eens, Mona

5.1.2.i

5.1.2.i

09:13

5.1.2.e

5.1.2.e

Ah zo

09:13

5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap



22

5.1.2.e

4 mrt. 2021

Ik vind het beeld niet kloppen, EZK was altijd kritisch over encryptie. Ook in het voortraject.

09:14

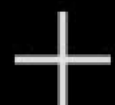
5.1.2.e

Is een bijpraat zo handig?

09:30

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap

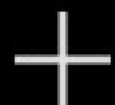


23

5.2.1

5.2.1

5.1.2.e



Nieuw bericht





Tapperdetap



5.1.2.e

5.2.1

21:10

4 mrt. 2021

24

5.2.1

5.1.2.e

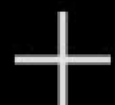
5.1.2.e
je?

is morgen de opzet van de sessie definitief denk

5.1.2.e

dan neem ik aan dat we interne nota maken en dergelijke?

21:22



Nieuw bericht



5.1.2.e



Tapperdetap



25

5.1.2.e

4 mrt. 2021

Ik zag dat 5.1.2.e en 5.1.2.e van ezk ook in die groep
zitten. 5.2.1

5.1.2.e

5.2.1

5.2.1



Nieuw bericht





Tapperdetap



5.1.2.e

26

Maar aan ons zal het niet liggen. 4 mrt. 2021. Heb overigens nog niet gereageerd naar 5.1.2.e was ook wel benieuwd of JenV nog wat zou hebben maar die zijn nog stil.

5.1.2.e

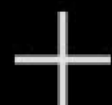
dan neem ik aan dat we interne nota maken en dergelijke?

Die nota zou ik idd maar alvast gaan opstellen. Moet volgende week vast nog aangepast maar zaak om daar alvast de basis voor te hebben klaarstaan.

21:25



iii



Nieuw bericht





Tapperdetap



27

5.2.1

Ok helder. Overigens sluit ik obv de mail niet uit dat die website
vóór 12/3 de lucht in gaat..

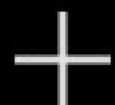
21:36

5.1.2.e

5.2.1

5.1.2.e

Veel wetenschappers zitten in hoek van critici. Er is



Nieuw bericht





28

5.1.2.e

4 mrt. 2021

Veel wetenschappers zitten in hoek van critici. Er is wetenschappelijke consensus dat plannen leiden tot verzwakking beveiliging

21:56

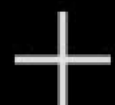
<https://berthub.eu/articles/posts/end-to-end-encryption-european-internet-forum/>

22:23

5.1.2.e

: ik snap de wens, maar zie geen reële mogelijkheid zonder vervelende bijeffecten

22:34



Nieuw bericht





Tapperdetap



29

5.1.2.e

5 mrt. 2021

5.1.2.e

Ha mensen, is de opzet voor volgende week nu rond toevallig?

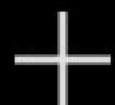
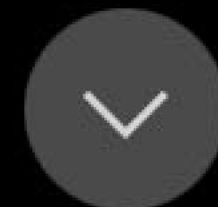
14:29

5.1.2.e

5.2.1

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



30

5.1.2.e

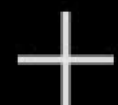
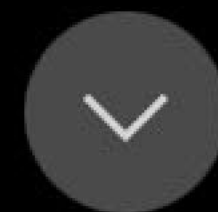
5.2.1

5.2.1

5.2.1

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



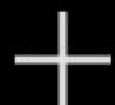
31

5.2.1

17:01

Niet voor nu (weekend!) maar wel voor maandag first thing:
Heb jullie concept antwoorden van JenV op KVs **5.1.2.e**
over ons favo onderwerp gestuurd. Onze reactie moet
maandag einde ochtend hun kant op **5.1.2.e** wil vóór 9/3
antwoord). Als wij dat nog door de lijn moeten trekken wordt
dat een uitdaging...

19:43



Nieuw bericht



5.1.2.e



Tapperdetap

19:43



32

5.1.2.e

5 mrt. 2021

Dank voor de attentie. Goeie kritische vragen las ik;) mijn mail synchroniseert btw nog steeds niet via telefoon. Fijn weekend vast.

20:12

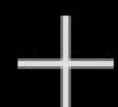
8 mrt. 2021

5.1.2.e

Morning all, kunnen jullie even kijken naar mijn mail over de KVs. Geef vooral tegengas als jullie anders zien!

09:33

Heb net gereageerd via mail. Groen is juiste toevoeging en mbt



Nieuw bericht



5.1.2.e



Tapperdetap

5.1.2.e al tegengas als jullie anders zien!

09:33



33

8 mrt. 2021

Heb net gereageerd via mail. Groen is juiste toevoeging en mbt paars verzoek aan jenv cc az die te schrappen.

09:35



5.1.2.e

Eens

En wat mij betreft kunnen we evt toevoegen dat EZK effecten wil laten onderzoeken

Zoals al in het eerdere NOS bericht staat

09:46



5.1.2.e

de club rondom het kartel van 5.1.2.e gebruikte



Nieuw bericht



5.1.2.e



Tapperdetap



34

8 mrt. 2021

Heb net gereageerd via mail. Groen is juiste toevoeging en mbt paars verzoek aan jenv cc az die te schrappen.

09:35

5.1.2.e

Eens

En wat mij betreft kunnen we evt toevoegen dat EZK effecten wil laten onderzoeken

Zoals al in het eerdere NOS bericht staat

09:46

5.1.2.e

de club rondom het kartel van 5.1.2.e gebruikte



Nieuw bericht





Tapperdetap



35

8 mrt. 2021

5.1.2.e de club rondom het kartel van 5.1.2.e gebruikte
toch ook eigen aangemaakte encryptie?

09:56

5.1.2.e

Zie mailbox voor nieuwe versie antwoorden op KVs 5.1.2.e
Graag zsm reactie.

Verder: zie onderstaand de concept spreeklijn van 5.1.2.e

5.2.1

5.2.1

Benieuwd naar jullie observaties, ik kijk
zelf vanmiddag ook nog.

12:46



Nieuw bericht





Tapperdetap



36

brandkast te verschaffen. ' 8 mrt. 2021 t uiteindelijk ook. Het bij de
betrokkene opeisen van de sleutel van de brandkast mag niet, vanuit
het nemo tene...

