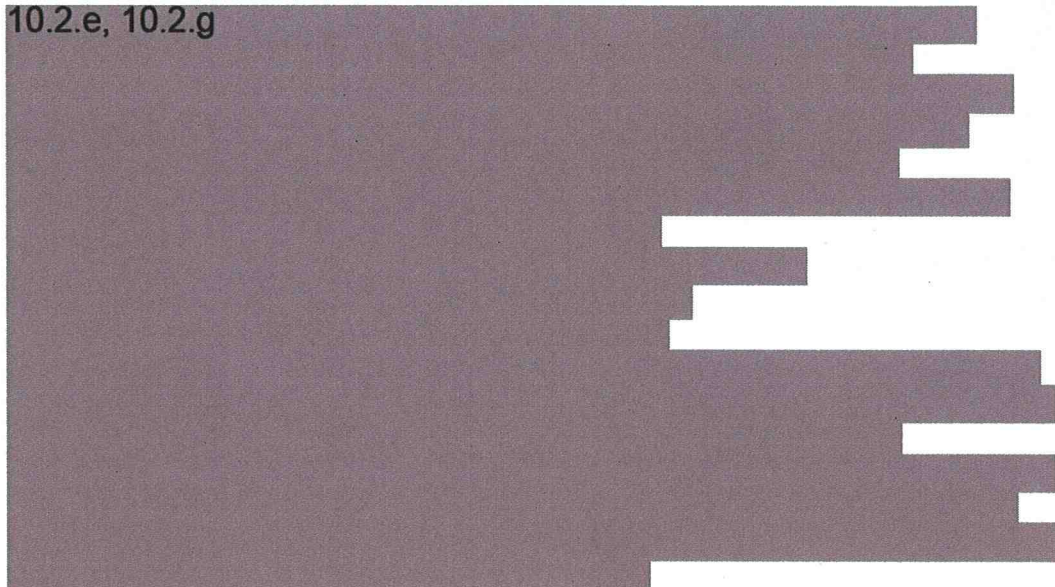
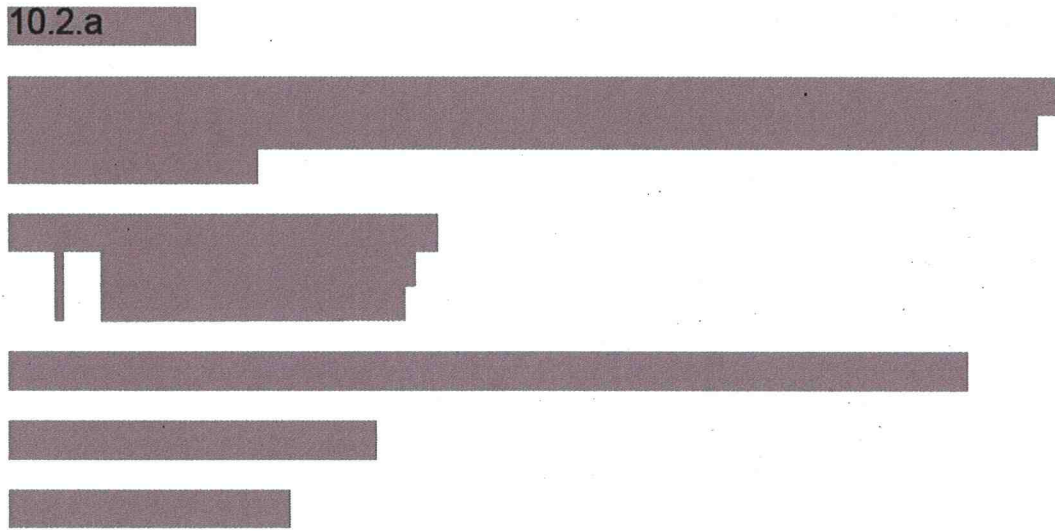


10.2.e, 10.2.g

A large rectangular area of the document is completely redacted with a solid black box.

Subject: Questionnaires on encryption

10.2.a

The content of section 10.2.a is redacted. It consists of several lines of text, each followed by a black redaction box. The first line is the longest, followed by a shorter line, then a bulleted item with a redacted body, and three more lines of redacted text.

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

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

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

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

**Ministry of Security and
Justice**

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

Our reference
708641

Date 4 January 2016
Subject Cabinet's view on encryption

Cabinet's view on encryption

Please find below the cabinet's view on encryption. This is in line with promises made during the debate of the standing committee on Economic Affairs on the Telecommunications Council of 10 June 2015 (TK 2014-2015, 21501-33, no. 552) and the debate of standing committee on Security and Justice on the JHA Council of 7 October 2015.

Introduction

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

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

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

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

Criminal Policy Department
(DSB)

Datum
4 January 2016

Ons kenmerk
708641

The importance of encryption for the government, companies and citizens

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

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

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

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

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

Encryption and the investigation, intelligence and security services

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

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

Criminal Policy Department
(DSB)

Datum
4 January 2016

Ons kenmerk
708641

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

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

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

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

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

Assessment and conclusion

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

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

Criminal Policy Department
(DSB)

Datum
4 January 2016

Ons kenmerk
708641

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

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

Given the preceding assessment, the following conclusion is reached:

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

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

Minister of Security and Justice,

Minister of Economic Affairs

G.A. Van der Steur

H.G.J. Kamp



DGRR

Minister van Justitie en
Veiligheid
DGRR_DRC-GC

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

Contactpersoon

10.2.c

T 10.2.c

Datum

12 juli 2021

Ons kenmerk

3430939

nota

Encryptie questionnaire Europese Commissie (deel B)

1 Doel nota

U wordt verzocht in te stemmen met de verzending van de bijgesloten antwoorden op de questionnaire van de Europese Commissie over de inventarisatie naar mogelijkheden voor rechtmatige toegang tot versleutelde informatie (encryptie).

Het gaat om het tweede deel van de questionnaire: over de aard en omvang van de problematiek voor de opsporing. De antwoorden op de eerste questionnaire - over wetgeving en jurisprudentie rondom rechtmatige toegang tot bewijs en appreciatie van diverse mogelijkheden die de Commissie kan onderzoeken - zijn enkele weken geleden verstuurd.

2 Aanleiding, gevraagde actie(s) en advies

De vragen en antwoorden zien op de aard en omvang van de beperkingen die opsporingsdiensten ondervinden bij het verkrijgen van toegang tot versleuteld materiaal ten behoeve van de opsporing en vervolging.

Daarnaast worden vragen beantwoord over de (effectiviteit van de) huidige technische en juridische (on)mogelijkheden en inzet van opsporingsdiensten om versleutelde informatie te ontsleutelen. Daarbij wordt afzonderlijk ingegaan op de mogelijkheden voor toegang tot data op end-points, data in motion en data op in beslag genomen devices. Ook wordt ingegaan op de vraag welke alternatieven er zijn voor toegang tot versleutelde data, zoals het gebruik van metadata. Bij deze vragen wordt ook aandacht besteed aan de mogelijkheden voor criminelen om eigen gemaakte versleutelde communicatiemiddelen te gebruiken en hoe effectief een verplichting om te ontsleutelen dan nog is.

Ten slotte worden ook vragen beantwoord over innovatieve methoden om toegang tot versleutelde informatie te verkrijgen en over de dialoog over het vraagstuk met stakeholders. In de beantwoording is aangegeven dat Nederland een expert gedreven aanpak en verkenning voorstaat, waar alle belangen in worden gekend en gewaarborgd - cybersecurity, fundamentele rechten en opsporing - en alle relevante stakeholders aan deelnemen. Voorgesteld wordt dat de EC onder meer de volgende dialogen opzet:

- Een multidisciplinaire commissie die proofs-of-concept (poc) van mogelijke technische oplossingen uitwerkt en de risico's en voordelen

daarvan in kaart brengt. Relevante disciplines voor zo'n commissie zijn: juristen, cryptografie experts, cybersecurity experts, opsporingsexperts, etc.

- Conferenties, waarin de operationele behoefte van opsporingsdiensten voor toegang tot versleutelde data bij IPS's in kaart wordt gebracht.
- Expert bijeenkomsten.

Minister van Justitie en
Veiligheid
DGRR_DRC-GC

Datum
12 juli 2021

Ons kenmerk
3430939

3 Toelichting op het advies

De vorige questionnaire was beleidsmatiger van aard en ging onder andere over toekomstige wensen en wetgeving. Deze is daarom aan de minister ter besluitvorming voorgelegd. Deze tweede set vragen gaat over de huidige stand van zaken binnen de opsporing. Daarom volstaat akkoord tot en met DGRR.

4 Dilemma's

Nvt.

5 Politieke en bestuurlijke context

De vragen en beantwoording zijn feitelijk van aard. De beleidsmatige lijn in de antwoorden is, naast feitelijke gegevens, dat digitale data dankzij de digitalisering steeds belangrijker wordt voor effectieve opsporing en vervolging. Tegelijkertijd staat de toegang hiertoe onder druk door steeds betere versleuteling die vaak standaard wordt aangeboden. Daarbovenop zijn er aanpalende discussies die de toegang tot data beïnvloeden, zoals het beginsel van dataminimalisatie waardoor organisaties minder opslaan. De vraag is hoe we bestaande bevoegdheden effectief kunnen houden in het digitale domein. Daarbij moeten de grote belangen van cybersecurity, privacy en opsporing worden meegenomen en gezocht worden naar mogelijkheden waarbij deze in balans zijn en worden gewaarborgd. Het verkennen van mogelijkheden moet vooral in EU-verband plaats vinden, omdat eventuele regulering van dit internationale vraagstuk ook op dat niveau het effectiefst zal zijn.

6 Communicatie

Nvt.

7 Afstemming

OM, politie, NFI, BOD'en, DWJZ, AIVD, MIVD, NCTV, EZK, BZ, BZK, DEIA.

8 Bijlagen

- Questionnaire B

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 29 oktober 2020 14:41
Aan: 10.2.e @bmi.bund.de
Onderwerp: FW: NL comments Draft Council Declaration Encryption (doc. 12143/20)
Bijlagen: 20201021 NL comments Draft Council Declaration Encryption (st12143.en20).docx

Dear 10.2.e

Thank you for a new version of the draft. FYI, our comments on the one circulated for COSI. The draft is getting along nicely, but we have some reservations on a legal framework and what can be considered solutions.

Happy to discuss when necessary, but I understand that you will have your hands full revising all the suggestions.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

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

From: 10.2.e
Sent: donderdag 29 oktober 2020 13:01
To: 10.2.e '10.2.e @diplo.de'; 10.2.g @bmi.bund.de' <10.2.g @bmi.bund.de>;
10.2.g @consilium.europa.eu 10.2.g @consilium.europa.eu>
Subject: NL comments Draft Council Declaration Encryption (doc. 12143/20)

Dear Colleagues,

Please find the NL comments in the margins or in track changes of the attached document.

As usual, happy to clarify when there are questions or comments.

Best regards,

10.2.e



10.2.e

10.2.e

**Permanent Representation of the Kingdom of the Netherlands
to the European Union**

Kortenberglaan 4-10

1040 Brussel, België

T: 10.2.e

Email 10.2.e@minbuza.nl

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

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

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

Nr. D.069

Meeting on encryption and lawful access, 25 May 2021

Agenda

1. Welcome
2. Context
3. Mapping of Member States' encryption landscape – draft questionnaire
 - Objectives and methodology of the draft questionnaire, including on confidentiality
 - Exchange of views
4. Next steps
5. AOB

Van: 10.2.e [REDACTED]@bmi.bund.de
Aan: 10.2.e [REDACTED]BD/DRC/CV
Cc: 10.2.e [REDACTED]@justice.gouv.fr; 10.2.e [REDACTED]@justice.gouv.fr
Onderwerp: AW: COSI encryption
Datum: maandag 5 oktober 2020 12:39:06

10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV

Gesendet: Samstag, 3. Oktober 2020 11:56

An: 10.2.e

Cc: 10.2.e ; 10.2.e @justice.gouv.fr'

Betreff: RE: COSI encryption

Hello 10.2.e

You managed to produce a very balanced statement, my compliments. Thanks again for this opportunity to react informally. I have some minor suggestions, for example the importance of this initiative for both online and offline public security could be made a bit more explicit. Also, I would introduce a few examples of the problems LEA face, and I would touch upon the importance of E-evidence in criminal investigations as whole.

Good luck with the consultation.

Yours sincerely,

10.2.e

Ministry of Justice and Security

Law Enforcement Department

Cybercrime unit

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

м10.2.е

10.2.e @minvenj.nl

www.government.nl/venj (<http://www.government.nl/...>)

Van: 10.2.e @bmi.bund.de <10.2.e @bmi.bund.de>

Verzonden: donderdag 1 oktober 2020 13:07

Aan: 10.2.e [redacted]@justice.gouv.fr; 10.2.e [redacted] - BD/DRC/CV

<10.2.e [redacted]@minjenv.nl>; 10.2.e [redacted]@justice.gouv.fr

Onderwerp: WG: COSI encryption

10.2.e [redacted],

10.2.a [redacted]

[redacted]

[redacted]

10.2.e [redacted]

10.2.e [redacted]

Von: 10.2.e [redacted]

Gesendet: Mittwoch, 30. September 2020 15:43

An: 10.2.e [redacted] ' <10.2.e [redacted]@justice.gouv.fr>; 10.2.e [redacted] - BD/DRC/CV

10.2.e [redacted]@minjenv.nl>

Cc: 10.2.e [redacted] <10.2.e [redacted]@justice.gouv.fr>

Betreff: AW: COSI encryption

10.2.a [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10.2.e [redacted]

Von: 10.2.e [redacted] 10.2.e [redacted]@justice.gouv.fr>

Gesendet: Mittwoch, 30. September 2020 10:56

An: 10.2.e [redacted] - BD/DRC/CV 10.2.e [redacted]@minjenv.nl>

Cc: 10.2.e [redacted] <10.2.e [redacted]e@bmi.bund.de>; 10.2.e [redacted]

10.2.e [redacted]@justice.gouv.fr>

Betreff: RE: COSI encryption

10.2.e [redacted]

10.2.a [redacted]

[redacted]

[redacted]

[redacted]

10.2.e [redacted]

De: 10.2.e [redacted] - BD/DRC/CV <10.2.e [redacted]@minjenv.nl>

Envoyé : mardi 29 septembre 2020 17:12

À: 10.2.e [redacted] 10.2.e [redacted]@justice.gouv.fr>

Cc: 10.2.e [redacted]@bmi.bund.de' <10.2.e [redacted]@bmi.bund.de>

Objet : COSI encryption

10.2.e [redacted],

Have you heard about the result in COSI? The German Presidency is going to write a statement on the issue of lawful access to encrypted data.

Our German colleague, 10.2.e [redacted], and I thought it might be a good idea to have a conference call and discuss the way forward together. For us it could be possible as early as tomorrow or Thursday around 15:00. Would you be willing and available?

By the way, I was also asked to check if you received our request for information on 5G policy in good order and if it raised any questions if you already had the chance to look at it.

Thank you in advance.

Bien cordialement.

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M10.2.e

@minvenj.nl

www.government.nl/venj (<http://www.government.nl/>...) (<http://www.government.nl/venj>)
.....

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e @bmi.bund.de
Verzonden: maandag 23 november 2020 17:38
Aan: 10.2.e - BD/DRC/CV
Onderwerp: AW: Encryption declaration

10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV
Gesendet: Montag, 23. November 2020 10:32
An: 10.2.e
Betreff: Encryption declaration

Hello 10.2.e

We haven't spoken in a while, also due to my two week holiday.

Just some words of support in what must be a hectic time for you.

You're doing a great job.

The declaration is a good compromise in the EU-landscape:

- Need for a technical solution is clear.
- the technical solution must be proportional, etc.
- the use of a technical solution must be proportional, etc.

Schritt für Schritt.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
m10.2.e

@minvenj.nl

www.government.nl/venj (<http://www.government.nl/...>)
.....

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: dinsdag 20 april 2021 14:26
Aan: 10.2.e @bmi.bund.de'
Onderwerp: RE: Lawfull access to encrypted data

Yes, it seems that we are on the same page. I will discuss this with the them.

I shall propose a time next week where we can call discuss this process further.

Good luck in the G7!

Yours sincerely,

10.2.e

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

.....
M 10.2.e
@minvenj.nl
www.government.nl/veni
.....

Van: 10.2.e @bmi.bund.de
Verzonden: dinsdag 20 april 2021 13:22
Aan: 10.2.e - BD/DRC/CV
Onderwerp: AW: Lawfull access to encrypted data

Dear 10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Gesendet: Dienstag, 20. April 2021 12:36
An: 10.2.e <10.2.e@bmi.bund.de>
Cc: 10.2.e BD/DRC/FO <10.2.e@minjenv.nl>; 10.2.e @minbuza.nl
Betreff: RE: Lawfull access to encrypted data

Hello 10.2.e

I just received a quite ambitious proposal for our multilateral meeting in May. I feel that our meeting in May should be limited to stock-taking, discussing best practices and looking forward to our respective processes amongst policy advisors and technical/LEA liaisons. Holding sessions like the UK proposes could be part of this third part of our meeting.