Meer lezen

12:52

Mooi 5.1.2.e zegt dat THTC, NCSC, NBV tegen het voorstel zijn.
Kan 5.1.2.e het op de drie organisaties afpellen? Per org waarom
ze het niet willen. Is inhoudelijk ook sterk.



Nieuw bericht





37

5.1.2.e

Verder vind ik het een goed 8 mrt. 2021 de tekst btw. Geen blad voor de mond.

13:53

5.1.2.e

Mcev as vrijdag wordt ingekort tot 30 minuten. Zit nu met az en jenv in de mail te ballen over wat dat betekent. Ik zet in op kortere inleiding, 2x 10 min presentaties, 5 min voor evt vragen en afronding. Die vragen moeten dan puur technisch zijn;

5.2.1

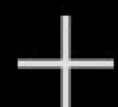
5.1.2.e

5.2.1

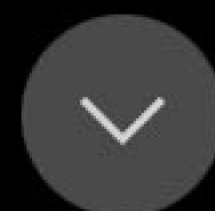
14:14

5.1.2.e

Ik hoorde het bij DMD een korte Verkeers over de plannen van



Nieuw bericht





Tapperdetap



14:14

8 mrt. 2021

38

5.1.2.e

Ik hoorde net bij BNR een boze 5.1.2.e over de plannen van JenV inzake encryptie

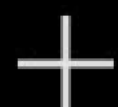
hij vindt het belachelijk en zelfs gevaarlijk voor de democratie dat het kabinet dit in zijn demissionaire status doet (was de strekking)

15:54

5.1.2.e

5.2.1

15:55



Nieuw bericht



5.1.2.e



Tapperdetap



39

5.1.2.e

8 mrt. 2021

5.2.1

15:55

9 mrt. 2021

5.1.2.e

5.1.2.e

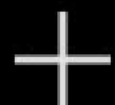
kan een van jullie achterhalen wat laatste stavaza met Europese onderzoek is?

09:39

5.1.2.e

Goeie 5.1.2.e misschien dat 5.1.2.e op de pv daar wat in kan betekenen. Moeten even precies weten hoe het zit.

09:45



Nieuw bericht





40

Ik begin met een uitgeschr 8 mrt. 2021 ntenlijn. Die kan dan later omgezet worden in bullet-points.

1. In de fysieke wereld kan de vraag gesteld worden: kan een burger een geheim in een brandkast verbergen zodat de overheid er niet bij kan? Het traditionele antwoord is: Nee! De overheid heeft machtsmiddelen om zich met fysiek geweld toegang tot de inhoud van de brandkast te verschaffen. Vaak lukt dat uiteindelijk ook. Het bij



Nieuw bericht





Tapperdetap



5.1.2.e

41

5.1.2.e

kan e 9 mrt. 2021

achterhalen wat laatste

stavaza met Europese onderzoek is?

09:39

5.1.2.e

Goeie 5.1.2.e

d, misschien dat 5.1.2.e

op de pv daar wat in kan

betekenen. Moeten even precies weten hoe het zit.

09:45

5.1.2.e

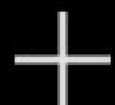
Ik ga mee naar MCEV,

5.1.2.e

doet 23/3 (meer onderwerpen op

agenda)

09:46



Nieuw bericht



5.1.2.e



Tapperdetap



42

5.1.2.e

9 mrt. 2021

Ik zal 5.1.2.e vragen

5.1.2.e

Oh 5.1.2.e is me voor;) 09:55

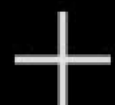
Ben ook zoek naar 06 maar nergens te vinden 10:02



5.1.2.e

Je kan Bellen naar de PV zelf

Die verbinden je door 11:31



Nieuw bericht





Tapperdetap



43

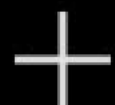
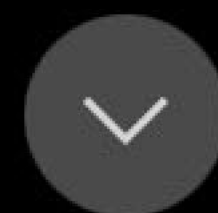
5.2.1

5.1.2.e

5.2.1

5.1.2.e

Begreep van 5.1.2.e dat hij het onderwerp
donderdag in CSR ook aan de orde stelt. Prima wat mij betreft



Nieuw bericht





Tapperdetap



44

5.1.2.e

Begreep van 5.1.2.e 9 mrt. 2021 het onderwerp
donderdag in CSR ook aan de orde stelt. Prima wat mij betreft
om geluid uit wetenschap te laten horen. 5.2.1

5.2.1 5.1.2.e zit ook in CSR.

11:56

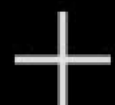
5.1.2.e

ledereen akk met concept mail AZ tbv mcev? 12:47

5.1.2.e

Ja

12:57



Nieuw bericht



5.1.2.e



Tapperdetap



45

5.1.2.e

9 mrt. 2021

Publiciteitsoffensief van politie over kraken encryptie en opsporen grootschalige criminaliteit. 5.2.1 Kunnen wij achterhalen hoe dit precies zit?

5.1.2.e

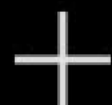
Toont wel aan dat de echte criminelen niet op whatsapp zitten.. 19:40

Zag het net ook. Wonderbaarlijk.

Zal morgen collega bij politie contacten. 19:43



5.1.2.e



Nieuw bericht





Tapperdetap



46

5.1.2.e

9 mrt. 2021

Las het ook!

Mede nav dit bericht:

5.2.1

5.2.1

5.2.1

maar het is duidelijk dat ook in andere

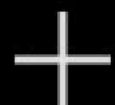
takken van criminaliteit het ontsleutelen van OTT niet de silver bullet gaat zijn.

19:51

By the way, ends 2 end start helemaal los van kp. Kp wordt veelal gedownloadven geupload van darkweb. Ferd heeft die thema's voor het gemak met elkaar verbonden. Verhaal

5.1.2.e het liefst los van kp.

19:57



Nieuw bericht





Tapperdetap

19:57



47

5.1.2.e

9 mrt. 2021

5.1.2.e Eens. Daarom wil ik het wat aanpassen. 19:58

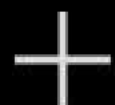
Graag. Mooi 19:58

5.1.2.e

En juist cyber crime krijgt meer kansen bij wegvallen e2e

5.1.2.e Kan dat er ook in? 21:18

Het schijnt dat Politie servers van SKY ECC heeft gekraakt, c
op vordering gecompromitteerd, dat weten we niet zeker. En zo



Nieuw bericht





48

9 mrt. 2021

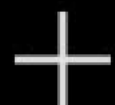
Het schijnt dat Politie van SKY ECC heeft gekraakt, of op vordering gecompromitteerd, dat weten we niet zeker. En zo een MITM (man in the middle attack) geregeld (in feite zelf een backdoor geïnstalleerd)

Dit bewijst dat ze met de CC3 (huidige wet sinds vorig jaar) voldoende bevoegdheden hebben om criminelen te kunnen pakken.

21:20

Vraag is of deze dienst end2end encrypted was of dat deze voorzien was van geniale codering.

21:24



Nieuw bericht





Tapperdetap

21:24



49

5.1.2.e

9 mrt. 2021

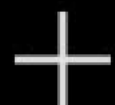
Maar E2E valt te hacken

Althans een apparaat valt te hacken

5.1.2.e

Dat bedoel ik 21:25

5.2.1



Nieuw bericht





Tapperdetap



50

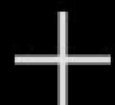
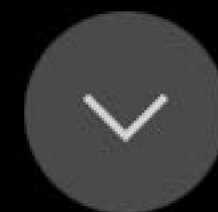
5.2.1

10 mrt. 2021



Brede coalitie richt zich tegen regeringsplannen om encrypti...

Diverse maatschappelijke organisaties en
bedrijven spreken zich uit tegen de
mogelijke inperking van versleuteling wa



Nieuw bericht





Tapperdetap



51

5.1.2.e Breed gesteunde oproep aan
toekomstig kabinet 10 mrt. 2021

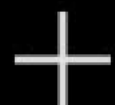
Een brede coalitie van
technologiebedrijven, maatschappelijke
organisaties en privacy-voorvechters ma...

www.volkskrant.nl · 10 mrt. 2021

[https://www.volkskrant.nl/cs-
bb59e899](https://www.volkskrant.nl/cs-bb59e899)

5.1.2.e

En VK op de voorpagina van de site 07:14



Nieuw bericht



5.1.2.e



Tapperdetap

Wikipedia: de informatiepagina van de site

07:14



52

5.1.2.e

10 mrt. 2021

5.2.1

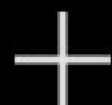
5.1.2.e

5.1.2.e

5.2.1

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



53

5.2.1

07:52

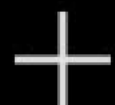
5.1.2.e

5.2.1

Op NRC staat btw een artikel over hacken en aanpakken criminelen



Encryptie is niet meer weg te denken uit het criminele milieu



Nieuw bericht





Tapperdetap



54

Encryptiesoftware: Opnieuw '10 mrt. 2021
Nederlandse politie criminele
communicatie. Hacken is hét wapen in d...

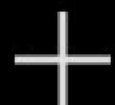
www.nrc.nl

[https://www.nrc.nl/nieuws/2021/03/09/
encryptie-niet-meer-weg-te-denken-
uit-criminele-milieu-a4034876](https://www.nrc.nl/nieuws/2021/03/09/encryptie-niet-meer-weg-te-denken-uit-criminele-milieu-a4034876)

5.1.2.e

Bij mij staat ie achter de betaalmuur helaas 08:02

5.2.1



Nieuw bericht





Tapperdetap



5.1.2.e

5.2.1

55

De cryptotelefoon is ook na de hacks niet meer weg te denken uit het criminele milieu, klinkt het onder telecomtechnen. De beveiliging zal omhoog gaan en mogelijk worden de netwerken kleiner en meer besloten. Maar dat crypto-communicatie blijft, staat buiten kijf, ook voor 5.1.2.e – 5.1.2.e

5.1.2.e

„Ze moeten blijven communiceren.”

Is ook helemaal los op twitter

08:07



5.1.2.e



Nieuw bericht





Tapperdetap

Is ook helemaal los op twitter

08:07



56

5.1.2.e

5.1.2.e

10 mrt. 2021

5.2.1

Meeste berichten gaan over beweging van BOF en gisteren ingrijpen op SKY

5.1.2.e

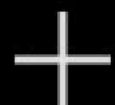
08:14



5.1.2.e

Wat VK mooi vloodlegt is dat de natuurlijke tegenpolen van privacy activisten en big tech, met steun van de wetenschap, verenigd zijn in hun verzet tegen voornemens JenV.

09:05



Nieuw bericht



5.1.2.e



Tapperdetap



57

5.1.2.e

10 mrt. 2021

Fyi: Nota voor deze MCEV ligt bij klas 09:46

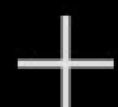
Btw soortgelijk nieuwsbericht over plannen JenV inzake encryptie ook op de site van NRC sinds 9:15 10:13

Heel even: welke concrete taken moeten we nog doen richting deze MCEV voorbereiding? 10:43

5.1.2.e

5.1.2.e

gisteren drie keer 5.1.2.e benaderd ivm svz F...
onderzoek. Zojuist reminder gemaild. Nog steeds geen
antwoord



Nieuw bericht





Tapperdetap



11:00

58

10 mrt. 2021

5.1.2.e

Anders kunnen 5.1.2.e even het hoofd van de EZ afdeling vragen als we dit spoedeisend vinden?

11:01

Heb haar aan telefoon

11:02

Zo ver we kunnen zien nog geen actie op EU onderzoek

12:27

5.1.2.e

Heb je nog meer info 5.1.2.e

12:39



Nieuw bericht



5.1.2.e



Tapperdetap

5.1.2.e



10 mrt. 2021

59

5.1.2.e

Mbt derogatie op de man, mbt onderzoek, heeft een hoop dics/mails doorgespit maar kon niets vinden over start onderzoek. De EC moet dat initiëren en anders onder druk van LS.

12:42

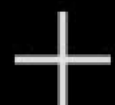


5.1.2.e

Thx. Kan 5.1.2.e niet even iemand (laten) bellen bij de cie?
Alleen een check op haar inbox vind ik te mager.

12:50

5.2.1



Nieuw bericht



5.1.2.e



10 mrt 2021

60

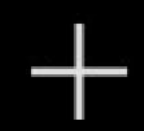
5.2.1

ik zie het al m in mijn vorig bericht, mail sloeg op terugkoppeling inz derogatorie, diebhad ik op de mail gezet

12:56

5.1.2.e

Het gaat me nu even niet om de derogatie maar om de opvolding van de raadsconclusies. Zou goed zijn om daarover



Nieuw bericht





Tapperdetap

12:56



61

5.1.2.e

10 mrt. 2021

Het gaat me nu even niet om de derogatie maar om de opvolging van de raadsconclusies. Zou goed zijn om daarover met cie te (laten) bellen.