The UK proposes to talk about this upcoming Friday. In this process I feel that Germany and NL should cooperate very closely and therefore I would like to hear your thoughts on the British proposal and my hesitation to set-up an ambitious agenda on such short notice and without discussing appropriate attendees and become acquainted with the other participants.

Would you be able to hold a short telephone call before Friday and/or do you want to join a telephone call with the British colleagues on Friday?

I CC'ed 10.2.e (whom you know) and also 10.2.e our colleague of the Perm Rep.

Kind regards,

10.2.e

Yours sincerely,

10.2.e

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

Van: 10.2.e <10.2.e@homeoffice.gov.uk>
Verzonden: dinsdag 20 april 2021 10:39
Aan: 10.2.e BD/DRC/CV 10.2.e @minjenv.nl; 10.2.e @homeoffice.gov.uk
cc: 10.2.e - BD/DRC/FO <10.2.e@minjenv.nl>; 10.2.e 10.2.e @homeoffice.gov.uk;
10.2.e (OSCT) <10.2.e@homeoffice.gov.uk>; 10.2.e (Sensitive) 10.2.e @fcdo.gov.uk;
10.2.e (Sensitive) <10.2.e@fcdo.gov.uk>; 10.2.e (Sensitive)
<10.2.e@fcdo.gov.uk>
Onderwerp: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

10.2.e

– Encryption Policy
National Security Directorate

Home Office

2 Marsham Street, London SW1P 4DF

T: +10.2.e

M: +10.2.e

www.gov.uk/home-office ([http://www.gov.uk/...](http://www.gov.uk/))

[@ukhomeoffice](https://twitter.com/) ([https://twitter.com/...](https://twitter.com/))

From: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>

Sent: 15 April 2021 09:59

To: 10.2.e 10.2.e @homeoffice.gov.uk>

Cc: 10.2.e - BD/DRC/FO <10.2.e @minjenv.nl>; 10.2.e 10.2.e @homeoffice.gov.uk>;

10.2.e (OSCT) 10.2.e @homeoffice.gov.uk>; 10.2.e <10.2.e @homeoffice.gov.uk>;

10.2.e (Sensitive) 10.2.e @fcdo.gov.uk>; 10.2.e (Sensitive)

10.2.e @fcdo.gov.uk>; 10.2.e (Sensitive) 10.2.e @fcdo.gov.uk>

Subject: RE: Lawfull access to encrypted data

Dear 10.2.e

Thank you very much for the paper and the good conversation that we had. I shall propose a meeting on the sixth of May in the afternoon.

Also, thank you for the contact information of our German colleagues, but do you have the French contacts as well? Other invitees that I want to invite are the European Presidency (Portugal) and the FBI. This would mean that UK, GER, FRA, EU presidency, FBI and NL will be in the meeting.

The aim of the meeting would be 'informal stock-taking', sharing each other domestic experiences so far, share best practices on how to approach this topic, and share possible way's forward in our respective processes.

Is this similar to what you had in mind?

Kind regards,

10.2.e

Yours sincerely,

10.2.e

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

M 10.2.e
@minjenvi.nl
[www.government.nl/venj \(https://gbr01.safelinks.protection.outlook.com/...\)](https://gbr01.safelinks.protection.outlook.com/...)
.....

Van: 10.2.e 10.2.e @homeoffice.gov.uk>
Verzonden: donderdag 1 april 2021 22:29
Aan: 10.2.e - BD/DRC/CV 10.2.e @minjenvi.nl>
cc: 10.2.e - BD/DRC/FO 10.2.e @minjenvi.nl>; 10.2.e <10.2.e @homeoffice.gov.uk>;
10.2.e OSCT) <10.2.e @homeoffice.gov.uk>; 10.2.e <10.2.e @homeoffice.gov.uk>;
10.2.e (Sensitive) 10.2.e @fcdo.gov.uk>; 10.2.e (Sensitive)
10.2.e @fcdo.gov.uk>; 10.2.e (Sensitive) 10.2.e @fcdo.gov.uk>
Onderwerp: RE: Lawfull access to encrypted data

10.2.a, 10.2.a

10.2.a, 10.2.e
10.2.a, 10.2.e

10.2.e

Home Office

2 Marsham Street, London SW1P 4DF

T: 10.2.e

M: 10.2.e

www.gov.uk/home-office (<https://qbr01.safelinks.protection.outlook.com/...>)

[@ukhomeoffice](https://twitter.com/ukhomeoffice) (<https://qbr01.safelinks.protection.outlook.com/...>)



From: 10.2.e [@homeoffice.gov.uk](mailto:10.2.e@homeoffice.gov.uk)>

Sent: 17 March 2021 15:28

To: 10.2.e BD/DRC/CV 10.2.e [>](mailto:10.2.e@minjenv.nl); 10.2.e

10.2.e [>](mailto:10.2.e@homeoffice.gov.uk); 10.2.e [>](mailto:10.2.e@homeoffice.gov.uk); 10.2.e

10.2.e [>](mailto:10.2.e@homeoffice.gov.uk)

Cc: 10.2.e BD/DRC/FO 10.2.e [>](mailto:10.2.e@minjenv.nl)

Subject: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

10.2.e

10.2.e

From: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>

Sent: 17 March 2021 15:21

To: 10.2.e @homeoffice.gov.uk>; 10.2.e @homeoffice.gov.uk>; 10.2.e <10.2.e @homeoffice.gov.uk>; 10.2.e <10.2.e @homeoffice.gov.uk>

Cc: 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>

Subject: RE: Lawfull access to encrypted data

10.2.e

Thank you for taking the time and catch up! Shall we meet Thursday the 25th 10:30-11:30 our time/09:30-10:30 your time? Not sure we need a full hour but my experience is that complex topics like this sometimes need a bit of time.

Is Webex a good platform for you?

Met vriendelijke groet,

10.2.e

M 10.2.e
invenj.nl

Van: 10.2.e @homeoffice.gov.uk>

Verzonden: dinsdag 16 maart 2021 11:42

Aan: 10.2.e BD/DRC/CV 10.2.e @minjenv.nl>; 10.2.e @homeoffice.gov.uk>; 10.2.e @homeoffice.gov.uk>; 10.2.e @homeoffice.gov.uk>; 10.2.e @homeoffice.gov.uk>

cc: 10.2.e J. - BD/DRC/FO 10.2.e @minjenv.nl>

Onderwerp: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

10.2.e

From: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>

Sent: 11 March 2021 08:56

To: 10.2.e 10.2.e @homeoffice.gov.uk; 10.2.e <10.2.e @homeoffice.gov.uk>
Cc: 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>
Subject: Lawfull access to encrypted data

Dear 10.2.e

My name is 10.2.e Dutch Ministry of Justice and Security. One of the topics in my portfolio is lawful access to encrypted data. Previously I had very good contact with 10.2.e on this issue, actually my last business trip before corona was to the Home Office and Thames House.

Recently in The Netherlands we have been exploring the possibility to intercept OTT-services and the GCHQ initiative of 2018 (Principles for a More Informed Exceptional Access Debate) was mentioned as a promising solution. I understand that this was met with backlash at the time and has not been pursued, but I was wondering if you could give use somewhat more background on this initiative. Also it would be very helpful to catch up on our searches to possible solutions. Would you be willing to discuss these issues with us through a videoconference?

Thank you in advance.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M 10.2.e
@minvenj.nl
www.government.nl/venj (https://gbr01.safelinks.protection.outlook.com/...)
.....

Van: 10.2.e <10.2.e @homeoffice.gov.uk>

Verzonden: donderdag 17 december 2020 11:33

Aan: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>; 10.2.e <10.2.e @homeoffice.gov.uk>

cc: 10.2.e (Sensitive) 10.2.e @fcdo.gov.uk; 10.2.e <10.2.e @homeoffice.gov.uk>

Onderwerp: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

10.2.a, 10.2.e

10.2.a

10.2.e

From: 10.2.e - BD/DRC/CV
Sent: 17 December 2020 10:17
To: 10.2.e
Cc: 10.2.e (Sensitive)
Subject: Lawfull access to encrypted data

Dear 10.2.e,

Please find attached the council resolution on lawfull access to encrypted data that has been published since Monday. I always appreciated the contact with 10.2.e on this issue, both in discussing a way forward or sharing common problems that our services experience. I hope we can continue this contact in the future. This is a topic that requires collective attention and action as your earlier statement on lawfull access also stipulates.

I want to wish you happy holidays despite the lockdown and hopefully we have a chance to meet again in 2021.

Yours sincerely,

10.2.e

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

M 10.2.e
@minvenj.nl
www.government.nl/venj (<https://gbr01.safelinks.protection.outlook.com/...>)
.....

Van: 10.2.e
Verzonden: donderdag 15 oktober 2020 15:30

Aan: 10.2.e - BD/DRC/CV
cc: 10.2.e
Onderwerp: Contacts

10.2.a, 10.2.e

10.2.e
ncryption and Online Safety,
Investigatory Powers Unit,
Office for Security and Counter Terrorism

Home Office
2 Marsham Street, London, SW1P 4DF
T: 10.2.e
E: 10.2.e @homeoffice.gov.uk

This email and any files transmitted with it are private and intended
solely for the use of the individual or entity to whom they are addressed.
If you have received this email in error please return it to the address
it came from telling them it is not for you and then delete it from your system.
This email message has been swept for computer viruses.

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

This email and any files transmitted with it are private and intended
solely for the use of the individual or entity to whom they are addressed.
If you have received this email in error please return it to the address
it came from telling them it is not for you and then delete it from your system.

This email message has been swept for computer viruses.

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

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system. This email message has been swept for computer viruses.

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

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system. This email message has been swept for computer viruses.

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

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system. This email message has been swept for computer viruses.

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: vrijdag 23 april 2021 12:16
Aan: 10.2.e; 10.2.e @bmi.bund.de'
CC: 10.2.e - BD/DRC/FO; 10.2.e @minbuza.nl
Onderwerp: Multilateral meeting on lawful access to encrypted data

Dear 10.2.e ,

I would like to finalize the details of our 'informal multilateral meeting amongst colleagues' with you and check if the proposed time and date suits you before sending out the invitations.

Date & time: 13th of May, 16:00-17:00 Amsterdam time

Platform: Webex

Topic: latest developments, goals, future sessions and opportunities for multilateral action.

Attendees: UK, Germany, US, France, current and future Presidency (PORT and SLOV), NL.
Each attending country is welcome to participate with a policy expert, a LEA representative and a technical expert.

Portugal and Slovenia can be invited through our Permanent Representation. The invitation of the US I can send through the FBI liaison in The Hague 10.2.e and for France my contact person is 10.2.e If you have additional contacts I need to include please let me know.

It would be great if I can send the invitation after the weekend.

Yours sincerely,

10.2.e

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

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

10.2.e - BD/DRC/FO

Onderwerp: Lawful access to encrypted data
Locatie: WEBEX

Begin: di 18-5-2021 16:00
Einde: di 18-5-2021 17:00
Tijd weergegeven als: Voorlopig

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator: 10.2.e - BD/DRC/CV

Verplichte deelnemers: 10.2.e @bmi.bund.de; 10.2.e (FBI);
10.2.e @diplomatie.gouv.fr; 10.2.e minbuza.nl; 10.2.e
10.2.e - BD/DRC/FO; 10.2.e @gov.si; 10.2.e - BD/PIDS;
10.2.e @om.nl; 10.2.e @policija.si; 10.2.e @policija.si;
10.2.e @policija.si

Dear colleagues,

As previously announced we want to invite you to a stock-taking meeting on lawful access to encrypted data. All invited countries have issued a statement or resolution on finding technical solutions to lawful access to encrypted data. This topic is complex, it requires the balancing of different important interests, the search for possible solutions often encounters engaging societal debate and in addition there is the dependency on the private sector. Given the complex nature of this issue we think it might be beneficial to hear experiences of colleagues that have been active on this issue, keep apprised of each other's' progress and discuss where we might cooperate in our respective processes.

We would like to invite colleagues that are active in (the policy field of) law enforcement and encourage different disciplines to participate in this meeting. Countries are free to invite, for example, a policy expert, a LEA representative and/or a technical expert.

The agenda shall include: latest developments, goals, future sessions and opportunities for multilateral action. If you have additional items please let me know.

I look forward to your participation and a lively meeting.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

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

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g

Deelnemen via telefoon

10.2.g

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g

U kunt ook 10.2.g kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.g

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: maandag 10 mei 2021 13:38
Aan: 10.2.e @bmi.bund.de
Onderwerp: RE: Meeting on the 18th

Hello 10.2.e

This meeting shall address these issues in a broad sense. Topics of this discussion are: latest developments, goals, future sessions and opportunities for multilateral action.

In this meeting we are going to share more practices, experiences, goals and we can discuss the need for more 'deep dives' at the end of the meeting. As you have seen the UK shared four possible meetings. At the end of this day I will send you and 10.2.e some questions for participants to prep, so I can distribute them tomorrow.

Met vriendelijke groet,

10.2.e

M 10.2.e
@minveni.nl

Van: 10.2.e @bmi.bund.de
Verzonden: maandag 10 mei 2021 08:25
Aan: 10.2.e - BD/DRC/CV
Onderwerp: Meeting on the 18th

Dear 10.2.e

10.2.a

10.2.e

10.2.e

Referat CI 6 (Grundsatz Cyberfähigkeiten der Sicherheitsbehörden)
Bundesministerium des Innern, für Bau und Heimat

Dienstgebäude: Alt Moabit 140, 10557 Berlin

Tel.: 10.2.e
E-Mail: 10.2.e @bmi.bund.de

10.2.e - BD/DRC/FO

Van: 10.2.e @bmi.bund.de
Verzonden: woensdag 12 mei 2021 07:04
Aan: 10.2.e BD/DRC/CV; 10.2.e @homeoffice.gov.uk
CC: 10.2.e @homeoffice.gov.uk
Onderwerp: AW: Update Multilateral meeting on working level 18th of May

Dear 10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV
Gesendet: Dienstag, 11. Mai 2021 17:58
An: 10.2.e ; 10.2.e
Cc: 10.2.e
Betreff: RE: Update Multilateral meeting on working level 18th of May

Dear 10.2.e

I am sorry to come back to you so quickly, but if we want to give the participants ample time to prepare I think it would be best to send the email tomorrow around lunchtime. If we are all in agreement that sending such preparation is beneficial for the outcome of the meeting of course.

Thank you very much for your understanding.

Kind regards,

10.2.e

Yours sincerely,

10.2.e

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

.....
M 10.2.e
@minvenj.nl
www.government.nl/venj (<http://www.government.nl/...>)
.....

Van: 10.2.e - BD/DRC/CV

Verzonden: maandag 10 mei 2021 17:55

Aan: 10.2.e ' <10.2.e @homeoffice.gov.uk>; 10.2.e @bmi.bund.de'

10.2.e @bmi.bund.de>

CC: ^{B2a} @minbuza.nl; 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>; 10.2.e

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

Onderwerp: Update Multilateral meeting on working level 18th of May

Dear 10.2.e

I wanted to give you an update on the participants for the meeting and I would like to ask you what you think of the idea of providing a bit more guidance to the attendees so they can better prepare.

Attendees

I have not received a reactive yet from 10.2.e which means we do not yet have a participant from France. 10.2.e did I understand correctly that you had good experiences with her? Could you maybe send a reminder? Please find the email that I sent her attached, I have also sent her the Outlook invitation. I have also not yet received a confirmation from Portugal. A reminder has been sent already.

I have received a confirmation from Slovenia, three experts along the requested fields of expertise will participate and the representative at the Perm Rep as well.

In case of the US I have only received a confirmation from the FBI 10.2.e I can enquire whether more people will join through him or do you prefer to do enquire into possible participants through your contacts 10.2.e ?

Guidance

In order to provide a bit more guidance to all the attendees I wanted to share some questions so they can deliberate on the answer beforehand. I have not received any additional topics other than the topics we previously discussed.

Introduction: lawful access to encrypted data knows many varieties. We could differentiate into the application of encryption (data in storage on a device/in the cloud, data in transit (interception), encryption of the device itself). One could also discuss the way encrypted data is lawfully accessed separately, either through an ISP or through covert access on the device.

This meeting is focussed on lawful access through an ISP, either through stored data or data in transit.

Goal of the meeting: share best practices, compare the different goals and identify future needs and opportunities for multilateral action.

Below you find some questions that you could think of when we meet on the 18th of May. We shall not go through these questions one-by-one, but hopefully this gives you an idea into what we hope to discuss.

I. Goals

- a. Where do you think a solution is most urgently needed: ordering data in transit through an ISP, ordering stored data through an ISP [or access to encrypted devices/the possibility for covert accessing a device]
- b. What do you think are the greatest obstacles to achieving your goals?
- c. What do you think is necessary to achieve these goals?
- d. Do you currently plan to, or are you engaged in, find(ing) a technical solution? Do you currently plan to, or are you engaged in, draft(ing) legislation to this effect?
- e. Do you have a strategy in place in order to address the issue of lawful access to encrypted data?

II. Latest developments

- a. Did you have consultations with other governmental bodies on the issue of lawful access to encrypted data and what were your experiences?
- b. Could you share experiences, if any, that you recently had with companies, academia or civil society on the issue of lawful access to encrypted data?
- c. Do you have any legislative or technical process in place to address lawful access to encrypted data?

III. Future sessions and opportunities for multilateral action

- a. Even though we have our respective processes we could benefit from each other's' expertise and experiences. Possible future sessions could include some 'deep dives':
 - i. Session 2: Technical experts seminar (opportunity for briefing from UK technical expert – 10.2.e – followed by discussion among participants)
 - ii. Session 3: Law enforcement seminar (discussion among law enforcement leads of current experience, impact of platforms moving to end-to-end encryption, powers and limits, collaboration, mitigation)
 - iii. Session 4: Policy and operational leads' seminar (opportunity for law enforcement leads to question and discuss issues with government policy officials and, possibly, technical experts).

Please share possible fields where a multinational dialogue would be constructive.

10.2.e Could you share your thoughts on the additional guidance to participants tomorrow afternoon so I can send it tomorrow at the end of the day? Or would Wednesday be more convenient for you?

I look forward to our conversation on the 18th.

Met vriendelijke groet,

10.2.e

M 10.2.e

@minvenj.nl

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: woensdag 12 mei 2021 13:52
Aan: 10.2.e; 10.2.e @bmi.bund.de 10.2.e (FBI);
10.2.e @diplomatie.gouv.fr; 10.2.e @minbuza.nl; 10.2.e
10.2.e BD/DRC/FO; 10.2.e @gov.si 10.2.e - BD/PIDS;
10.2.e @om.nl; 10.2.e @policija.si; 10.2.e @policija.si;
10.2.e @policija.si; 10.2.e @bka.bund.de
Onderwerp: RE: Lawful access to encrypted data

Dear colleagues,

In order to provide a bit more guidance I wanted to share some questions so you can deliberate on the answer beforehand.

We shall not go through these questions one-by-one, but hopefully this gives you an idea into what we hope to discuss.

Lawful access to encrypted data knows many varieties. We could differentiate into the application of encryption (data in storage on a device/in the cloud, data in transit (interception), encryption of the device itself). One could also discuss the way encrypted data is lawfully accessed, either through an ISP or through covert access on the device.

This meeting is focussed on lawful access through an ISP, either through stored data or data in transit.

Goal of the meeting: share best practices amongst colleagues, compare the different goals and identify future needs and opportunities for multilateral action.

Below you find some questions that you could think of when we meet on the 18th of May.

I. **Goals**

- a. Where do you think a solution is most urgently needed: ordering data in transit through an ISP, ordering stored data through an ISP [or access to encrypted devices/the possibility for covert accessing a device]
- b. What do you think are the greatest obstacles to achieving your goals?
- c. What do you think is necessary to achieve these goals?
- d. Do you currently plan to, or are you engaged in, find(ing) a technical solution? Do you currently plan to, or are you engaged in, draft(ing) legislation to this effect?
- e. Do you have a strategy in place in order to address the issue of lawful access to encrypted data?

II. **Latest developments**

- a. Did you have consultations with other governmental bodies on the issue of lawful access to encrypted data and what were your experiences?
- b. Could you share experiences, if any, that you recently met with companies, academia or civil society on the issue of lawful access to encrypted data?
- c. Do you have any legislative or technical process in place to address lawful access to encrypted data?

III. **Future sessions and opportunities for multilateral action**

- a. Even though we have our respective processes we could benefit from each other's' expertise and experiences. Possible future sessions could include some 'deep dives':
 - i. Session 2: Technical experts seminar (opportunity for briefing from UK technical expert – 10.2.e – followed by discussion among participants)
 - ii. Session 3: Law enforcement seminar (discussion among law enforcement leads of current experience, impact of platforms moving to end-to-end encryption, powers and limits, collaboration, mitigation)
 - iii. Session 4: Policy and operational leads' seminar (opportunity for law enforcement leads to question and discuss issues with government policy officials and, possibly, technical experts).

Please share possible fields where a multinational dialogue would be constructive.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

M 10.2.e

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

-----Oorspronkelijke afspraak-----

Van: 10.2.e - BD/DRC/CV

Verzonden: woensdag 28 april 2021 19:11

Aan: 10.2.e - BD/DRC/CV; 10.2.e; 10.2.e @bmi.bund.de; 10.2.e TH)
(FBI); 10.2.e @diplomatie.gouv.fr; 10.2.e @minbuza.nl; 10.2.e BD/DRC/FO;
10.2.e @gov.si; 10.2.e - BD/PIDS; 10.2.e @om.nl; 10.2.e @policija.si;
10.2.e @policija.si; 10.2.e @policija.si
cc: 10.2.e @bka.bund.de

Onderwerp: Lawful access to encrypted data

Tijd: dinsdag 18 mei 2021 16:00-17:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.

Locatie: WEBEX

Dear colleagues,

As previously announced we want to invite you to a stock-taking meeting on lawful access to encrypted data. All invited countries have issued a statement or resolution on finding technical solutions to lawful access to encrypted data. This topic is complex, it requires the balancing of different important interests, the search for possible solutions often encounters engaging societal debate and in addition there is the dependency on the private sector. Given the complex nature of this issue we think it might be beneficial to hear experiences of colleagues that have been active on this issue, keep apprised of each other's progress and discuss where we might cooperate in our respective processes.

We would like to invite colleagues that are active in (the policy field of) law enforcement and encourage different disciplines to participate in this meeting. Countries are free to invite, for example, a policy expert, a LEA representative and/or a technical expert.

The agenda shall include: latest developments, goals, future sessions and opportunities for multilateral action. If you have additional items please let me know.

I look forward to your participation and a lively meeting.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

M 10.2.e

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

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g

Deelnemen via telefoon

10.2.g

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g

10.2.g kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.g

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e - BD/DRC/FO

Van: 10.2.e <10.2.e@fbi.gov>
Verzonden: woensdag 19 mei 2021 13:33
Aan: 10.2.e - BD/DRC/CV
Onderwerp: Re: [EXTERNAL EMAIL] - Guidance

10.2.a

10.2.e
FBI
The Hague, NL
O: 10.2.e
M: 10.2.e
US: 10.2.e
email: 10.2.e@fbi.gov

From: 10.2.e - BD/DRC/CV
Sent: Friday, May 14, 2021 10:30 AM
To: 10.2.e (FBI)
Subject: RE: [EXTERNAL EMAIL] - Guidance
Hi 10.2.e

Unfortunately the way in which countries accept the meeting differs, so I do not have a complete view of the participants. Also countries were free to form their own delegation, combining the three disciplines was a suggestion.

I apologize if the format is a bit loose compared to what you might be accustomed to in multinational meetings. For the Netherlands this informal setting suits the stage of the process that we are in right now, a meeting amongst colleagues. If it is desirable to have multiple meetings after this it can be an iterative process where along the way we can adjust the attendance.

The title that you can think of is (senior) policy level/technical expert. From the Dutch side there is me as a senior policy advisor of the ministry, a senior policy advisor of our public prosecuting service and the Dutch participant in ILETS meetings. Countries like Germany, Slovenia en the UK send representatives from the ministries and from the police.

'Working level' was a term the British used. Again, I am sorry if this is too vague, but does it help a little?
Met vriendelijke groet,

10.2.e
M 10.2.e
@minvenj.nl

Van: 10.2.e
Verzonden: vrijdag 14 mei 2021 09:42
Aan: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
Onderwerp: [EXTERNAL EMAIL] - Guidance
10.2.a, 10.2.e

10.2.e

-
On May 12, 2021 9:23 AM, "10.2.e" - BD/DRC/CV" <10.2.e@minjenv.nl> wrote:

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 toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: woensdag 28 april 2021 09:28
Aan: 10.2.e @diplomatie.gouv.fr
Onderwerp: Lawful access to encrypted data

Dear 10.2.e ,

My name is 10.2.e Law Enforcement department of the Dutch Ministry of Justice and Security. I received your email from 10.2.e because I want to organize a multilateral meeting on lawful access to encrypted data. As you know, at the end of last year the Council on Justice and Home affairs issued a resolution on this topic as did the 'five eyes' plus India and Japan. In preparation of the European process that we initiated in December I think it might be beneficial to hear experiences of colleagues that have been active on this issue, keep apprised of each other's' progress and discuss where we might cooperate in our respective processes.

Today you will receive an invitation for an informal stock-taking meeting amongst colleagues on the 18th of May. Invitees are France, the UK, Germany, the current and upcoming EU Presidency and the US. Each attending country is welcome to participate with a policy expert, a LEA representative and a technical expert. The topic of this meeting is: latest developments, goals, future sessions and opportunities for multilateral action. I hope that you will be able to join us and look forward to a good cooperation.

Bien cordialement.

10.2.e

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

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

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 27 mei 2021 09:07
Aan: 10.2.e 10.2.e 10.2.e @homeoffice.gov.uk
Onderwerp: Bilateral meeting Home Secretary & Minister of Justice and security

Hello 10.2.e

I just learned that mrs. Patel en mr. Grapperhaus will meet on the 3rd of June and possibly speak about encryption. I will prepare him with some remarks on the recognition on both the importance of encryption and the negative impact, a word of appreciation for our long-standing good cooperation on this issue and aspiration for continued bilateral effort for finding a proportionate solution and desire to play an active role in the EU process.

Regarding context, as you know encryption is a sensitive issue and in The Netherlands currently negotiations are ongoing on forming a new coalition government.

Is there anything in particular coming from your side that I would need to prep him for?

And for our multilateral process, do you think we can communicate a safe the date this week?

Thank you in advance!

Yours sincerely,

10.2.e

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

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: vrijdag 4 juni 2021 10:41
Aan: 10.2.e
CC: 10.2.e; 10.2.e; 10.2.e
Onderwerp: RE: Bilateral meeting Home Secretary & Minister of Justice and security

10.2.e

I heard that our ministers had a good conversation and have voiced appreciation for our current cooperation as well as a desire to continue that cooperation.

Regarding the follow-up meeting if you could indicate what is achievable that would be great. I am a bit hesitant to reverse the order of the meetings given that there was such broad support and enthusiasm for the technical meeting and we haven't really discussed the other topics. Also I think we identified that presenting a workable and safe technical solution would benefit the discussion and in finding that solution is where the biggest challenge is.

Of course it would be really great and interesting if 10.2.e could attend himself, but if it is more pragmatic to invite a colleague who worked on the proposal that would also be very much appreciated, right? This would also fit with the working-level character of our meetings.

I would really like to have another meeting before the summer in order to keep momentum in the process. Maybe the first week of July/last week of June?

Looking forward to hearing your thoughts.

Yours sincerely,

10.2.e

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

.....
M 10.2.e
@mlnvent.nl
www.government.nl/veni
.....

Van: 10.2.e
Verzonden: vrijdag 28 mei 2021 21:05
Aan: 10.2.e - BD/DRC/CV
CC: 10.2.e; 10.2.e; 10.2.e
Onderwerp: RE: Bilateral meeting Home Secretary & Minister of Justice and security

022.022

10.2.a, 10.2.e

[illegible]

10.2.e [REDACTED] – Encryption Policy
National Security Directorate

2 Marsham Street, London SW1P 4DF

M: 10.2.e

@ukhomeoffice

Sent: 27 May 2021 08:07

To: 10.2.e <10.2.e@homeoffice.gov.uk>; 10.2.e 10.2.e @homeoffice.gov.uk>; 10.2.e

10.2.e @homeoffice.gov.uk>

Subject: Bilateral meeting Home Secretary & Minister of Justice and security

Hello 10.2.e

I just learned that Mrs. Patel en Mr. Grapperhaus will meet on the 3rd of June and possibly speak about encryption. I will prepare him with some remarks on the recognition on both the importance of encryption and the negative impact, a word of appreciation for our long-standing good cooperation on this issue and aspiration for continued bilateral effort for finding a proportionate solution and desire to play an active role in the EU process.

Regarding context, as you know encryption is a sensitive issue and in The Netherlands currently negotiations are ongoing on forming a new coalition government.

Is there anything in particular coming from your side that I would need to prep him for?

And for our multilateral process, do you think we can communicate a safe the date this week?

Thank you in advance!

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M^{102s}
@minvenj.nl
www.government.nl/venj
.....

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system. This email message has been swept for computer viruses.

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: zondag 6 juni 2021 12:12
Aan: 10.2.e; 10.2.e @bmi.bund.de; 10.2.e (TH) (FBI);
10.2.e @diplomatie.gouv.fr; 10.2.e @minbuza.nl; 10.2.e
10.2.e - BD/DRC/FO; 10.2.e @gov.si; 10.2.e - BD/PIDS;
10.2.e @om.nl; 10.2.e @policija.si; 10.2.e c@policija.si;
10.2.e @policija.si
CC: 10.2.e @bka.bund.de; 10.2.e @ZITIS.bund.de; 10.2.e
10.2.e
Onderwerp: Lawful access to encrypted data
Bijlagen: Synopsis multilateral meeting on encryption 18th May.docx

Dear colleagues,

I want to thank you again for your participation on the 18th of May I thought it was very informative and useful. I have written a synopsis outlining the different notions that have been voiced without attributing them to speakers. I wanted to combine this email with a save the date for our next meeting, but unfortunately we have yet not been able to find an appropriate time. We aim to organize a next meeting before the summer break.

If you have any additional contributions to the synopsis please let me know.

Kind regards,

10.2.e

Yours sincerely,

10.2.e

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

M 10.2.e
@minvenl.nl
www.government.nl/veni
.....

-----Oorspronkelijke afspraak-----

Van: 10.2.e - BD/DRC/CV
Verzonden: woensdag 28 april 2021 19:11
Aan: 10.2.e BD/DRC/CV; 10.2.e @bmi.bund.de; 10.2.e (TH)
(FBI); 10.2.e @diplomatie.gouv.fr; 10.2.e @minbuza.nl; 10.2.e BD/DRC/FO;
10.2.e @gov.si; 10.2.e - BD/PIDS; 10.2.e @om.nl; 10.2.e @policija.si;
10.2.e @policija.si; 10.2.e @policija.si
CC: 10.2.e @bka.bund.de; 10.2.e @ZITIS.bund.de; 10.2.e
Onderwerp: Lawful access to encrypted data

Tijd: dinsdag 18 mei 2021 16:00-17:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.
Locatie: WEBEX

Dear colleagues,

As previously announced we want to invite you to a stock-taking meeting on lawful access to encrypted data. All invited countries have issued a statement or resolution on finding technical solutions to lawful access to encrypted data. This topic is complex, it requires the balancing of different important interests, the search for possible solutions often encounters engaging societal debate and in addition there is the dependency on the private sector. Given the complex nature of this issue we think it might be beneficial to hear experiences of colleagues that have been active on this issue, keep appraised of each other's progress and discuss where we might cooperate in our respective processes.

We would like to invite colleagues that are active in (the policy field of) law enforcement and encourage different disciplines to participate in this meeting. Countries are free to invite, for example, a policy expert, a LEA representative and/or a technical expert.

The agenda shall include: latest developments, goals, future sessions and opportunities for multilateral action. If you have additional items please let me know.

I look forward to your participation and a lively meeting.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M 10.2.e
@minjenvi.nl
www.government.nl/veni
.....

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g

Deelnemen via telefoon

10.2.g

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g

10.2.g kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.g

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: maandag 14 juni 2021 15:52
Aan: 10.2.e @bmi.bund.de'
Onderwerp: RE: OECD Principle of access

That would be awesome, thank you so much!

On encryption ☺, the UK doesn't seem to be responding to mails on the second meeting which is disappointing. How would you feel about changing the order and have a legislative comparative session before the summer? We could discuss options on limiting the possible instrument for democratic countries and adhere to human rights.

I think it would be a pity since the technical issues are so much more urgent in the discussion. However, I cannot force their hand and want to keep momentum going into the summer.

Yours sincerely,

10.2.e

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

Van: 10.2.e @bmi.bund.de
Verzonden: maandag 14 juni 2021 15:40
Aan: 10.2.e - BD/DRC/CV
Onderwerp: AW: OECD Principle of access

10.2.a, 10.2.e

Von: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
Gesendet: Mittwoch, 9. Juni 2021 16:22
An: 10.2.e <10.2.e @bmi.bund.de>
Betreff: FW: OECD Principle of access

Dear 10.2.e

I hope you are doing well! I am reaching out to you in another file, because of our previous discussion on the need for government access. In the OECD we are drafting certain principles that regulate government access to data held by the private sector. 10.2.a

I have emailed the colleague's below of the BMWI and BMI, I do not know if you are familiar with them. But if you are and could pitch the need for government access somehow that would be great.

Kind regards,

10.2.e

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M 10.2.e

@minvenj.nl

www.government.nl/venj (<http://www.government.nl/...>)
.....