12:58

Deze terugkoppeling ging niet over derogatorie maar over opvolging raadsconclusies. Even bellen

13:09

5.1.2.e

Krijg net binnen dat de MCEV niet doorgaat vrijdag... 16:47



Heb meteen A7 gebeld en gemarkeerd dat het agendapunt dan



Nieuw bericht





Tapperdetap



62

Heb meteen AZ gebeld en 10 mrt. 2021 dat het agendapunt dan ook van de mcev van 23/3 moet worden afgehaald; dat waren ze met me eens.

5.2.1

5.2.1

5.1.2.e

5.2.1

16:52

5.1.2.e

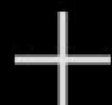
5.1.2.e

Top, ik bel zo ook nog even met 5.1.2.e

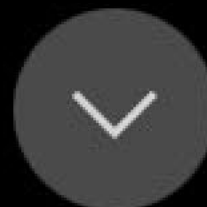
16:53

5.1.2.e

5.2.1



Nieuw bericht



5.1.2.e



Tapperdetap



63

5.1.2.e

10 sept 2021

5.2.1

5.1.2.e

5.1.2.e

Dank 5.1.2.e zou je ook kunnen vragen wat de plannen zijn met de rest van het wetgevingstraject?

16:59

5.1.2.e

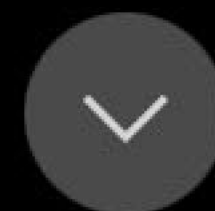
5.1.2.e

Doe ik! 17:00

5.1.2.e



Nieuw bericht





Tapperdetap



64

5.1.2.e

5.1.2.e

Doe ik! 17:00

10 mrt. 2021

5.1.2.e

En je kan vragen naar de nfi presentatie!

5.2.1

5.1.2.e

5.2.1

17:27

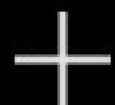
5.1.2.e

5.1.2.e gaat er ook van uit dat er geen verdere besluitvorming is. Hij volgende week overleggen met ons over hoe nu verder.

5.1.2.e

Grapperhaus stuurt vanavond nog brief naar TK. Checken jullie bij 5.1.2.e

17:29



Nieuw bericht



Tapperdetap

10 mrt. 2021

Doe ik! 17:31

5.1.2.e

5.2.1

17:33

5.1.2.e

Er is idd een brief. Zie bijlage. Graag zsm reactie, JenV maakt

Nieuw bericht

5.1.2.e



Tapperdetap

17:48



66

5.1.2.e

10 mrt. 2021

5.1.2.e

Yes done 18:26

5.1.2.e

5.1.2.e

Reactie Stas: mooi 19:41

5.1.2.e

5.1.2.e

Mooi teamwork van ons allemaal 👍 20:38

Eens. top 👍 20:39



5.1.2.e



Nieuw bericht





Tapperdetap



67

11 mrt. 2021

Just because you don't see cyber threats,
doesn't mean they're not there.

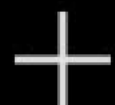


FOX IT
part of necgroup

Call us before
you need us.

5.1.2.e

Sterke encryptie onmisbaar
voor onze veiligheid – Fox-IT



Nieuw bericht





68

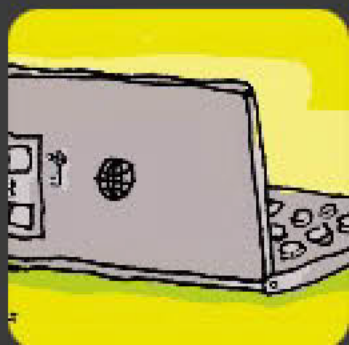
5.1.2.e

<https://www.fox-it.com/nl/actualiteiten/ingestuurde-sterke-encryptie-onmisbaar-voor-onze-veiligheid/> 11 mrt. 2021 08:14

5.1.2.e

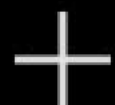
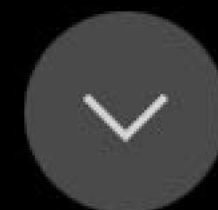
5.1.2.e

Op FD staat er ook een opinie stuk over



Grapperhaus legt een bom onder veilig internet

Het ondermijnen van versleuteling is en blijft technisch onmogelijk, economisch



Nieuw bericht





Tapperdetap



69

Het ondermijnen van versleut 11 mrt. 2021
blijft technisch onmogelijk, economisch
rampzalig, juridisch onhaalbaar en zowel...

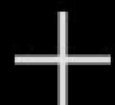
fd.nl

[https://fd.nl/opinie/1376523/
grapperhaus-legt-een-bom-onder-
veilig-internet](https://fd.nl/opinie/1376523/grapperhaus-legt-een-bom-onder-veilig-internet)

10:03

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



70

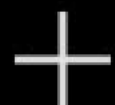
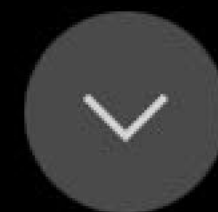
5.1.2.e

5.2.1

5.1.2.e

5.1.2.e

Ik stel voor dat we eerst met JenV om tafel gaan. Is ook al zo
besproken. Moeten nu kijken of we in gezamenlijkheid de



Nieuw bericht



5.1.2.e



Tapperdetap



71

5.1.2.e

Ik stel voor dat we eerst m. 11 mrt. 2021 .afel gaan. Is ook al zo besproken. Moeten nu kijken of we in gezamenlijkheid de volgende stappen kunnen bepalen. Het Europese spoor is er daar een van.

10:19

5.1.2.e

Dat staat in raadsconclusies. Komt voort uit encryptie dossier waar 5.1.2.e en ik had op hebben ingezet. Belangrijk is dat in EU verband gezamenlijkheid bekend wordt weekje innovatieve opsporings mogelijkheden er zijn. Dat is de kern. Anders blijft die over de boeg van vele dossiers spelen. Dus jenv aanmoedigen hier bij de cie op aan te dringen. Dus via PV jenv.



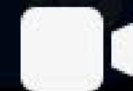
Nieuw bericht





Tapperdetap

10:20



72

5.1.2.e

11 mrt. 2021

Ik zou ook aanbevelen om de telecom werkgroep hierbij te betrekken en niet te passeren. Dus zowel justitie als telecom gelederen uit de EU betrekken voor een compleet beeld. Maar we bespreken dit nog wel op korte termijn.

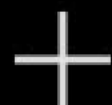
10:22

5.1.2.e

5.1.2.e

5.2.1

5.1.2.e



Nieuw bericht





Tapperdetap

10:25



73

5.2.1

5.1.2.e

5.2.1

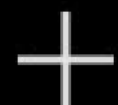
5.2.1

5.1.2.e



dacht dat die al rond was

13:02



Nieuw bericht



5.1.2.e



Tapperdetap

13:01



74

11 mrt. 2021

...acht dat die al rond was

13:02

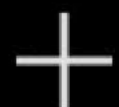


5.1.2.e

5.2.1

5.1.2.e

Nieuwe brief in jullie inbakken. 17:01



Nieuw bericht



5.1.2.e



Tapperdetap



Leuven en nu in jullie inbakken. 17:01

11 mrt. 2021

75

5.1.2.e

Terugkoppeling 5.1.2.e CSR: oproep om advies van CSR. Bezien wat goede timing is. Ook goed om aan te sluiten bij Europese onderzoek.

17:40

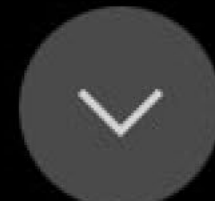
5.1.2.e

5.1.2.e

5.2.1

5.1.2.e

19:37



Nieuw bericht





76

5.1.2.e

11 mrt. 2021

5.2.1

5.1.2.e

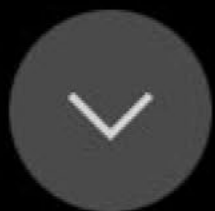
Dank 5.1.2.e zou je ook kunnen vragen wat de plannen zijn met de rest van het wetgevingstraject?

5.1.2.e

had je toevallig van JenV nog gehoord hoe het met de rest



Nieuw bericht





Tapperdetap



77

5.1.2.e

had je toevallig van Jer' '11 mrt. 2021' word hoe het met de rest van het wetgevingstraject staat qua planning (roamingdeel)?

19:45

5.1.2.e

5.2.1

5.1.2.e

5.2.1

20:50

5.1.2.e

5.1.2.e

5.2.1



Nieuw bericht



5.1.2.e



Tapperdetap

compositie



20:51



78

5.1.2.e

11 mrt. 2021

<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/03/11/tk-aftapbaarheid-ott-diensten/tk-aftapbaarheid-ott-diensten.pdf>

5.2.1

12 mrt. 2021

5.1.2.e



Nieuw bericht





Tapperdetap



79

5.1.2.e

12 mrt 2021

5.2.1

5.1.2.e

5.2.1

5.1.2.e

5.2.1



Nieuw bericht



5.1.2.e



Tapperdetap



80

5.1.2.e

12 mrt. 2021

JenV pakt onze uitnodiging voor een gesprek op. Willen volgende week met ons om tafel. Zal ik iets inschieten? Aan hun kant betreft het 5.1.2.e Stel voor dat wij ook met 3 man komen.

16:20

5.1.2.e

5.1.2.e

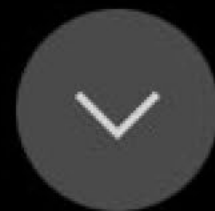
Prima plan.

5.1.2.e

Goed weekend

17:47

13 apr. 2021



Nieuw bericht





Tapperdetap



81

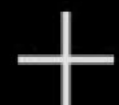
13 apr. 2021

5.1.2.e

Het Forensisch Instituut kan steeds
meer, maar gaat steeds minder doen

5.1.2.e

Het



Nieuw bericht





Tapperdetap



82

5.1.2.e

13 apr. 2021

Het

Nederlands Forensisch Instituut gaat minder onderzoeken doen. „Dit verhoudt...

www.nrc.nl

5.1.2.e

<https://www.nrc.nl/nieuws/2021/04/12/het-forensisch-instituut-kan-steeds-meer-maar-gaat-steeds-minder-doen-a4039515>

11:24



Nieuw bericht





Tapperdetap



83



5.1.2.e 5.1.2.e

toegevoegd.

16 apr. 2021

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



84

5.2.1

Bon weekend!

15:52



5.2.1



Nieuw bericht





5.1.2.e



Tapperdetap



15:52

16 apr. 2021

85

5.2.1

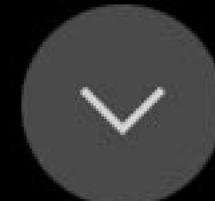
16:16



5.1.2.e

5.2.1

5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap

16:18



86

5.1.2.e

16 apr. 2021

1) wat een briljante naam voor deze appgroep!

2) eens. 5.2.1

5.2.1

Goed om bij de ambtelijke versie aanwezig te zijn. AZ zit hier niet niet tussen toch? 5.2.1

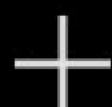
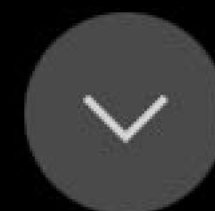
5.1.2.e

5.2.1

16:28

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



87

5.1.2.e

5.2.1

20 apr. 2021

5.1.2.e

5.1.2.e neem jij nog contact op met counterpart bij JenV of zal ik 5.1.2.e benaderen?

12:32

5.1.2.e 5.2.1

5.2.1



Nieuw bericht





Tapperdetap

14:55



88

5.1.2.e

20 apr. 2021

5.1.2.e

Benader jij 5.1.2.e maar 5.1.2.e

15:01

5.1.2.e

Allright

5.2.1

5.1.2.e

Welke nota precies? Over de stakeholdersessies?