Van: 10.2.e - BD/DRC/CV

Verzonden: woensdag 9 juni 2021 16:14

Aan: 10.2.e @bmwi.bund.de' 10.2.e @bmwi.bund.de>; 10.2.e @bmi.bund.de'

10.2.e @bmi.bund.de>

Onderwerp: OECD Principle of access

Dear colleague's from Germany,

My name is 10.2.e I work in the Ministry of Justice and Security of the Netherlands, and I am the representative in the OECD process on principles for government access to personal data held by the private sector.

10.2.a

10.2.a

10.2.a

10.2.a

NB. It is not decided that we are going to introduce this text. I think it is important that we have a realistic chance of getting this in the text or at least a proper discussion, therefore the opinions of prominent contributors to the process is important. Also, I think having European partners support on this is important. Fortunately, we already have quite a bit of support.

In order to not delay our important work further I would like to provide the secretariat with a text that already enjoys wide support. This is why I reach out to you. You find the current version of our draft attached.

Thank you in advance for your consideration. Of course I would be happy to discuss this via a video conference and explain our proposal in more detail.

Yours sincerely,

10.2.e

.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit

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

.....
M^{102a}

@minvenj.nl

www.government.nl/venj (<http://www.government.nl/...>)
.....

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e

- BD/DRC/FO

Onderwerp: Opsporing, Nationale Veiligheid en Encryptie
Locatie: ZAAL WIJZIGING N22-05 - Schiermonnikoog – zaal

Begin: do 27-2-2020 15:00
Einde: do 27-2-2020 16:30

Terugkeerpatroon: (geen)

Vergaderingsstatus: Organisator van vergadering

Organisator:

Verplichte deelnemers:

10.2.e - BD/DRC/CV
10.2.e @om.nl; 10.2.e PaG Den Haag)
10.2.e @om.nl; 10.2.e @om.nl; 10.2.e @politie.nl;
10.2.e @politie.nl; 10.2.e - BD/DRC/CV;
10.2.e @belastingdienst.nl; 10.2.e @belastingdienst.nl;
10.2.e @belastingdienst.nl; 10.2.e @belastingdienst.nl; 10.2.e
@minbzk.nl; 10.2.e @minbzk.nl; 10.2.e - BD/DRC/CV; 10.2.e -
BD/PIDS; 10.2.e @minaz.nl; 10.2.e
10.2.e @belastingdienst.nl; 10.2.e - BD/DRC/CV; 10.2.e
10.2.e @politie.nl; 10.2.e @mindef.nl; 10.2.e (Landelijk Parket
Rotterdam) 10.2.e @om.nl; 10.2.e ; 10.2.e @minbzk.nl;
10.2.e @mindef.nl
10.2.e @mindef.nl; 10.2.e 10.2.e

Optionele deelnemers:

Urgentie: Hoog

Collega's,

Excuus er is iets mis gegaan met de zaal reservering!

Ik zie dat we in de NOORD toren zitten in zaal N22-05 - Schiermonnikoog – zaal

Beste collega's,

Vele van jullie zijn op de hoogte van de lopende inventarisatie naar toegang tot versleutelde informatie en de voor- en nadelen daarvan. Mijn collega 10.2.e heeft reeds in diverse bestaande gremia dit onderwerp met verschillende organisaties gesproken. Bijvoorbeeld, in het kader van Platform Interceptie, Decryptie en Sensing of het Platform Internetveiligheid.

We zouden dit overleg graag willen continueren en nodigen jullie uit om verder te praten over de behoeftes en mogelijkheden in dit dossier. Mochten anderen binnen jullie organisatie meer aangewezen zijn om aan te sluiten vraag ik deze naam aan mij door te geven.

Met vriendelijke groet,

10.2.e

Ministerie van Veiligheid en Justitie
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag |
Postbus 20301 | 2500 EH | Den Haag

.....
M10.2.e [redacted]
[redacted]@minvenj.nl
www.rijksoverheid.nl/venj
.....

Voor een veilige en rechtvaardige samenleving
.....

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: maandag 2 maart 2020 06:11
Aan: 10.2.e @minjenv.nl; 10.2.e (PaG Den Haag) 10.2.e @om.nl
Onderwerp: FW: PPT WG Opsporing, Nationale Veiligheid en Encryptie.pptx
Bijlagen: Opsporing, Nationale Veiligheid en Encryptie.pptx

Goedemorgen,

Ik zou iedereen nog even de ppt sturen plus de vragen:

- hoe vaak komt men encryptie tegen
- hoe vaak is tóch inzicht verkregen
- hoe? Breken encryptie, andere opsporingsmethode
- in wat voor opsporingsonderzoek
- welke toepassing encryptie: versleuteling van apparaat, Cloud, andere opgeslagen data, stromende data

Als jullie betere ideeën bij de vragen hebben hoor ik het graag.

Groeten,

10.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
Datum: woensdag 26 feb. 2020 18:46
Aan: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
Onderwerp: PPT WG Opsporing, Nationale Veiligheid en Encryptie.pptx

Ha 10.2.e
Fijne vakantie gehad?
Hierbij de presentatie die ik wil geven morgen.
Tot morgen,

10.2.e

Nr. E.006a

Opsporing, Nationale Veiligheid en Encryptie

Achtergrond

- Kabinetsstandpunt 2016
- Werkgroep OTT
- Brief van Barr et al
- Inventarisatie

Inventarisatie tot nu toe

- KP
- Partners van het kabinetsstandpunt
- Private partners
- Platform Interceptie, Decryptie en Sensing
- Academia

Waarom dit overleg?

- Probleem van encryptie beter inzichtelijk maken in de opsporing
- Inventariseren van oplossingen

Het probleem inzichtelijk

- Wat is het grootste probleem?

Het probleem inzichtelijk

- Wat is het grootste probleem?
 - Het apparaat is versleuteld; na beslagname is uitlezen lastig of onmogelijk.
 - De communicatiestroom is versleuteld; ondanks een bevel kan geen inzicht worden verkregen in stromende data.
 - Opgeslagen data is versleuteld; toegang tot een verdachte zijn CLOUD wordt steeds ingewikkelder.
 - De informatieverstrekking van derden wordt verstoord, E2E van Facebook Messenger

Het apparaat is versleuteld

Smartphone encryptie statistieken in Manhattan Oktober 1, 2014 – Oktober 31, 2017					
	2014	2015	2016	2017	Totaal
IOS					
Ontsleuteld	40	145	171	199	555
Versleuteld	59	382	538	466	1445
IOS totaal	99	527	709	665	2000
ANDROID					
Ontsleuteld	103	324	371	282	1180
Versleuteld	19	188	259	236	702
ANDROID totaal	122	512	630	618	1882
Totaal	221	1039	1339	1283	3882

Het apparaat is versleuteld

Crime type of all mobile devices in Manhattan January 1, 2019 – September 1, 2019	
Larceny/Forgery/Fraud/Cybercrime/ID Theft	25.8%
Sex crime	17.5%
Drug Charge	16.1%
Homicide/attempted murder	14.0%
Assault/Robbery/Burglary	13.4%
Weapon charge	7.8%
Other	5.5%

De communicatiestroom is versleuteld

Indicatoren Unit Landelijke Interceptie	
	2018
Aantal nummers waarvoor een bevel tot aftappen is gegeven	23.458
Gemiddeld aantal taps per dag	1.397
IP-taps*	
Gemiddeld aantal IP- taps per dag	
Aantal aanvragen op historische gegevens**	56.882
* Dit betreft zowel internettaps als e-mailtaps. Sinds de invoering van de nieuwe interceptiestandaard wordt, zowel technisch als procedureel, geen onderscheid meer gemaakt tussen een telefoontap en een internettap. Het onderscheid in de tellingen komt hiermee m.i.v. 2014 te vervallen. ** Zoals verkeersgegevens en identificerende gegevens. Het gaat bij deze nummers niet alleen over telefoonnummers, maar ook over IP-adressen en emailadressen.	

De communicatiestroom is versleuteld

Tap statistieken in de VS			
	Aantal taps	Encryptie	Geen inzicht verkregen
2013	3.576	41	9
2014	3.554	22	2
2015	4.148	7	7
2016	3.168	57	48
2017	3.813	102	97
2018	2.937	220	192

De communicatiestroom is versleuteld

2018	Total: 2937
Narcotics	1.354 (46%)
Conspiracy	389 (13%)
Homicide and Assault	130 (4%)
Racketeering	91
Corruption	28
Larceny, Theft, Robbery	13
Gambling	12
Kidnapping	0
Other	920

Opgeslagen data: golden age of surveillance

<u>Vergelijking van databronnen</u>				
	Device	iCLOUD	Google Cloud Storage	Phone company
iMessage content	Yes	No (1)	N/A	No
iMessage detail (dates, times, phone numbers involved)	Yes	No (1)	N/A	No
SMS/MMS content	Yes	No (1)	Perhaps (2)	Perhaps (3)
SMS/MMS details (dates, times, phone numbers involved)	Yes	No (1)	Perhaps(2)	Yes
Phone call detail (dates, times, phone numbers involved)	Yes	Yes	Perhaps(2)	Yes
Historical cell site data	No	No	Perhaps(2)	Perhaps (4)
Historical other cell tower-related data	Perhaps (5), (6)	No	Perhaps (7)	No
Historical Wi-Fi network data	Perhaps (6)	Yes	Perhaps (7)	No
Historical GPS or other satellite data	Perhaps (6)	Perhaps, some (2), (8)	Perhaps (7)	No
Contacts	Yes	Perhaps (2)	Perhaps (2)	No
Photo's/video's	Yes	Perhaps (2)	Perhaps (2)	No
Internet Search History	Yes	Perhaps (2)	Unknown	No
Internet Bookmarks	Yes	Perhaps (2)	Unknown	No
Third-Party App data	Perhaps (6)	No	Unknown	No

De informatieverstrekking van derden wordt verstoord

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

Oplossingen? – een breed overzicht

- Kabinetsstandpunt 2016
- 1a Reguleren encryptietechnologie
- 1b Rekenkracht van de opsporing
- 1c Samenwerking met derde partij
- 2 Alternatieven

Reguleren encryptietechnologie

- Verzwak encryptie
- Versimpel het verzamelen of volgen van sleutels
 - Key escrow
 - Centraal bij overheid, provider of derde partij
 - Decentraal op het apparaat
 - In stukken bij verschillende partijen

Rekenkracht van de opsporing

- Raden van de sleutel
- Deactiveren van het maximum aantal pogingen voor ontgrendeling in het individuele geval

Derde partij

- Masterkey of achterdeur
- Valse update
- Zonder voorgeschreven technische oplossing

Mogelijk in het individuele geval?

Alternatieven

Decryptiebevel verdachten	Toegang tot het device (CCIII)
Verbeter kennis bij de opsporing over data die (nog) wel beschikbaar is	Voeg een dienst toe aan de chat
Homomorphic encryption	Investeer in financiële en technische mogelijkheden bij de opsporing
Vergemakkelijk medewerking van Inlichtingen en Veiligheidsdiensten	Vind een plaintext kope (bv een niet versleutelde oude kopie)
Stel verstrekking, bezit of gebruik strafbaar als strafverzwarende omstandigheid	Verdere ontwikkelingen; restricted key

Kritiek

- Dit is ineffectief.
 - Dit levert onacceptabele risico's op voor cybersecurity.
 - Dit is een onacceptabel risico voor privacy en burgerlijke vrijheden.
 - Men stelt dienstverleners voor een onmogelijke opgave
 - Dit schaadt de innovatie van encryptie.
-

Dus houd rekening met

- 1)effectiviteit van de oplossing op het gebied van schaalbaarheid, betrouwbaarheid en duurzaamheid of bestendigheid, 2) veiligheid van data of apparaat en cybersecurity, 3) privacy, burgerlijke vrijheden en mensenrechten, 4) handel, competitiviteit en innovatie, 5) financiële kosten en de dragers daarvan, 6) prioriteiten binnen de opsporing, 7) de internationale context, en 8) evaluatie en toezicht
- 1) voorkom absolute stellingname, 2) start het debat door het vaststellen van een gezamenlijke zorg, 3) erken dat veiligheid vele vormen aanneemt en verweekeld is met privacy en afhankelijk is van wat mogelijk is, 4) neem diverse belangen in overweging: privacy, cybersecurity, maatschappelijke veiligheid, nationale veiligheid, competitief vermogen, buitenlands beleid, vrijheid van meningsuiting, burgerlijke vrijheden en de noodzaak voor een open internet, 5) weest bewust van internationale dynamieken, 6) denk aan de lange termijn, 7)accepteer imperfectie, 8) splits de discussie zo nodig in meerdere onderdelen, 9) plaats encryptie in de brede context van opsporingsbevoegdheden, 10) accepteer dat er geen puur technische oplossing is, 11)erken de uitdaging van een effectieve implementatie, 12) balanceer de behoefte voor een strategische benadering en de behoefte voor technisch detail, en 13) produceer goede data en onderbouwing voor de risico's en voordelen van een oplossing.
- 1) gemeenschappelijke verantwoordelijkheid, verminderde toegang tot data is een onderwerp waar alle betrokken actoren een verantwoordelijkheid in hebben. Dienstverleners moeten kunnen voldoen aan de wet en overheden moeten accepteren dat door encryptie in bepaalde gevallen geen toegang kan worden verkregen tot data. 2) De rechtstaat en rechtswarborgen staan voorop, toegang tot data moet worden gereguleerd door de bescherming voor burgers die de rechtstaat biedt. 3) vrijheid in de keuze voor rechtmatige toegang, dienstverleners worden aangemoedigd om zelf met oplossingen te komen met respect voor ieders technische infrastructuur. Indien oplossingen uitblijven kan een technische oplossing worden afgedwongen.

Wat willen we met de werkgroep

- Kunnen we nut en noodzaak beter onderbouwen?
- Uitwerken oplossingen
- Afstemmen resultaten en initiatieven

10.2.e

- BD/DRC/FO

Onderwerp: Geannuleerd: Opsporing, Nationale Veiligheid en Encryptie
Locatie: N22-01 - Texel - zaal

Begin: wo 18-3-2020 15:00
Einde: wo 18-3-2020 17:00
Tijd weergegeven als: Vrij

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator:

Verplichte deelnemers:

10.2.e - BD/DRC/CV
10.2.e @om.nl; 10.2.e (PaG Den Haag)
10.2.e @om.nl; 10.2.e @om.nl; 10.2.e @politie.nl;
10.2.e @politie.nl; 10.2.e - BD/DRC/CV;
10.2.e @belastingdienst.nl; 10.2.e @belastingdienst.nl;
10.2.e @belastingdienst.nl; 10.2.e r@belastingdienst.nl; 10.2.e
@minbzk.nl; 10.2.e @minbzk.nl; 10.2.e - BD/DRC/CV; 10.2.e -
BD/PIDS; 10.2.e @minaz.nl; 10.2.e
10.2.e @belastingdienst.nl; 10.2.e - BD/DRC/CV; 10.2.e
10.2.e @politie.nl; 10.2.e @mindef.nl; 10.2.e (Landelijk Parket
Rotterdam) 10.2.e @om.nl; 10.2.e ; 10.2.e @minbzk.nl;
10.2.e @mindef.nl; 10.2.e @mindef.nl; 10.2.e
10.2.e @politie.nl)
10.2.e

Optionele deelnemers:

Urgentie: Hoog

Hallo allemaal,

Deze vergadering wordt geannuleerd. We hebben de vorige keer gevraagd aan organisaties om te inventariseren welke toepassing van encryptie het meest problematisch is en hoe groot de problematiek daarbij is. We hebben toen enkele vragen verspreid:

- hoe vaak komt men encryptie tegen?
- hoe vaak is toch inzicht verkregen?
- hoe? Breken encryptie, andere opsporingsmethode?
- in wat vooropsporingsonderzoek?
- welke toepassing encryptie: versleuteling van apparaat, Cloud, andere opgeslagen data, stromende data.

Zouden jullie mij donderdag kunne mailen met welke mogelijkheden jullie zien in jullie organisaties om hier een beeld van te krijgen?

10.2.e

- BD/DRC/FO

Onderwerp: Encryptie: opsporing en nationale veiligheid
Locatie: Webex

Begin: wo 14-10-2020 14:00
Einde: wo 14-10-2020 15:00

Terugkeerpatroon: (geen)

Vergaderingsstatus: Organisator van vergadering

Organisator:

Verplichte deelnemers:

10.2.e - BD/DRC/CV
 10.2.e 10.2.e @politie.nl; 10.2.e @politie.nl;
 10.2.e @minbzk.nl; 10.2.e - BD/DRC/FO; 10.2.e
 10.2.e (PaG Den Haag) 10.2.e @om.nl; 10.2.e @om.nl; 10.2.e
 10.2.e - BD/DRC/CV; 10.2.e 10.2.e -
 BD/DGPenV/PPBT/PBO; 10.2.e - BD/DEIA/EU; 10.2.e - BD/DRC/CV;
 10.2.e @minbzk.nl; 10.2.e @mindef.nl; 10.2.e @minbzk.nl;
 10.2.e - BD/PIDS; 10.2.e @minbzk.nl
Optionele deelnemers:
 10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e -
 BD/DGPenV/PPBT/PBO; 10.2.e - BD/DGPenV/PBT/PBI

Hallo allemaal,

We zijn een tijdje niet bij elkaar gekomen over dit onderwerp. Er is in de tussentijd veel gebeurd, voornamelijk op Europees niveau. Daar praat ik jullie graag even over bij en zal toelichten wat dit kan betekenen voor de nationale verkenning naar mogelijkheden voor rechtmatige toegang voor versleuteld bewijs.