15:45



Nieuw bericht





Tapperdetap

20 apr. 2021



89

10 mei 2021

5.1.2.e

Beste allemaal, ik zou graag even kort stavaza willen doornemen op dit dossier. Indien jullie dit ook een redelijk idee vinden dan plan ik even wat in. Grt

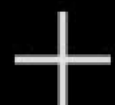
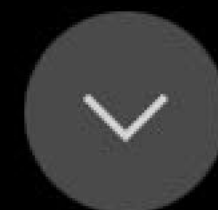
09:57

5.1.2.e

Hallo prima wat mij betreft

10:49

5.1.2.e



Nieuw bericht





Tapperdetap



5.1.2.e

90

5.1.2.e

10 mei 2021

5.1.2.e

Overleg staat nu voor woensdagochtend 20:20

11 mei 2021

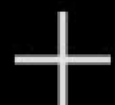
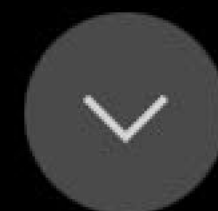


Openbaar Ministerie: encryptie
nooit bedoeld als schild voor...

www.security.nl

5.1.2.e

[https://www.security.nl/posting/
702983/](https://www.security.nl/posting/702983/)



Nieuw bericht



5.1.2.e



Tapperdetap

18:52



91

11 mei 2021

Comments onderaan 😊

18:56



12 mei 2021

5.1.2.e

Precies. Sommige klinken bekend die we in het fiche willen hebben en houden

08:24

5.1.2.e

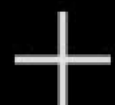
5.1.2.e

Gesprek is 13:30 - 14:30

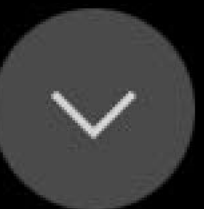
13:57

5.1.2.e

17 mei 2021



Nieuw bericht





Tapperdetap



92

5.1.2.e

17 mei 2021

5.1.2.e

Ha collega's ik heb nog niets vernomen. Jullie wel? 13:04

Nee

13:08



5.1.2.e

BBR stelt dat de Stas denkt dat BZK ook betrokken zou worden in her vervolgtraject met stakoholders.5.2.1

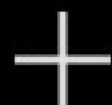
5.1.2.e

5.2.1

17:29



5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap

17 mei 2021



93

18 mei 2021

5.1.2.e

5.1.2.e

van BBR zegt dat Mona wel ff met Ferd vandaag gaat bellen.

10:06

5.1.2.e

5.1.2.e

5.2.1

10:26

5.1.2.e

5.1.2.e

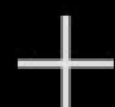
Tja ben benieuwd wat er uit komt

10:40

5.1.2.e



Ingeval hzk aan de orde komt is hz ibkv ELI traject interessant



Nieuw bericht



5.1.2.e



Tapperdetap



94

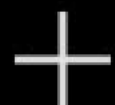
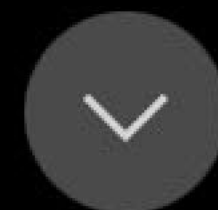
Ingeval bzk aan de 18 mei 2021 s bz ihkv EU traject interessant

10:45

20 mei 2021

5.1.2.e

5.2.1



Nieuw bericht





Tapperdetap



95

5.2.1

5.1.2.e

Meer lezen

16:08

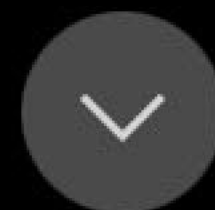
5.1.2.e

Dank voor de info. Ik moet van BBR nog horen of er nog iets is uitgekomen uit gesprek van mona met ferd

Let u know 17:04



Nieuw bericht





Tapperdetap



96

Let u know 17:04

20 mei 2021

5.1.2.e

BBR heeft niks gehoord meer inzake gesprek Mona - Ferd 17:50

28 mei 2021

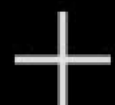
5.1.2.e

Ha allen, ik heb in de nota expres het stukje mbt AT laten staan. Dat heb ik nu afgestemd met 5.1.2.e van AT. Dus wmb laten we dat erin.

Ik kon gisteren gelukkig nog met hem snel schakelen



Bij afwezigheid vaste counterpart



Nieuw bericht





Tapperdetap



97

Ik kon gisteren gelukkig na 28 mei 2021 snel schakelen

5.1.2.e

Bij afwezigheid vaste counterpart 08:12

Mooi 08:18

5.1.2.e

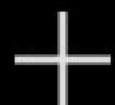
Ok, mocht de vraag van medeparaaf AT nog open staan, 5.2.1

5.1.2.e

5.2.1 dit gaat om beleidsvorming

08:38

Klopt puur afstemming, medeparaf slechts ivm besluitvorming
bewindspersoon



Nieuw bericht





Tapperdetap



98

5.1.2.e

28 mei 2021

5.2.1

5.1.2.e

Dat heb ik met AT besproken 09:15

3 jun. 2021

5.1.2.e

Hoi collega's ik heb met 5.1.2.e bouwstenen ontworpen voor de ambtelijke sessies. Willen jullie daar eerst nog even naar kijken voordat ik deze stuur einde middag? Grt

10:05



Btw nota ott fiche en terugkoppeling gesprek minienv met veld



Nieuw bericht





Tapperdetap



99

5.1.2.e

Btw nota ott fiche en terugkonnelling gesprek minjenv met veld
hangt nu bij SG

3 jun. 2021

10:20

5.1.2.e

5.1.2.e

Hi 5.1.2.e ik kan het komend uur even kijken

10:50

5.1.2.e

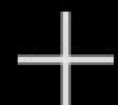
5.1.2.e

Prima stuur ik het je zo

10:50



5.1.2.e heeft de groep verlaten.



Nieuw bericht





Tapperdetap



5.1.2.e

Ik kijk ook nog ff strakkies.

3 jun. 2021

100

5.1.2.e

Ok 5.1.2.e Wil jij aanvullen op een stuk dat ik heb aangepast heb nav opmerkingen van 5.1.2.e? Grt

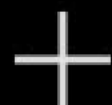
14:53

5.1.2.e

7 jun. 2021

5.1.2.e

Hallo collega's nav mail 5.1.2.e wil ik me aansluiten bij je standpunt 5.1.2.e Ik denk dat het het best is om een sessie in de CSR te doen a la de beoogde MCEV expertsessie. Met name gelet op de fase van dit traject (démisionnaire status) en dat we



Nieuw bericht





Tapperdetap



09:16

101

7 jun. 2021

5.2.1

5.1.2.e

5.1.2.e

Dank 5.1.2.e ik zag ook de reacties van 5.1.2.e Ik zal 5.1.2.e langs deze lijn informeren en dan bij 5.1.2.e terugleggen.

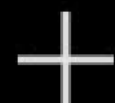
09:40

5.1.2.e

8 jun. 2021

5.1.2.e

Collega's mijn voorstel is om even kort mondeling overleg te



Nieuw bericht





Tapperdetap



102

5.1.2.e

Collega's mijn voorstel is om 8 jun. 2021 mondeling overleg te voeren voor de CSR. Ik zou graag dan even willen bespreken wat we van de csr willen? Is dat een idee? Zo ja dan plan ik wat in.