Een kort overzicht wat is gebeurd/gepubliceerd:
 -'deep dive' met Facebook

-CTC paper

Analyse van de ervaren problematiek met diverse toepassingen van encryptie. Hierin wordt oa de vraag aan COSI gesteld wat de uitdagingen zijn bij encryptie. Daarnaast worden diverse initiatieven genoemd als 'Moving forward'.

-Europese Commissie paper

Analyse van ervaren problematiek met E2EE. Hierin wordt oa de vraag aan COSI gesteld hoe de EU een rol kan spelen in dit debat. Daarnaast worden diverse initiatieven genoemd als 'Moving forward'.

-Europees Voorzitterschap paper

Document over hoe het voorzitterschap het onderwerp verder wilt brengen. Hierin wordt oa de vraag aan COSI gesteld welke rol het VZS kan vervullen.

-Cosi bespreking 23 sept jl.

Encryptie (doc.nrs 10728/20 en 10730/20) - 10.2.a

onder meer NL stond positief tegenover een gemeenschappelijke positie c.q. EU-verklaring over encryptie; op basis van de schriftelijke opmerkingen die LS indienen (voor 7 oktober), zal het Vzschap bekijken of op werkgroepniveau of in COSI de verklaring nader kan worden uitgewerkt;

-EU security union strategy

Document waarin de noodzaak voor een technische oplossing voor rechtmatige toegang wordt toegelicht in de strijd tegen online kindermisbruik.

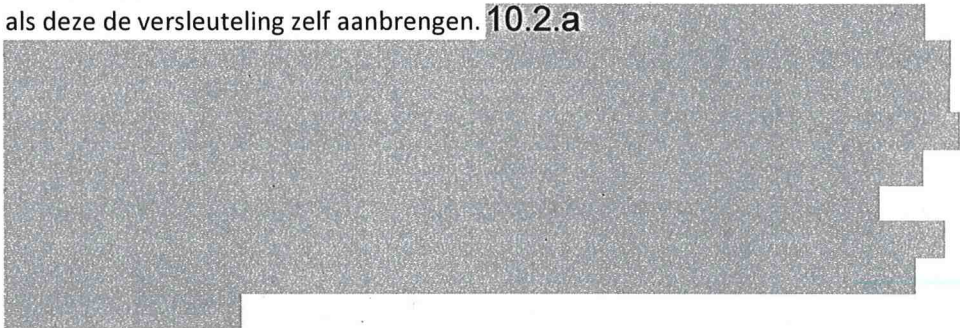
Essentie: De problematiek wordt erkend. Goed om mogelijke technische oplossingen met ISP's te inventariseren. Sluit hierbij zo weinig mogelijk oplossingen bij voorbaat uit om goed de impact van oplossingen te inventariseren op fundamentele rechten en veilige communicatie en deze af te wegen tegen de noodzaak voor een efficiënte en zorgvuldige opsporing.

Nederland is op dit moment tegen wettelijke beperkingen rond de beschikbaarheid, ontwikkeling en het gebruik van encryptie. Men is tot deze conclusie gekomen op basis van de beschikbare oplossingen in 2016 en de afweging tussen de negatieve – en positieve gevolgen van versleuteling. Het is goed wanneer er een inventarisatie plaatsvindt om te bezien of de negatieve gevolgen voor de opsporing- en veiligheidsdiensten kunnen worden verzacht terwijl de positieve karakteristieken van versleuteling zoals fundamentele rechten en veilige communicatie voldoende kunnen blijven worden gewaarborgd.

Appreciatie:

Dank aan de CIE voor de informatie en haar initiatieven tot nu toe.

NL herkent het dilemma rond encryptie die in het stuk worden geschetst. Sterke en standaard encryptie belemmert een steeds meer data afhankelijke opsporing in steeds grotere mate, terwijl tegelijkertijd sterke encryptie belangrijk is voor het borgen van fundamentele rechten en vertrouwelijke communicatie. We moeten daarbij niet uit het oog verliezen dat ook de voordelen van een datagedreven opsporing, zoals een scherpere gerichtheid en grotere doeltreffendheid, teniet kunnen worden gedaan. Versleuteling belemmert immers het betrekken van data in de datagedreven opsporing.

1. Er zijn wel een aantal opmerkingen te maken bij het stuk van de CIE:
 - Wat is het probleem?
 - 10.2.a . Zoals vermeld in het CTC paper zijn er diverse toepassingen van versleuteling die wellicht andere oplossingen vragen: naast stromende data is daar de versleuteling van opgeslagen data (CLOUD), versleuteling van social media platformen en de versleuteling van apparaten.
 - Kan de CIE een terugkoppeling geven of en hoe deze diverse toepassingen van versleuteling zijn besproken in de expertmeeting? Heeft men aangegeven dat de problematiek bij end-to-end versleuteling het meest urgent is?
 - Als de Commissie of Lidstaten een meer gedetailleerde cijfermatige onderbouwing hebben van de problematiek houdt Nederland zich aanbevolen.
 - Wat lossen we op?
 - Nederland kent voor traditionele telecommunicatie aanbieders een ontsleutelplicht als deze de versleuteling zelf aanbrengen. 10.2.a 
 - Een punt voor opheldering: De CIE benoemt terecht de problematiek rond apps zoals Encrochat, door technische oplossingen bij ISP's lossen we dit probleem niet op. Het opzetten van nieuwe apps kan met de juiste expertise relatief snel gebeuren en aan de zicht van de opsporing worden onttrokken. Hoe ziet de CIE dit?

- Voorwaarden en waarborgen
 - NL ondersteunt de noodzaak voor proportionaliteit, subsidiariteit, effectiviteit.
 - In het gedeelte 'Moving Forward' staat dat verzwakking van encryptie niet wordt ondersteund. 10.2.a

[REDACTED]

Uitgangspunt is dat fundamentele rechten moeten worden gerespecteerd en veilige communicatie niet op een onacceptabele manier moet worden geschaad.

- Bedrijven worden gevraagd zelf met targeted oplossingen komen voor de verschillende categorieën van encryptie.

2. Standpunt NL tot nu toe:

- Kabinetsstandpunt NL 2016:
 - It is the responsibility of the cabinet to guarantee the security of the Netherlands and to investigate criminal offences. The cabinet underlines the necessity of lawful access to information and communication in this respect. Additionally, government authorities, companies, and citizens benefit from maximum security of digital systems. The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.

The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands.

- In het kader van de inventarisatie naar mogelijkheden voor rechtmatige toegang steunt NL een initiatief om oplossingen te inventariseren voor de rechtmatige toegang tot versleuteld bewijs. NL pleit voor een brede inventarisatie: zonder het bij voorbaat uitsluiten van oplossingen en op alle door de CTC erkende toepassingen van encryptie. Op deze manier kan een afweging over proportionaliteit en subsidiariteit over de gehele breedte worden uitgevoerd.
- NL steunt dat dit initiatief wordt aangekondigd in een statement vanuit de EU of een groep Lidstaten.

5. Questions for discussion

Delegations are invited to reflect and express their views on the following questions:

- What are the most pressing challenges related to the use encryption that law enforcement and judicial authorities are facing in your Member State? How are your national authorities tackling or planning to tackle these challenges?

- The problem described in the paper is recognizable. Three current powers of law enforcement are affected by encryption: interception, the production order and reading confiscated automated works. This leads to three challenges:

1. How do we ensure an open, free and secure internet? Criminal investigations are increasingly dependent on electronic evidence. 10.2.a

2. How do we ensure that decisions in the digital realm do not negatively affect security in the offline world. The decision of Facebook to encrypt its messaging platform has consequences for the fight against child abuse. The security standards of the 5G network has negative consequences for the interception of communication services which is an indispensable asset in the fight against organised crime. The increasing encryption of phones restricts law enforcement to identify social contacts and networks of criminals, for example in the San Bernadino case.

3. 10.2.a
OTT-services are increasingly popular and with the Electronic Communications Code OTT-services are considered similar to traditional telecommunication services. 10.2.a
A legal obligation in the Netherlands is that no telecommunication service or provider should be available that cannot be intercepted. In addition telecommunication service providers have the obligation to decrypt their communication services.

- How do we tackle these challenges:

1. 10.2.a

- What is your view on the proposed guidelines for an optimal solution?

10.2.a

- How the EU can best support Member States to address these challenges? What is your view on the proposed recommendations?

First the observatory role of Europol is highly appreciated, as well as the practical measures. Furthermore, the current availability of possible technical solutions should 10.2.a

10.2.e - BD/DRC/FO

Onderwerp: Encryptie: opsporing en nationale veiligheid
Locatie: Webex

Begin: wo 16-12-2020 14:30
Einde: wo 16-12-2020 16:00

Terugkeerpatroon: (geen)

Vergaderingsstatus: Organisator van vergadering

Organisator:

Verplichte deelnemers:

10.2.e - BD/DRC/CV
10.2.e @politie.nl; 10.2.e @politie.nl;
10.2.e @minbzk.nl; 10.2.e - BD/DRC/FO; 10.2.e
10.2.e (PaG Den Haag) 10.2.e @om.nl; 10.2.e @om.nl; 10.2.e
10.2.e - BD/DRC/CV; 10.2.e 10.2.e -
BD/DGPenV/PPBT/PBO; 10.2.e - BD/DEIA/EU; 10.2.e - BD/DRC/CV;
10.2.e @mindef.nl; 10.2.e @minbzk.nl; 10.2.e -
BD/DGPenV/PPBT/PBO; 10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e -
BD/PIDS; 10.2.e - BD/DGPenV/PBT/PBI; 10.2.e @minbzk.nl;
10.2.e @holmes.nl; 10.2.e @om.nl; 10.2.e (Landelijk Parket Rotterdam)
10.2.e @om.nl; 10.2.e @mindef.nl; 10.2.e @holmes.nl;
10.2.e @politie.nl; 10.2.e - BD/DRC/CV
10.2.e - BD/DRC/CV; 10.2.e - BD/DGPenV/PPBT/PBO;
10.2.e @politie.nl'

Optionele deelnemers:

Beste collega's,

Er zijn weer de nodige ontwikkelingen op het gebied van rechtmatige toegang tot versleuteld bewijs die we graag met de partijen in de opsporing en nationale veiligheid bespreken. Eerder hebben we de apart gesproken met de beleidsverantwoordelijken en de technische experts. Gezien de onderwerpen die we met jullie bespreken is het denk ik goed om beide expertises tegelijkertijd uit te nodigen.

De agenda is wat ons betreft:

1. Er is toestemming gegeven om via het WODC een onderzoek uit te zetten naar het effect van encryptie op de opsporing. We bespreken graag wat een wenselijke scope is en de mogelijkheden die we richting onderzoekers kunnen presenteren.
2. De dynamiek rond OTT-diensten en 'crypto-diensten die voor en door criminelen worden gebruikt' in de discussie rond rechtmatige toegang tot versleuteld bewijs.
3. Een vooruitblik van het EU-traject.

Als er vanuit jullie nog onderwerpen zijn neem dan gerust contact met mij op.

Bijgevoegd VSO en GA die nav de JBZ zijn opgesteld zijn openbaar.

De Raadsresolutie en het document 'going forward EC' zijn niet openbaar, graag vertrouwelijk behandelen.

Met vriendelijke groet,

10.2.e

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g

Netherlands Toll

10.2.g

United States Toll

Deelnemen via telefoon

10.2.g

Netherlands Toll

10.2.g

United States Toll

[Algemene inbelnummers](#)

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g

U kunt ook 10.2.g kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.g

Als u een host bent, [klik dan hier](#) om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e

- BD/DRC/FO

Van:

Verzonden:

Aan:

10.2.e - BD/DRC/CV

maandag 14 december 2020 19:13

10.2.e @politie.nl; 10.2.e @politie.nl;

10.2.e @minbzk.nl; 10.2.e - BD/DRC/FO; 10.2.e

(PaG Den Haag) 10.2.e @om.nl; 10.2.e @om.nl; 10.2.e

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

BD/DGPenV/PPBT/PBO; 10.2.e BD/DEIA/EU; 10.2.e - BD/DRC/CV;

10.2.e @mindef.nl; 10.2.e @minbzk.nl; 10.2.e

BD/DGPenV/PPBT/PBO; 10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e

BD/PIDS; 10.2.e - BD/DGPenV/PBT/PBI; 10.2.e @minbzk.nl;

10.2.e @holmes.nl; 10.2.e @om.nl; 10.2.e (Landelijk Parket Rotterdam)

10.2.e @om.nl; 10.2.e @mindef.nl; 10.2.e @holmes.nl;

10.2.e @politie.nl; 10.2.e - BD/DRC/CV

CC:

10.2.e - BD/DRC/CV; 10.2.e BD/DGPenV/PPBT/PBO;

10.2.e @politie.nl

Onderwerp:

Bijlagen:

RE: Encryptie: opsporing en nationale veiligheid

eindversie ST_13084_2020_REV_1_en.pdf; TK Raadsconclusies over rechtmatige

toegang tot versleuteld bewijs.docx; EUR in beslag genomen telefoon 2598-

volledige-tekst_tcm28-74084.pdf

Beste collega's,

Sinds vanochtend 10:00 is bijgevoegde raadsresolutie openbaar en zojuist is ook de bijgevoegde brief verstuurd. De raadsresolutie is hier te vinden: <https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/>

Als derde voeg ik ook een onderzoek bij van 2016 over onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken. Dit kan wellicht ter inspiratie dienen voor ons eigen onderzoek. Met een 'ctrl+F' op encryptie kun je de relevante passage over encryptie vinden.

Tot woensdag.

Met vriendelijke groet,

10.2.e

10.2.e

10.2.e

@minveni.nl

-----Oorspronkelijke afspraak-----

Van: 10.2.e - BD/DRC/CV

Verzonden: woensdag 2 december 2020 12:53

Aan: 10.2.e - BD/DRC/CV; 10.2.e @politie.nl; 10.2.e @politie.nl;

10.2.e @minbzk.nl; 10.2.e - BD/DRC/FO; 10.2.e (PaG Den Haag)

10.2.e @om.nl; 10.2.e @om.nl; 10.2.e - BD/DRC/CV; 10.2.e

10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e - BD/DEIA/EU; 10.2.e - BD/DRC/CV;

10.2.e @mindef.nl; 10.2.e @minbzk.nl; 10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e . -
BD/DGPenV/PPBT/PBO; 10.2.e BD/PIDS; 10.2.e - BD/DGPenV/PBT/PBI; 10.2.e @minbzk.nl;
10.2.e @holmes.nl; 10.2.e @om.nl; 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl);
10.2.e @mindef.nl; 10.2.e @holmes.nl; 10.2.e @politie.nl; 10.2.e - BD/DRC/CV
CC: 10.2.e - BD/DRC/CV; 10.2.e BD/DGPenV/PPBT/PBO; 10.2.e @politie.nl'

Onderwerp: Encryptie: opsporing en nationale veiligheid

Tijd: woensdag 16 december 2020 14:30-16:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm, Wenen.

Locatie: Webex

Beste collega's,

Er zijn weer de nodige ontwikkelingen op het gebied van rechtmatige toegang tot versleuteld bewijs die we graag met de partijen in de opsporing en nationale veiligheid bespreken. Eerder hebben we de apart gesproken met de beleidsverantwoordelijken en de technische experts. Gezien de onderwerpen die we met jullie bespreken is het denk ik goed om beide expertises tegelijkertijd uit te nodigen.

De agenda is wat ons betreft:

1. Er is toestemming gegeven om via het WODC een onderzoek uit te zetten naar het effect van encryptie op de opsporing. We bespreken graag wat een wenselijke scope is en de mogelijkheden die we richting onderzoekers kunnen presenteren.
2. De dynamiek rond OTT-diensten en 'crypto-diensten die voor en door criminelen worden gebruikt' in de discussie rond rechtmatige toegang tot versleuteld bewijs.
3. Een vooruitblik van het EU-traject.

Als er vanuit jullie nog onderwerpen zijn neem dan gerust contact met mij op.

Bijgevoegd VSO en GA die nav de JBZ zijn opgesteld zijn openbaar.

De Raadsresolutie en het document 'going forward EC' zijn niet openbaar, graag vertrouwelijk behandelen.

Met vriendelijke groet,

10.2.e

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g Netherlands Toll
10.2.g United States Toll

Deelnemen via telefoon

10.2.g
10.2.g

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g

U kunt ook 10.2.g kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 1759511256.rijksvideo@lync.webex.com

Als u een host bent, [klik dan hier](#) om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e

BD/DRC/FO

Onderwerp: Encryptie: opsporing en nationale veiligheid startnotitie WODC
Locatie: Webex

Begin: do 18-2-2021 09:00
Einde: do 18-2-2021 10:15

Terugkeerpatroon: (geen)

Vergaderingsstatus: Organisator van vergadering

Organisator:

Verplichte deelnemers:

10.2.e BD/DRC/CV
10.2.e @politie.nl; 10.2.e @politie.nl;
10.2.e @minbzk.nl; 10.2.e BD/DRC/FO; 10.2.e
(PaG Den Haag) 10.2.e @om.nl; 10.2.e @om.nl; 10.2.e
- BD/DRC/CV; 10.2.e
BD/DGPenV/PPBT/PBO 10.2.e - BD/DEIA/EU; 10.2.e BD/DRC/CV;
10.2.e @mindef.nl; 10.2.e @minbzk.nl; 10.2.e
BD/DGPenV/PPBT/PBO; 10.2.e - BD/DGPenV/PPBT/PBO; 10.2.e
BD/PIDS; 10.2.e - BD/DGPenV/PBT/PBI; 10.2.e @minbzk.nl;
10.2.e @holmes.nl; 10.2.e @om.nl; 10.2.e Landelijk Parket Rotterdam)
10.2.e @om.nl; 10.2.e @mindef.nl; 10.2.e @holmes.nl;
10.2.e @politie.nl; 10.2.e - BD/DRC/CV; 10.2.e
BD/DGPenV/PPBT/PBO; 10.2.e @politie.nl; 10.2.e - BD/DRC/CV

Hallo collega's,

We hebben de concept-startnotitie van het WODC onderzoek binnen naar het effect van encryptie op de opsporing. Het WODC heeft gevraagd om deze niet uitgebreid te verspreiden, dus ik zal h'm later alleen nasturen aan degene die volgende week donderdag aanwezig kunnen zijn. Het onderzoek ziet op de opsporingsdiensten, maar het staat de collega's van de IenV diensten vrij om aan te sluiten.

Met vriendelijke groet,

10.2.e

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.g

Wachtwoord voor vergadering: 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.g Netherlands Toll

10.2.g [redacted] United States Toll

Deelnemen via telefoon

10.2.g [redacted] Netherlands Toll

10.2.g [redacted] United States Toll

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.g [redacted]

U kunt ook 10.2.g [redacted] kiezen en uw vergaderingsnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.g [redacted]@lync.webex.com

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e - BD/DRC/FO

Van: 10.2.e BD/DRC/CV
Verzonden: vrijdag 12 februari 2021 16:53
Aan: 10.2.e @politie.nl; 10.2.e BD/DRC/FO; 10.2.e
10.2.e (PaG Den Haag); 10.2.e @om.nl; 10.2.e @om.nl; 10.2.e
; 10.2.e @mindef.nl; 10.2.e - BD/PIDS; 10.2.e @holmes.nl;
10.2.e @om.nl; 10.2.e @holmes.nl; 10.2.e @minbzk.nl; 10.2.e
BD/DGPenV/PPBT/PBO; 10.2.e @minbzk.nl
CC: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
Onderwerp: Startnotitie WODC encryptie
Bijlagen: concept_startnotitie_3218.docx

Beste collega's,

Jullie hebben het overleg volgende week over de startnotitie van het WODC voor het onderzoek 'de impact van encryptie op de opsporing' (voorlopig) geaccepteerd. Drie punten waar we in ieder geval jullie vragen om naar te kijken zijn:

- 1) Afbakening van de reikwijdte van het onderzoek. Wat zijn mogelijkheden om het onderzoek meer af te bakenen, bijvoorbeeld door het te beperken tot bepaalde toepassingen van encryptie (geautomatiseerde werken en stromende data) / opsporingsbevoegdheden (Inbeslagname geautomatiseerde werken en interceptie) / misdrijven,
- 2) De risico's en onzekerheden en beslispunten paragraaf. We zijn ons bewust dat niet alle data voorhanden is , maar wat is mogelijk en onmogelijk / kunnen we bevel turven in de tapkamer of bij het NFI / hoe kunnen we moeilijkheden mitigeren?
- 3) Gekozen misdrijven de juiste?

Andere punten zijn uiteraard ook welkom.

Zelf zijn we overwegend tevreden over het eerste concept. Bijvoorbeeld de structuur dat eerst de makke kwantitatief wordt geprobeerd in kaart te brengen, en dan kwalitatief het effect op het verloop van het onderzoek en de uitkomst van opsporingsonderzoeken. Naast bovenstaande punten vonden we het onderwerp 'mensenhandel' in de eerste paragraaf verassend. We denken dat 10.2.c

Groot gebrek in de onderzoeksopzet is de aandacht voor 'vervolgning', opzet lijkt nu beperkt tot identificatie/stoppen en verstoren.

Ik kijk uit naar jullie input, alvast bedankt!

Fijn weekend.

Met vriendelijke groet,

10.2.e

M 10.2.e

@minveni.nl

Nr. E.013

Oproep aan kabinet: stimuleer encryptie (stimuleer-encryptie.nl)

“Wij roepen het volgende kabinet op de ontwikkeling, de beschikbaarheid en de toepassing van alle vormen van encryptie te stimuleren.”

Techbedrijven	Cybersecurity	Maatschappelijk middenveld	Wetenschap
A2B Internet	Cyberveilig Nederland Belangenvereniging voor zo'n 60 bedrijven in de cybersecurity sector	Amnesty International	ACCSS Vereniging voor wetenschappers die actief zijn op het terrein van cybersecurity
AMS-IX	Dutch Institute for Vulnerability Disclosure (DIVD)	Bits of Freedom	10.2.e Universiteit van Amsterdam
Apple	Fox-IT	Expertisecentrum Online Kindermisbruik (EOKM)	10.2.e Vrije Universiteit Amsterdam
BIT	ISOC NL	Free Press Unlimited	10.2.e Universiteit Leiden
Facebook	Secura	Kennisnet	10.2.e Universiteit van Amsterdam
Freedom Internet	10.2.e 10.2.e cyber security research NWO; 10.2.e dcypher en 10.2.e ACCSS	Open State Foundation	10.2.e 10.2.e Hogeschool Utrecht
Google	10.2.e 10.2.e IAB en IESG best current practice over encryptie technologie	Privacy Management Partners	10.2.e TU Eindhoven
KPN	10.2.e Government crypto specialist	Qiy Foundation	10.2.e (CSR) Radboud Universiteit
Leaseweb Global	10.2.e Beveiligingsexpert	Stichting NLnet	10.2.e Universiteit van Tilburg
Microsoft		Transparency International	10.2.e Universiteit van Amsterdam
NXP Semiconductors		Vrijdschrift	10.2.e TU Eindhoven
Procolix		Waag	10.2.e

			Universiteit Leiden en partner Considerati
SIDN		10.2.e Internet Society	10.2.e Universiteit van Amsterdam
Schuberg Philis		BRANCHORGANISATIES	10.2.e (CSR) Universiteit Leiden
T-Mobile		Vereniging van Onderzoeksjournalisten (VVOJ) Vereniging van zo'n 600 onderzoeksjournalisten	10.2.e Universiteit Twente
VodafoneZiggo		SURF Vereniging van zo'n 100 onderwijs- en onderzoeksinstellingen	10.2.e Universiteit Leiden
Voys en VoIPGRID		NDP Nieuwsmedia Brancheorganisatie van nieuwsmedia	10.2.e Open Universiteit
WhatsApp		Nederlandse Vereniging van Journalisten (NVJ) Vereniging van zo'n 8.000 journalisten en mediamakers	10.2.e (CSR) TU Delft
BRANCHEORGANISATIES		Dutch Startup Association	10.2.e Universiteit van Amsterdam
DINL Coalitie van organisaties voor een sterke digitale infrastructuur		Consumentenbond	10.2.e Universiteit Twente
Dutch Cloud Community Branchevereniging voor zo'n 80 hostingbedrijven (v/h DHPA en ISPConnect)		American Chamber of Commerce in the Netherlands	10.2.e Radboud Universiteit
Dutch Data Center Association Brancheorganisatie voor zo'n 120 datacenters			
NLconnect			

Brancheorganisatie van zo'n 80 bedrijven in de breedbandindustrie			
NLdigital Brancheorganisatie van zo'n 600 ICT- bedrijven			
Nationale Beheersorganisatie Internet Providers (NBIP)			
Vereniging van Registrars Brancheorganisatie voor zo'n 1.250 .nl- registrars			



MJenV

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

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

Contactpersoon

10.2.e

10.2.e

T 10.2.e

@minjenv.nl

Datum

19 maart 2021

Projectnaam

Encryptie / OTT

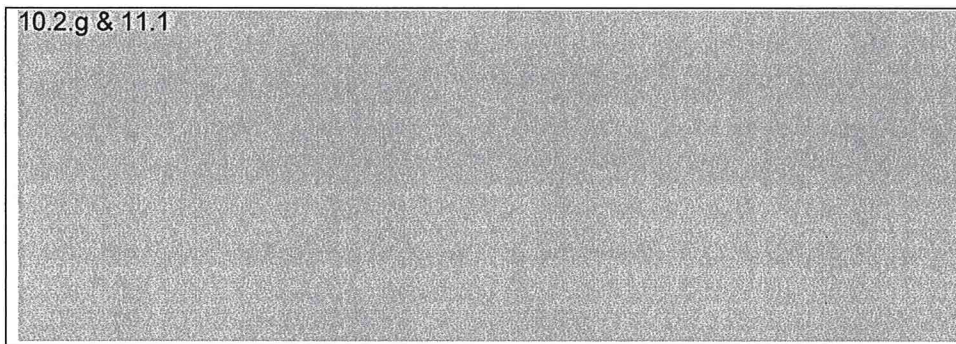
Ons kenmerk

3270470

nota

Gesprek ondertekenaars oproep encryptie

10.2.g & 11.1



1 Doel nota

- Akkoord op de vormgeving van het gesprek met de ondertekenaars van de oproep die het volgende kabinet aanspoort de ontwikkeling, beschikbaarheid en toepassing van alle vormen van encryptie te stimuleren.

U wordt geadviseerd om conform uw toezegging zo snel mogelijk in gesprek te gaan met een selectie van de ondertekenaars van de oproep. Parallel kunt u uw ambtenaren de opdracht geven om met een bredere groep ondertekenaars in gesprek te gaan. Tevens is vernomen dat de Cybersecurityraad (CSR) dit onderwerp ambtelijk wenst te bespreken. 10.2.e staat op de lijst om te worden uitgenodigd in het gesprek met u. KPN en de overige wetenschappers van de CSR worden voor de ambtelijke overleggen uitgenodigd.

Het voorstel is om ook Stas EZK uit te nodigen voor het overleg met de MJenV. Ambtelijk EZK wordt uitgenodigd bij de ambtelijke overleggen.

- U te informeren dat u op korte termijn een adviesnota ontvangt over het mogelijke vervolgproces – MCEV, formatie e.d. – voor het wetsvoorstel 5G en interceptie van OTT-communicatiediensten.

2 Aanleiding, gevraagde actie(s) en advies

In totaal hebben 75 partijen de oproep ondertekend. Dit zijn te veel partijen om het gesprek mee aan te gaan, daarom wordt een verdeling voorgesteld. Het voorstel is om twee gesprekken te voeren op ambtelijk niveau en één gesprek met de MJenV en Stas EZK.

De ondertekenaars zijn te verdelen in vier categorieën: het bedrijfsleven, wetenschap, het maatschappelijk middenveld en cybersecurity experts. Bij u aan tafel wordt vanuit elke categorie één vertegenwoordiger uitgenodigd. Het voorstel is om vanuit het bedrijfsleven Facebook als vertegenwoordiger uit te nodigen. Voor cybersecurity kan 10.2.e worden uitgenodigd (hij was tevens aanwezig bij het gesprek in februari 2020 met 10.2.e). Vanuit het maatschappelijk middenveld kan Bits of Freedom worden uitgenodigd als mede-initiator van de oproep, en vanuit de wetenschap 10.2.e (lid Cybersecurityraad). Daarbovenop wordt voorgesteld om ook de branchevereniging NLdigital, als mede-initiator van de oproep, bij u aan de tafel uit te nodigen. Vanuit de behoeftestellers (OM, politie, IenV diensten) zal ook een vertegenwoordiger worden uitgenodigd.

Deze personen worden ook bij de ambtelijke overleggen uitgenodigd, maar daar zal het totaal waar het gesprek mee wordt gevoerd komen op 21 partijen. Het ambtelijk gesprek kan worden gevoerd met afdelingshoofden en beleidsambtenaren.

Het voornemen is om een eerste ambtelijk overleg te plannen in de eerste week van april (afhankelijk van de voortgang van deze nota en ruimte in de agenda's). Het gesprek met de MJenV en de Stas EZK kan in de daaropvolgende week plaatsvinden en het laatste ambtelijk overleg in de week erna. EZK zal ook hieraan deelnemen, gelet op de verantwoordelijkheid voor communicatieverkeer en de Telecomwet.

3 Toelichting op het advies

De insteek van de gesprekken is primair om de zorgen uit het veld aan te horen, waar mogelijk te adresseren en deze mee te nemen in de besluitvorming over de invulling van het verdere traject. Secundair wordt meer toelichting gegeven bij de zorgvuldige aanpak waarin de verschillende belangen moeten worden gewaarborgd en in evenwicht worden gebracht. Op deze manier kunt u als minister uw vertrekpunt, aanpak en wenselijk einddoel schetsen. Tot slot kunnen de gesprekken worden gebruikt om met de verschillende stakeholders te bezien of er (alternatieve) technologische mogelijkheden zijn die de moeite van het verkennen waard zijn.

4 Dilemma's

Wanneer een selectie wordt gemaakt van de ondertekenaars kunnen partijen het gevoel hebben niet te worden gehoord, echter tegelijkertijd kan geen contact met 75 partijen worden onderhouden. Voor de ambtelijke gesprekken is gekozen voor een groep belangen die (op andere beleidsterreinen) al regelmatig contact hebben met de overheid. Zie hiervoor de bijlage.

Ook is overwogen om eerst de ambtelijke gesprekken af te wachten voor het gesprek met de bewindspersonen te plannen, maar hierdoor komt het gesprek op bewindspersonenniveau verder in de toekomst te liggen, terwijl de toezegging was om deze maand (maart) met hen in gesprek te gaan. Daarnaast kan het beeld ontstaan dat men niet wordt uitgenodigd bij de bewindspersonen vanwege hun houding in het ambtelijke gesprek.

5 Politieke en bestuurlijke context

Het gesprek met de belanghebbenden is een voorwaarde voor het vervolg van het traject voor de aftapbaarheid van OTT-communicatiediensten en de rechtmatige

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

Datum
19 maart 2021

Ons kenmerk
3270470

toegang tot versleuteld bewijs. Dit is een politiek gevoelig traject en op bestuurlijk vlak raakt dit vele belangen (fundamentele rechten, cybersecurity, de technologiesector, buitenlands beleid, opsporing en nationale veiligheid).

Het is noodzaak dat de gevoelde urgentie gepaard gaat met de nodige zorgvuldigheid waar de betrokken belangen zich gehoord en vertegenwoordigd voelen. Het betrekken van deze belangen komt een weloverwogen besluitvorming ten goede. In het vervolgtraject kunnen wetenschap, bedrijfsleven en behoeftezoekers periodiek worden betrokken. In dat kader is ook de Europese dimensie relevant, aangezien in de Raadsverklaring van 14 december jl. de Commissie is gevraagd samen met het bedrijfsleven en de wetenschap een inventarisatie uit te voeren naar technische mogelijkheden voor rechtmatige toegang tot versleuteld bewijs.

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

Datum
19 maart 2021

Ons kenmerk
3270470

6 Communicatie

Media-aandacht wordt verwacht indien de inhoud van de gesprekken naar buiten komt.

7 Afstemming

Met NCTV en EZK. Deze nota is tevens gedeeld met de opsporings-, inlichtingen- en veiligheidsdiensten.

8 Bijlagen

- 1) Voorstel deelnemers ambtelijke overleggen:

Er worden twee ambtelijke gesprekken gepland. Bij elk gesprek worden ongeveer 10 personen uitgenodigd. Van de eerder in deze nota genoemde categorieën zullen meerdere vertegenwoordigers per categorie worden uitgenodigd.

Tech bedrijven

- 1 Apple
- 2 Facebook (tevens bij MJenV)
- 3 Google
- 4 Microsoft
- 5 KPN
- 6 T-mobile
- 7 VodafoneZiggo
- 8 NLdigital (tevens bij MJenV, initiator oproep)
- 9 DINL (coalitie van organisaties voor een sterke digitale infrastructuur)

Cybersecurity

- 1 Cyberveilig Nederland (Belangenvereniging voor zo'n 60 bedrijven in de cybersecurity sector)
- 2 10.2.e
- 3 Fox IT

Maatschappelijk middenveld

- 1 Amnesty international
- 2 Bits of Freedom (tevens bij MJenV)
- 3 Expertisecentrum Online Kindermisbruik
- 4 10.2.e Internet Society

5 NLNet (stichting die tot doel heeft: het bevorderen van elektronische informatie-uitwisseling en al hetgeen daarmee verband houdt of daartoe bevorderlijk kan zijn.)