Grt

17:07

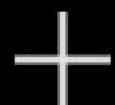
5.1.2.e

Hoi 5.1.2.e lijkt mij prima om een half uurtje te plannen deze week

17:09

5.1.2.e

Ok done 17:10



Nieuw bericht



5.1.2.e



Tapperdetap

17:09



103

5.1.2.e

8 jun. 2021

5.1.2.e

Ok done 17:19

5.1.2.e

Prima. Net gebeld door 5.1.2.e hierover. Kan dan mooi terugkoppelen.

5.1.2.e

En jullie zagen vast zijn stuk in het csr-pakket.

17:30

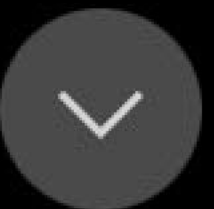
5.1.2.e

Yes dat stuk was aardig kritisch

;)



Nieuw bericht





Tapperdetap



104

;)

8 jun. 2021

5.1.2.e

Yes dat stuk was aardig kritisch

5.1.2.e

5.2.1

17:33

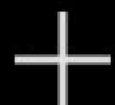
5.1.2.e

Ik heb morgenmiddag interdepartementale voorbespreking ter voorbereiding op de CSR. Ik hou mij aan de hoofdlijn die we al hebben

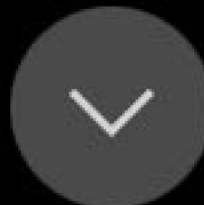
18:12

5.1.2.e

5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap

22:05



106

5.1.2.e

8 jun. 2021

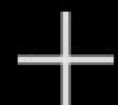
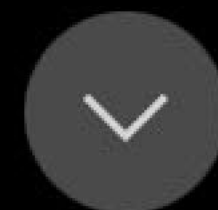
Buiten reikwijdte

5.1.2.e

9 jun. 2021

5.1.2.e

Ik heb niet helemaal scherp wat inhoudelijk de andere blokken
vb nationale wetsvoorstel zijn als aftappen OTT eruit is



Nieuw bericht





Tapperdetap



108

5.1.2.e

9 jun 2021

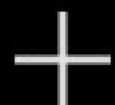
Buiten reikwijdte

5.1.2.e

5.1.2.e

Buiten reikwijdte

Net voorbereidingsgroep CSR gehad ambtelijk. De veiligheidsclubs en met name zoetermeer maken zich erg



Nieuw bericht





Tapperdetap



109

zorgen

9 jun. 2021

Ze willen dat 5.1.2.e op encryptie een procesvoorstel doet dat de CSR hier nog een paar keer over van gedachten wisselt maar verder geen advies uit brengt. 5.2.1

5.1.2.e

5.2.1

15:49

5.1.2.e

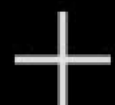
5.1.2.e

Wat is kern van de zorgen?

15:50

5.1.2.e

5.2.1



Nieuw bericht



5.1.2.e



Tapperdetap



110

5.1.2.e

9 jun 2021

5.2.1

5.1.2.e

5.1.2.e

15:53

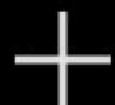
5.1.2.e

5.1.2.e

Ik denk dat 5.1.2.e zichzelf wel als neutraal ziet 15:57



5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap



5.1.2.e

111

5.2.1

9 jun. 2021

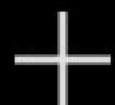
5.2.1

5.2.1

Sprak daar vanmiddag ook met 5.1.2.e over; een advies zou wat ons betreft kunnen, maar zou het ingezette proces (overleg met stakeholders, eu-spoor, wodc onderzoek, input richting formatie) niet moeten verstoren. Idealiter zelfs onderschr...

Meer lezen

16:01



Nieuw bericht



5.1.2.e



Tapperdetap



16:01

9 jun. 2021

112

5.1.2.e

5.2.1

5.2.1

Ik heb benadrukt

dat het voor de discussie en evt followup beiden kanten vh
dilemma goed moeten worden geschetst

16:32

5.1.2.e

5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap

9 jun. 2021



113

10 jun. 2021

5.1.2.e

5.1.2.e

Voorafgaand aan ons overleg van vanmiddag stuur ik een voorzet vd annotatie die ik met 5.1.2.e heb gemaakt. Grt 11:22

5.1.2.e



5.1.2.e

11:36

5.1.2.e



Nieuw bericht



5.1.2.e



Tapperdetap



114

5.1.2.e

10 jun. 2021

Mijn voorstel is om het volgende te bespreken:

- annotatie
- wat willen we van de CSR

5.1.2.e

5.2.1

13:37

5.1.2.e

5.1.2.e

Ik denk dat het laatste punt vanzelf aan de orde komt

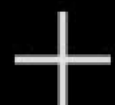
13:39

5.1.2.e

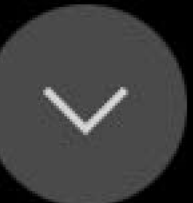
5.1.2.e

Dat is dan goed;) want dat is mijns inziens een relevant punt.

13:47



Nieuw bericht



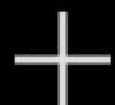
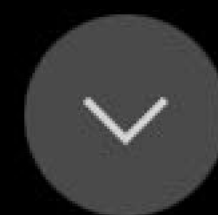


Tapperdetap



115

5.1.2.e



Nieuw bericht





Tapperdetap



116

5.1.2.e

5.2.1

www.algemenebestuursdienst.nl

5.1.2.e

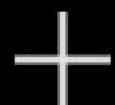
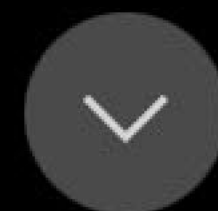
[https://](https://www.algemenebestuursdienst.nl/actueel/nieuws/2022/01/24/5.1.2.e)

[www.algemenebestuursdienst.nl/](https://www.algemenebestuursdienst.nl/actueel/nieuws/2022/01/24/5.1.2.e)

[actueel/nieuws/2022/01/24/5.1.2.e](https://www.algemenebestuursdienst.nl/actueel/nieuws/2022/01/24/5.1.2.e)

5.1.2.e [directie-](#)

[rechtshandhaving-en-](#)



Nieuw bericht





117

ma 7 mrt.

5.1.2.e

Inlichtingendiensten grijpen
Oekraïne-crisis aan om bevoe...

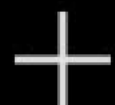
Een nog geheim wetsvoorstel, ingezien
door de Volkskrant, geeft de AIVD en de
MIVD meer ruimte tot grootschalige inter...

www.volkskrant.nl · 7 mrt. 2022

5.1.2.e

[https://www.volkskrant.nl/a-
b8d270d93](https://www.volkskrant.nl/a-b8d270d93)

21:01



Nieuw bericht



5.1.2.e



Tapperdetap



118

wo 11 mei

5.1.2.e

<https://www.bitsoffreedom.nl/2022/05/11/europese-commissie-wil-vertrouwelijkheid-op-internet-opheffen/>

5.1.2.e

5.1.2.e dat wordt opletten met het voorstel EC voor bestrijding
kinderporno

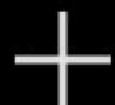
14:02

Zeker

15:33



wo 25 mei



Nieuw bericht





5.1.2.e

wo 25 mei

5.1.2.i

5.

Meer lezen

20:42



Nieuw bericht



120

5.1.2.e



Tapperdetap

20:42



5.1.2.e

wo 25 mei

5.1.2.e

Dank! 21:12

5.1.2.e

5.1.2.e

Ah thx. Wel prima dat er een goed artikel komt in de krant. 21:52

za 4 jun.

5.1.2.e

5.1.2.e

Artikel gezien? Vandaag in NRC! Ik herken onze teksten en redenering.. 20:33



Nieuw bericht





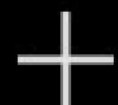
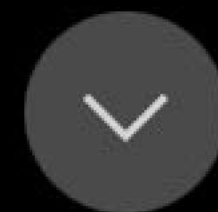
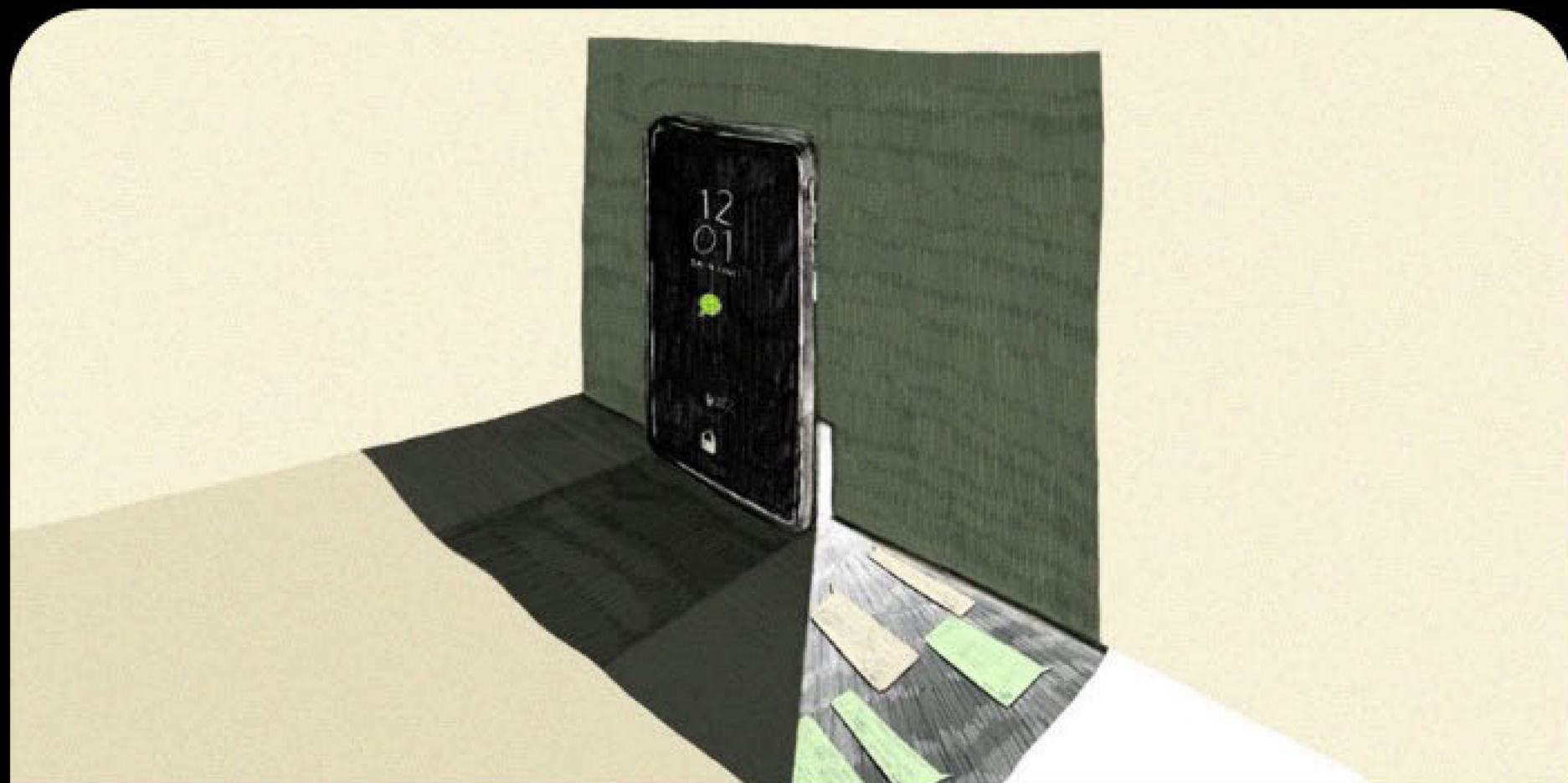
Tapperdetap



121

5.2.1

5.1.2.e



Nieuw bericht





Tapperdetap



122

'WhatsApp dreigde uit Nederland
vertrekken om aftapplicht' za 4 jun.

Telecomwet: WhatsApp zou stoppen in
Nederland als opsporingsdiensten de
berichten via een 'achterdeurtje' gingen...

www.nrc.nl

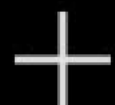
5.1.2.e

[https://www.nrc.nl/nieuws/
2022/06/03/whatsapp-dreigde-te-
vertrekken-om-aftapplicht-a4132175](https://www.nrc.nl/nieuws/2022/06/03/whatsapp-dreigde-te-vertrekken-om-aftapplicht-a4132175)



5.1.2.e

Super 20:35



Nieuw bericht



123

5.1.2.e



Tapperdetap



5.1.2.e

5.1.2.e

Heb

5.1.2.e

ook ff geappt. za 4 jun.

20:41

5.1.2.e

5.1.2.e

Heel goed!

20:50



20:58



de 20 jun



Nieuw bericht