Wetenschap

- 1 10.2.e (CSR, 10.2.e, 10.2.g)
- 2 10.2.e (10.2.e, 10.2.g)
- 3 10.2.e (CSR, 10.2.e, 10.2.g)
- 4 10.2.e (CSR, 10.2.e, 10.2.g)

2) In aparte bijlage: Overzicht ondertekenaars oproep.

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

Datum
19 maart 2021

Ons kenmerk
3270470

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 1 april 2021 17:46
Aan: 10.2.e (Landelijk Parket); 10.2.e - BD/DRC/FO
CC: 10.2.e Landelijk Parket Rotterdam; 10.2.e (PaG Den Haag)
Onderwerp: RE: Notities sessie gisteren bij JenV

Dankjewel en bedankt voor je inbreng gister!
Fijne paas dagen.

Van: 10.2.e (Landelijk Parket)
Verzonden: donderdag 1 april 2021 15:22
Aan: 10.2.e BD/DRC/FO; 10.2.e BD/DRC/CV
CC: 10.2.e (Landelijk Parket Rotterdam); 10.2.e (PaG Den Haag)
Onderwerp: Notities sessie gisteren bij JenV

Beste 10.2.e,

Dank voor het overleg van gisteren. Het was goed om met elkaar te zitten en van gedachten te wisselen. Bijgaand mijn ruwe aantekeningen, in cursief mijn eigen opmerkingen aan het begin. Los van de brainstorm en de vergezichten, was het ook goed om kort te praten over de voortgang van het wetsvoorstel ter implementatie van de 5 functionele eisen uit de beleidsnota 5G. Kunnen we daar volgende week een apart overleg voor plannen om knopen door te hakken?

Groeten,

10.2.e

=====

1. *Kijk je naar de criminaliteitsfenomen of naar de methoden van opsporing (cybercrime, drugshandel, CTER)*
2. *Technologisch/juridisch:*
 - a. *Toegang tot digitale sporen of bewijsmateriaal*
 - b. *Versleuteling is problematisch, wat wordt er bewaard (Bewaarplicht), hoe snel kom je er bij (e-Evidence), kun je dit zelf (medewerkplichten, Modernisering Sv)*
 - c. *Data-analyse + AI/ML (Wpg, AVG, art. 8 EVRM)*
 - d. *Welke eisen worden er gesteld door rechter aan inzet van bob-middelen en de transparantie van bewijs (verdedigbaarheid, herleidbaarheid)(Art. 6 EVRM)*
 - e. *Opsporen op het internet (netwerkzoeking, hackbevoegdheid – consensus)*
3. *Maatschappelijk:*
 - a. *Verhaal vertellen over opsporing in een digitale wereld: hoe moeten wij ons werk doen? Data-analyses (zie verweren in de advocatuur)*
 - b. *Dwingt de technologie zich op en staat de wetgever er dan bij te kijken (standaardisering – strategie NL + EU)*
 - c. *Misbruik van kwetsbaarheden houdbaar in the long run?*
4. Quantum-computing en versleuteling
5. Lokalisatie van bedrijfsactiviteiten in de EU of nationaal (I&V diensten)
6. Versnippering van de markt
7. Data-analyses die voorspellend kunnen werken zodat je pro-actiever kan werken als politie
8. Welke wetgever is competent?
9. Politiek moet ook draagvlak creëren voor onze behoeftes
10. Belangen tussen politie/justitie en diensten niet altijd hetzelfde (95 vs. 5 %)
11. Held – slachtoffer – dader driehoek (I&V diensten telkens dader of slachtoffer, te weinig helden)
12. Ander narratief
13. 10.2.c

14. Effectiever gebruik van kwetsbaarheden
15. Behouden wat we nu hebben
16. Interne overeenstemming (binnen de overheid), presenteren als een dilemma
17. Digitale soevereiniteit of autonomie (10.2.a)
18. Draagvlak creëren
19. Technologie is niet neutraal, je kan technologie ontwikkelen die ook belangen van opsporing kunnen bevredigen
20. EZK kan een partner zijn
21. Niet alleen maar oude norm op nieuwe situatie, technologie en communicatie is wel veranderd & communicatiestrategie
- & rechtshulp (hostingsector reguleren, meewerkplichten private sector)
- & rechtspraak CJEU (academische literatuur)
- & innovatiewet aanpak
- Met vriendelijke groet,

10.2.e

Openbaar Ministerie
Landelijk Parket

10.2.e

@om.nl
www.om.nl

Dit bericht kan informatie bevatten die niet voor u bestemd is. Als 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. Het Openbaar Ministerie aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Openbaar Ministerie

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 Netherlands Public Prosecution Service accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Netherlands Public Prosecution Service

10.2.e - BD/DRC/FO

Onderwerp: Strategiesessie OTT e.a.
Locatie: (fysiek) JenV, Turfmarkt, zaal N36.11 (Noord-brabant zaal) Den Haag

Begin: wo 31-3-2021 12:30
Einde: wo 31-3-2021 16:00

Terugkeerpatroon: (geen)

Vergaderingsstatus: Geaccepteerd

Organisator: 10.2.e - BD/DRC/FO

Verplichte deelnemers: 10.2.e - BD/DRC/CV; 10.2.e BD/PIDS;
10.2.e @mindef.nl; 10.2.e 10.2.e
(Landelijk Parket); 10.2.e (PaG Den Haag); 10.2.e
BD/DWJZ/SSR; 10.2.e (Landelijk Parket Rotterdam);
10.2.e @belastingdienst.nl

Dag allen,

Op basis van de reacties lijkt dit de beste datum voor de strategiesessie interceptie OTT en aanpalende onderwerpen met OM, BOD, Politie, I&V diensten, PIDS en JenV. Ik heb een zaal op het ministerie gereserveerd waar we met max. 14 personen Covid-proof kunnen vergaderen.

Programma en opzet volgen nog, en daarvoor maak ik ook graag gebruik van jullie wensen en ideeën. Dit kunnen we oa dinsdag rondom het fische bespreken.

Groet,

10.2.e

Spreektekst 19 mei gesprek ondertekenaars petitie

- **Sterke encryptie is noodzakelijk in een digitale samenleving.** Dit kabinet onderstreept de noodzaak voor sterke encryptie. Goede encryptie is belangrijk voor het beveiligen van onze digitale informatie en communicatie en voor het in vrijheid uitoefenen van fundamentele rechten zoals het recht op privacy en vrijheid van meningsuiting.
- **Ik verneem ook de keerzijde van encryptie voor de opsporing,** zoals in het geval van versleuteling die de opsporing praktisch uitsluit van toegang tenzij je heimelijk binnendringt op een apparaat of dienst
- Een prangend vraagstuk daarbij is het verlies aan toegang tot communicatie van criminelen via de voor het brede publiek toegankelijk communicatiediensten. Lang niet elke crimineel communiceert alleen maar via diensten als SKY of Encrochat, denk aan:
 - Onlinehandel in drugs, wapens of andere illegale goederen.
 - De corrupte douanier of de vrachtwagenchauffeur verantwoordelijk voor het transport van drugs.
 - Grooming van kinderen wat toch voornamelijk op plekken gebeurt waar kinderen actief zijn.
- Dit zijn slechts enkele voorbeelden.
- De bredere impact van encryptie op de opsporing wordt door het WODC onderzocht.
- Ik zou graag willen **onderzoeken welke technische mogelijkheden er zijn,** en wat die betekenen voor de verschillende belangen.
- Veelbelovende oplossingsrichtingen moeten kunnen worden uitgewerkt zodat de risico's en voordelen beter in kaart kunnen worden gebracht.

- Denk bijvoorbeeld aan het voorstel van het Britse GCHQ uit 2018. Daarin worden 6 principes uitgewerkt, bijvoorbeeld:
 - Privacy en veiligheid zijn fundamenteel voor het publieke vertrouwen.
 - Opsporingsmogelijkheden moeten zich kunnen ontwikkelen naarmate de technologie voortschrijdt.
 - Rechtmatige toegang moet geen onbeperkte toegang betekenen.
- Vervolgens wordt een voorstel gedaan voor het toevoegen van de opsporing aan een chatgroep zonder dat de overige leden van de chatgroep dit (kunnen) zien.
- Belangrijk uitgangspunt bij dit idee is dat de versleuteling voor het individu of een beperkte groep mensen wordt aangepast, maar voor overige gebruikers sterk blijft.
- Vraag die bij mij rijst is hoe we die mogelijkheid om toegevoegd te worden dan zouden kunnen beschermen.
- Ik noem dit idee als voorbeeld, dit is misschien maar een van de mogelijke oplossingen.
- Als ik dit soort voorbeelden hoor zou ik graag met kundige experts bespreken wat de voor- en nadelen van dergelijke oplossingen zijn.
- Het in kaart brengen van de voor- en nadelen vind ik belangrijk, zodat er niet alleen goed geïnformeerde besluitvorming kan plaatsvinden, maar ook een onderbouwd en eerlijk publiek debat gevoerd kan worden.
- Wanneer bij voorbaat nader onderzoek uit de weg wordt gegaan doet dat geen recht aan het legitieme opsporingsbelang in deze discussie.
- Effectieve opsporing is ook in het digitale domein noodzakelijk zodat dit geen vrijhaven voor criminelen wordt.
- Een inventarisatie naar rechtmatige toegang tot versleutelde informatie wil ik niet alleen doen. Wanneer je de EU-verklaring van december leest dan staat daar ook

expliciet in dat dit in **gezamenlijkheid met het bedrijfsleven en academici** moet gebeuren.

- We zitten hier tezamen omdat jullie het volgend kabinet hebben opgeroepen om de ontwikkeling, de beschikbaarheid en de toepassing van alle vormen van encryptie te stimuleren
- Die oproep steun ik ook met volle overtuiging, als er maar ruimte blijft voor technische oplossingen om toegang in specifieke gevallen ten behoeve van de opsporing te realiseren
- Nu ik mijn standpunt met jullie heb kunnen delen hoor ik graag jullie zienswijze op dit dilemma.
- *[Overleg met genodigden]*
- Ik hoop dat dit een eerste overleg is in een proces waar periodiek de voortgang van het traject wordt besproken. En er een beroep op jullie kennis en inzichten kan worden gedaan bij de verkenning van oplossingen en het realiseren daarvan.
- Het betrekken van het bedrijfsleven en academici, maar ook het maatschappelijk middenveld, vind ik hierin belangrijk.



MJenV

nota

Voorbereiding gesprek ondertekenaars petitie sterke encryptie

1 Doel nota

Deze nota is voor het voorbereidingsoverleg van 10 mei voor het gesprek van 19 mei met ondertekenaars van de petitie voor sterke encryptie.

U wordt gevraagd akkoord te gaan op:

- de inzet/spreeklijn,
- dat het gesprek fysiek plaatsvindt,
- dat de inhoud van het gesprek naar buiten kan worden gebracht.

U wordt ook gevraagd aan te geven of u het wenselijk vindt het OM aanwezig is. Het OM reageerde terughoudend, omdat de insteek van het gesprek het overbrengen van uw verhaal aan de deelnemers is, maar is aanwezig als u dat wenst.

Vanuit DRC wordt u geadviseerd om indien u de noodzaak vanuit de opsporing wilt benadrukken het OM uit te nodigen. Daarnaast vinden we het voorstelbaar dat het OM niet aanwezig hoeft te zijn indien u dit overleg wilt gebruiken om voornamelijk uw uitgangspunt toe te lichten. DRC zal u tijdens het overleg vergezellen.

De voorbereiding wordt 10 mei besproken. Indien de spreeklijn akkoord is, wordt dit uitgewerkt in een spreektekst en QenA's en verwerkt in een dossier.

2 Aanleiding, gevraagde actie(s) en advies

Het gesprek van 19 mei duurt een uur. Het doel van het overleg is om een toelichting te geven aan genodigden over het doel van de inventarisatie naar mogelijkheden voor toegang tot versleuteld bewijs en het zorgvuldige proces dat wordt uitgelopen. De genodigden zullen u wijzen op de risico's van dit traject en mogelijke alternatieven. In de bijlage staan profielen met enkele uitlatingen over encryptie en de inventarisatie.

De spreeklijn die wordt voorgesteld is als volgt:

- De opsporing is steeds meer afhankelijk van digitale informatie, echter deze data is steeds vaker standaard versleuteld waardoor de opsporing steeds vaker niet (tijdig) toegang heeft tot deze informatie. Ook kennen we een interceptiebevoegdheid die niet meer aansluit bij het gebruik van communicatiediensten van deze tijd.
- Ik ben op zoek naar mogelijkheden waarop recht kan worden gedaan aan het opsporingsbelang, het belang van cybersecurity en het belang van privacy.

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

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

Contactpersoon

10.2.e

T 10.2.e

E 10.2.e @minjenv.nl

Datum

5 mei 2021

Projectnaam

encryptie OTT

Ons kenmerk

3320939

- Ik wil een geïnformeerde besluitvorming over de mogelijkheden om deze drie belangen te combineren en daarom onderzoeken we welke oplossingen dit mogelijk maken om vervolgens de risico's en de voordelen af te wegen.
- Dat kan ik niet alleen. Er is een Europees traject geïnitieerd waar ik een actieve rol in wil spelen. Daarnaast moeten de betrokken belangen hier goed bij betrokken worden zodat elke invalshoek wordt gehoord.

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

Datum
5 mei 2021

Ons kenmerk
3320939

Genodigden zijn:

- 10.2.e, 10.2.g [redacted] NLdigital),
- 10.2.e (Facebook, 10.2.e [redacted])
- 10.2.e (Bits of Freedom, 10.2.e [redacted] en
- 10.2.e (Hunt & Hackett, cybersecurity).

Dit politieke overleg wordt opgevolgd door een aantal gesprekken op ambtelijk niveau. Tevens heeft de Cybersecurityraad aangegeven dit onderwerp op ambtelijk niveau op 17 juni te willen bespreken.

3 Toelichting op het advies

Het overleg van 19 mei geeft private partners vanuit het bedrijfsleven, het maatschappelijk middenveld en academici een stoel aan de tafel. Dit is een natuurlijk moment in de inventarisatie aangezien tot nu toe voornamelijk is ingezet op het internationale/Europese netwerk en samenwerking. Het Europees traject gaat nu van start gaat en de ambitie bestaat om meer concreet te zoeken naar 'proofs of concept'.

Alle deelnemers zijn of vertegenwoordigen prominente spelers in het maatschappelijke debat over encryptie en hebben kennis van zaken over encryptie en privacy. 10.2.e is onderdeel geweest van de Toetsingscommissie inzet bevoegdheden van de WIV (de TIB) en 10.2.e is onderdeel geweest van de Evaluatiecommissie WIV 2017. Deze deelnemers hebben daarmee ook expertise in het werk van de IenV-diensten.

Gegeven deze achtergrond is het advies de deelnemers mee te geven dat het bij voorbaat uitsluiten van het opsporingsbelang in de encryptie discussie een weloverwogen besluitvorming niet ten goede komt. De gevoelde urgentie in de opsporing is daarvoor te groot. Voor het zorgvuldig afwegen van de belangen is een inventarisatie van mogelijke oplossingen nodig om de gunstige effecten voor de opsporing af te zetten tegen de gevreesde effecten die vanuit de hoek van cybersecurity en privacy worden vernomen. Twee belangen waar u als minister ook verantwoordelijkheid voor draagt.

Verschillende trajecten die nu lopen zijn: het WODC onderzoek naar de impact van encryptie op de opsporing, het Europese traject en het uitwerken van mogelijkheden om tot een 'proof of concept' te komen. Het WODC onderzoek is uitgezet onder offranten die kunnen reageren op de opdracht. Het Europese traject is afhankelijk van een plan van de Commissie. Voor het 'proof of concept' verwijs ik naar de andere nota die u voor het overleg over de 'way forward' op dit dossier ontvangt, dit staat ook gepland op 19 mei.

De oproep aan het nieuwe kabinet welke de genodigden hebben ondertekend luidt: "Wij roepen het volgende kabinet op de ontwikkeling, de beschikbaarheid en de toepassing van alle vormen van encryptie te stimuleren."

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

4 Dilemma's

N.v.t.

Datum
5 mei 2021

5 Politieke en bestuurlijke context

De deelnemers hebben aangegeven dat zij wensen dat dit overleg een 'publiek karakter' heeft, dat wil zeggen dat ze over de inhoud van het gesprek willen kunnen schrijven/twitteren/bloggen.

Ons kenmerk
3320939

6 Communicatie

De voorbereiding wordt gedeeld met DCOM.

7 Afstemming

De nota is gedeeld met de NCTV, de opzet is concept-gedeeld met EZK.

8 Bijlagen

a) Mogelijke vragen (antwoorden worden op dit moment opgesteld en afgestemd)

- Waarom is een inventarisatie nodig?
- Er zijn toch voldoende alternatieven?
- Is de minister zich bewust van het effect van zijn wens op repressieve regimes?
- Weet de minister de voordelen van encryptie, ook voor de opsporing en nationale veiligheid?
- Heeft de minister zicht op concrete oplossingen?
- Waarom wacht u het WODC onderzoek naar effecten van encryptie op de opsporing niet af?
- Waarom wacht u de evaluatie van CCIII niet af?
- Welke rol gaat u spelen in het Europese traject?
- Hoe houdt ons betrokken in het aankomende traject?
- Criminelen behouden toch altijd toegang tot encryptie?

b) Profielen

10.2.e, 10.2.g

[Redacted content]

10.2.e, 10.2.g

[Redacted content]

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

Datum
5 mei 2021

Ons kenmerk
3320939

10.2.e, 10.2.g

[Redacted content]

10.2.e, 10.2.g

[Redacted content]

Datum
5 mei 2021

Ons kenmerk
3320939

10.2.e, 10.2.g

10.2.e, 10.2.g

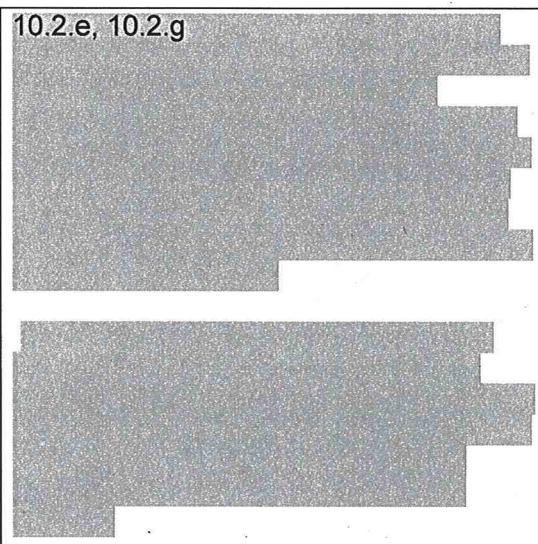
10.2.e, 10.2.g

10.2.e, 10.2.g

10.2.e, 10.2.g

10.2.e, 10.2.g

10.2.e, 10.2.g



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

Datum
5 mei 2021

Ons kenmerk
3320939



MJenV

nota

Voorbereiding gesprek ondertekenaars petitie sterke encryptie

Datum: 19 mei, 13:30-14:30

Locatie: WEBEX

Deelnemers:

10.2.e, 10.2.g NLdigital
10.2.e, 10.2.g
10.2.e, 10.2.g Facebook
10.2.e, 10.2.g Bits of Freedom
10.2.e, 10.2.g Hunt and Hackett
10.2.e, 10.2.g Officier van justitie 10.2.e, 10.2.g
10.2.e, 10.2.g Directie Bestuursondersteuning
10.2.e, 10.2.g voorlichting
10.2.e, 10.2.g Criminaliteit en Veiligheid,
Directie Rechtshandhaving en Criminaliteitsbestrijding
10.2.e, 10.2.g cybercrime

In dit dossier:

- Spreektekst
- QenA
- Kabinetsstandpunt encryptie 2016
- Raadsresolutie encryptie Europese Commissie
- Kamerbrief Raadsresolutie encryptie Europese Commissie
- Brief aftappen OTT-diensten van maart 2020

Spreeklijn:

De spreeklijn die wordt voorgesteld is als volgt:

- Het kabinet onderstreept het belang van sterke encryptie.
- We kunnen onze ogen niet sluiten voor de schaduwzijde voor de opsporing: i) De opsporing is steeds meer afhankelijk van digitale informatie, echter deze data is steeds vaker standaard versleuteld, ii) we kennen een interceptiebevoegdheid die niet meer aansluit bij het gebruik van communicatiediensten van deze tijd.
- Ik ben op zoek naar mogelijkheden waarop recht kan worden gedaan aan het opsporingsbelang, het belang van cybersecurity en het belang van privacy.

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

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

Contactpersoon

10.2.e

T 10.2.e

E 10.2.e @minjenv.nl

Datum

5 mei 2021

Projectnaam

encryptie OTT

Ons kenmerk

3320939

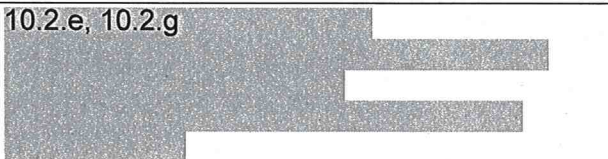
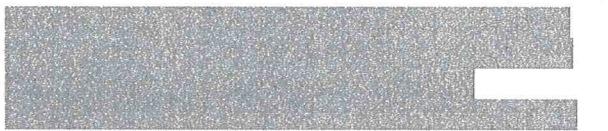
- Veelbelovende technische oplossingen moeten kunnen worden onderzocht. Bijvoorbeeld het voorstel van GCHQ. Ik moedig het presenteren van dergelijke oplossingen aan, zodat deze kunnen worden geanalyseerd op mogelijke voor- en nadelen.
- Vervolgens vindt geïnformeerde besluitvorming plaats waar de risico's en voordelen worden afgewogen en wordt gezien of de verschillende zwaarwegende belangen kunnen worden gecombineerd.
- Dat kan ik niet alleen. Er is een Europees traject geïnitieerd waar ik een actieve rol in wil spelen. Daarnaast moeten de betrokken belangen hier goed bij betrokken worden zodat elke invalshoek wordt gehoord.

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

Datum
5 mei 2021

Ons kenmerk
3320939

Introductie genodigden:

10.2.e, 10.2.g 	10.2.e, 10.2.g 
	
	
	
	

10.2.e, 10.2.g

10.2.e, 10.2.g

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

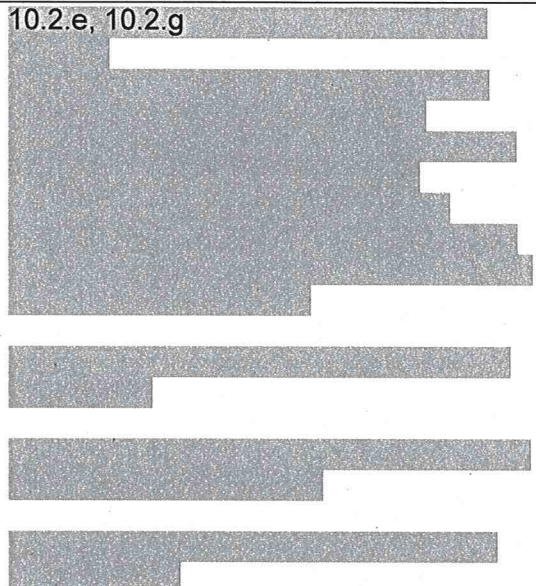
Datum
5 mei 2021

Ons kenmerk
3320939

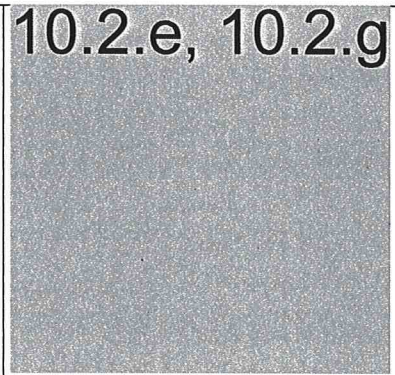
10.2.e, 10.2.g

10.2.e, 10.2.g

10.2.e, 10.2.g

A large rectangular area of the document is redacted with a grey stippled pattern. The redaction covers the majority of the left column of the first table.

10.2.e, 10.2.g

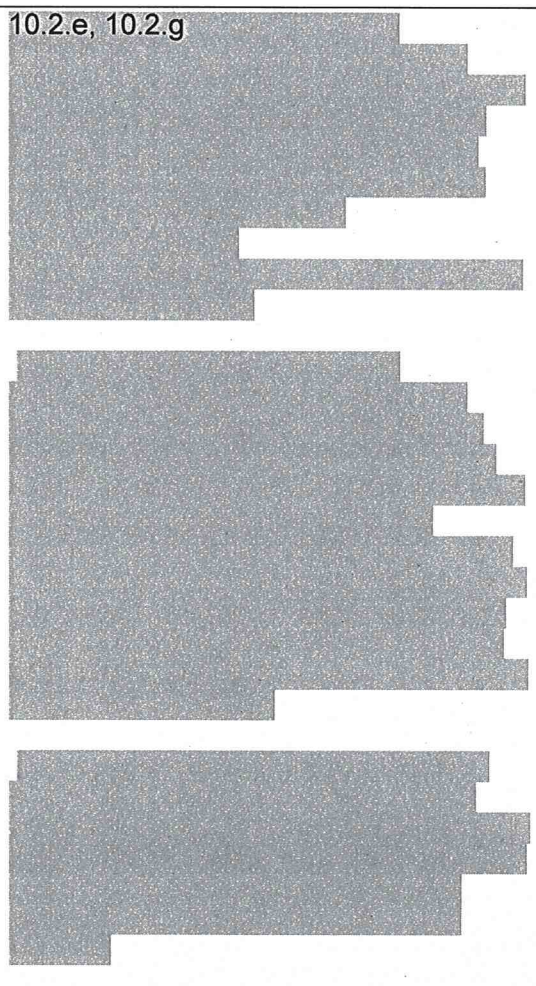
A rectangular area of the document is redacted with a grey stippled pattern, covering the top half of the right column of the first table.

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

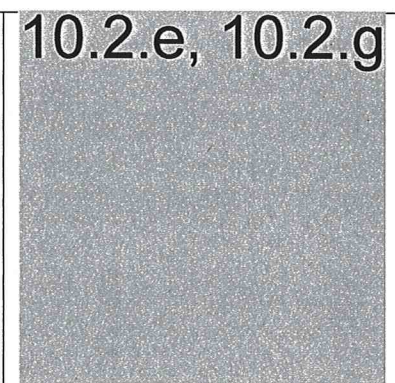
Datum
5 mei 2021

Ons kenmerk
3320939

10.2.e, 10.2.g

A large rectangular area of the document is redacted with a grey stippled pattern. The redaction covers the majority of the left column of the second table.

10.2.e, 10.2.g

A rectangular area of the document is redacted with a grey stippled pattern, covering the top half of the right column of the second table.

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

Datum
5 mei 2021

Ons kenmerk
3320939

10.2.e

BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: woensdag 12 mei 2021 15:36
Aan: Secretariaat - Minister van Justitie en Veiligheid; Directiesecretariaat - DRC
Onderwerp: 17 mei 15:00-15:30 "way forward" op encryptie
Bijlagen: Projectplan inventarisatie rechtmatige toegang versleuteld bewijs.docx;
Spreektekst 19 mei gesprek ondertekenaars petitie.docx; QenA.docx

Beste 10.2.e

Hierbij de stukken voor maandag 17 mei het gesprek over de 'way forward'.

Zouden jullie deze in IBABS willen plaatsen?

Alvast bedankt.

Met vriendelijke groet,

10.2.e

10.2.e

@minvenj.nl

10.2.e

BD/DRC/FO

Onderwerp: Encryptie: opsporing en nationale veiligheid
Locatie: WEBEX

Begin: ma 17-5-2021 10:00
Einde: ma 17-5-2021 11:00

Terugkeerpatroon: (geen)

Vergaderingsstatus: Organisator van vergadering

Organisator:

Verplichte deelnemers:

10.2.e - BD/DRC/CV
10.2.e (PaG Den Haag) 10.2.e @om.nl;
10.2.e @om.nl; 10.2.e @om.nl; 10.2.e - BD/PIDS;
10.2.e @politie.nl; 10.2.e
10.2.e @politie.nl; 10.2.e f@mindef.nl; 10.2.e
10.2.e @belastingdienst.nl; 10.2.e BD/DRC/FO;
10.2.e @politie.nl; 10.2.e 10.2.e (DBS);
10.2.e (DBS)

Beste collega's,

Het lijkt mij goed om weer even bij elkaar te komen. Ik zal ook vanmiddag een reeks starten zodat er wat meer duidelijkheid is in de agenda's. Volgens mij was dit ook een puntje dat wij nog op moesten pakken nav ons vorige overleg...

Ik stel de volgende agenda voor:

- Europese traject
- Vooruitblik multinationalaal overleg 18 mei
- Vooruitblik gesprek MJenV en ondertekenaars oproep voor sterke encryptie 19 mei & ambtelijke overleggen
- Projectplan rechtmatige toegang tot versleutelde informatie (en capaciteit/inzet), waaronder proof of concept/Horizon Europe

Als jullie nog punten hebben hoor ik ze graag!

@10.2.e als 10.2.e hier bij wilt zijn kunnen jullie dan de vergadering doorsturen? Ik heb z'n email niet.

Groeten,

10.2.e

-- De volgende tekst niet verwijderen of wijzigen. --

Wanneer het tijd is, kunt u hier deelnemen aan uw Rijksvideo Vergadering.

Vergaderingsnummer (toegangscode): 10.2.e, 10.2.g

Wachtwoord voor vergadering: 10.2.e, 10.2.g

Deelnemen aan vergadering

Tik om deel te nemen vanaf een mobiel apparaat (alleen deelnemers)

10.2.e, 10.2.g

Deelnemen via telefoon

10.2.e, 10.2.g

Algemene inbelnummers

Deelnemen via een videosysteem of -toepassing

Kies 10.2.e, 10.2.g

kiezen en uw vergaderingnummer invoeren.

Deelnemen met Microsoft Lync of Microsoft Skype voor Bedrijven

Kies 10.2.e, 10.2.g

Als u een host bent, klik dan hier om hostgegevens weer te geven.

Hebt u hulp nodig? Ga naar <http://help.webex.com>

10.2.e

- BD/DRC/FO

Van:

10.2.e - BD/DRC/CV

Verzonden:

woensdag 12 mei 2021 09:21

Aan:

10.2.e (PaG Den Haag) 10.2.e @om.nl);
10.2.e @om.nl; 10.2.e s@om.nl; 10.2.e
10.2.e @politie.nl; 10.2.e
@politie.nl; 10.2.e @mindef.nl; 10.2.e
@belastingdienst.nl; 10.2.e - BD/DRC/FO;
10.2.e @politie.nl; 10.2.e (DBS);
10.2.e (DBS)

Onderwerp:

RE: Encryptie: opsporing en nationale veiligheid

Bijlagen:

Preparation for multilateral meeting.docx; Todo schema encryptie 20210407.docx

Hallo collega's,

Ter voorbereiding van maandag deel ik wat extra informatie:

-Europese traject: Terugkoppeling gesprek met de Europese Commissie en vooruitblik

-Vooruitblik multinationalaal overleg 18 mei: zie bijgevoegd stuk voor verdere informatie. Voor maandag is het denk ik goed om te bespreken waar na 18 mei behoefte aan is? VK deed dit voorstel van opeenvolgende sessies:
Session 2: Technical experts seminar (opportunity for briefing from UK technical expert - 10.2.e - followed by discussion among participants)

Session 3: Law enforcement seminar (discussion among law enforcement leads of current experience, impact of platforms moving to end-to-end encryption, powers and limits, collaboration, mitigation)

Session 4: Policy and operational leads' seminar (opportunity for law enforcement leads to question and discuss issues with government policy officials and, possibly, technical experts).

-Vooruitblik gesprek MJenV en ondertekenaars oproep voor sterke encryptie 19 mei & ambtelijke overleggen:

Het advies is om deze spreeklijn aan te houden:

-uitgangspunt kabinet: sterke encryptie voor het beveiligen van communicatie en het in vrijheid uitoefenen van fundamentele rechten.

-voorbeelden van waar de opsporing tegen aanloopt: online handel in illegale goederen, drugshandel en grooming.

-veelbelovende technische oplossingen willen we onderzoeken, voorbeeld GCHQ. Voordelen afwegen tov de nadelen.

-Forward looking, inclusief traject, gekoppeld aan het EU-traject: in gezamenlijkheid met bedrijfsleven, academici en maatschappelijk middenveld.

Deelnemers kan worden meegegeven dat het bij voorbaat uitsluiten van het opsporingsbelang in de encryptie discussie een weloverwogen besluitvorming niet ten goede komt. De gevoelde urgentie in de opsporing is daarvoor te groot. Voor het zorgvuldig afwegen van de belangen is een inventarisatie van mogelijke oplossingen nodig. Op deze manier kunnen de gunstige effecten voor de opsporing worden afgezet tegen de gevreesde effecten die vanuit de hoek van cybersecurity en privacy worden vernomen. Twee belangen waar u als minister ook verantwoordelijkheid voor draagt.

-Projectplan rechtmatige toegang tot versleutelde informatie (en capaciteit/inzet), waaronder proof of concept/Horizon Europe: zie bijgevoegd concept-projectplan ter informatie en de stukken die eerder door bureau PIDS zijn verspreid. Relevante onderwerpen zijn het fiche, het 'proof of concept', en de actieve informatievoorziening.

Met vriendelijke groet,

10.2.e

M 10.2.e

inveni.nl

Identiek aan E.022

Identiek aan E.022