

Tel.: 10.2.e
Fax: 10.2.e
Mailto: 10.2.e@bnetza.de
<http://www.bundesnetzagentur.de>

-----Ursprüngliche Nachricht-----

Von: 10.2.e - BD/DRC/CV [mailto:10.2.e@minjenv.nl]
Gesendet: Montag, 28. Oktober 2019 09:29
An: IS16a
Cc: 10.2.e - BD/PIDS
Betreff: RE: EECC aankomende vrijdag

Dear 10.2.e,

The discussion on interception and OTT is moving a bit more quickly here than anticipated. Would you be able to provide some insight in the approach taken in possible legislation regarding this topic and a possible basis in the EECC? If it is more preferable that I contact a colleague in the Ministry of Interior Affairs or the Ministry of Justice, could you provide me with a contact?

Thank you very much 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

10.2.e@minvenj.nl <mailto:10.2.e@minvenj.nl> www.government.nl/venj
<<http://www.government.nl/venj>>

.....
Van: 10.2.e - BD/DRC/CV
Verzonden: dinsdag 15 oktober 2019 20:43
Aan: 10.2.e@BNetzA.de
CC: 10.2.e - BD/PIDS <10.2.e@minjenv.nl>

Onderwerp: RE: EECC aankomende vrijdag

Dear 10.2.e ,

My name is 10.2.e 10.2.e in The Netherlands. One of my portfolio's is 'interception'. Our ministry of Economic Affairs is currently implementing the EECC, without the possibility to send OTT's an interception order. 10.2.e has told me that Germany is currently implementing the EECC including an obligation for OTT's to answer to orders of law enforcement for interception. We are really keen to learn more about how this obligation is worded, what is required of the OTT's and what article in EECC this obligation is based on. Also in light of the encryption debate and whether it would require OTT's to provide decrypted information.

I am sorry if I am over-asking you. However, we have been told that the EECC does not cover possibilities for law enforcement. After some scrutiny of the text we learned that it was possible for member states to intercept communications of number dependent OTT's (SkypeOut), however we haven't found the base for intercepting communications of all OTT's. Currently Economic Affairs is finalizing the consultation process of the implementation legislation after which it will be sent to our parliamentary body fairly quickly. At which point we have no more possibilities to influence the legislative process.

Thank you very much in advance for your help.

Yours sincerely,

10.2.e
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
10.2.e @minvenj.nl <mailto:10.2.e @minvenj.nl> www.government.nl/venj
<http://www.government.nl/venj>

.....

Van: 10.2.e - BD/PIDS 10.2.e @minjenv.nl>
Verzonden: dinsdag 15 oktober 2019 17:02
Aan: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>
CC: R10.2.e @BNetzA.de
Onderwerp: RE: EECC aankomende vrijdag

Hello 10.2.e ,

You can contact 10.2.e on the implementation of the EECC and interception obligations for OTT in Germany (see the CC).

Regards,

10.2.e

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e <10.2.e@justice.gouv.fr>
Verzonden: maandag 28 oktober 2019 14:02
Aan: 10.2.e - BD/DRC/CV; 10.2.e
CC: 10.2.e; 10.2.e; 10.2.e @minbuza.nl
Onderwerp: RE: Interception and OTT

10.2.a & 10.2.e

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

De: 10.2.e - BD/DRC/CV
Envoyé : lundi 28 octobre 2019 10:08
À: 10.2.e; 10.2.e
Cc: 10.2.e; 10.2.e; 10.2.e @minbuza.nl
Objet : Interception and OTT

Dear 10.2.e,

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

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

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

Thank you in advance for your response.

Bien cordialement.

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

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

Ministerie van Justitie en Veiligheid

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

Ministry of Justice and Security

10.2.e - BD/DRC/FO

Van: 10.2.e <10.2.e@homeoffice.gov.uk>
Verzonden: vrijdag 28 februari 2020 12:34
Aan: 10.2.e - BD/DRC/CV
CC: 10.2.e ; 10.2.e 10.2.e
Onderwerp: RE: Facebook end-to-end encryption
Bijlagen: 2020.02.28_International Encryption Statement_V6.docx

10.2.a & 10.2.e

From: 10.2.e - BD/DRC/CV
Sent: 28 February 2020 11:11
To: 10.2.e
Cc: 10.2.e ; 10.2.e ; 10.2.e
Subject: RE: Facebook end-to-end encryption

10.2.e

You also asked me the time we will be heading back, departure time on Monday is 19:45 from Heathrow. I hope that fits with the schedule. Again many thanks for receiving us next Monday.

Have a good weekend.

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

.....

Van: 10.2.e
Verzonden: donderdag 27 februari 2020 11:30
Aan: 10.2.e - BD/DRC/CV
Cc: 10.2.e
Onderwerp: RE: Facebook end-to-end encryption

10.2.e

10.2.a, 10.2.e

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Encryption 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

From: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Sent: 24 February 2020 17:11
To: 10.2.e <10.2.e@fco.gov.uk>
Cc: 10.2.e@minbuza.nl
Subject: RE: Facebook end-to-end encryption

Dear 10.2.e,

That sounds great, thank you. We will make travel arrangements immediately. We aim to arrive on Heathrow around 08:00 am.

Kind regards,

10.2.e

Van: 10.2.e 10.2.e@fco.gov.uk>
Verzonden: vrijdag 21 februari 2020 10:01
Aan: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Onderwerp: RE: Facebook end-to-end encryption

10.2.e

10.2.a & 10.2.e

10.2.e Foreign and Security Policy | The Hague
British Embassy | Lange Voorhout 10 | 2514 ED | The Hague | The Netherlands

10.2.g@fco.gov.uk

UK in the Netherlands: [GOV.UK](https://www.gov.uk) | [Facebook](https://www.facebook.com/ukintheNetherlands) | [Twitter](https://twitter.com/ukintheNetherlands) | [LinkedIn](https://www.linkedin.com/company/ukintheNetherlands)



From: 10.2.e - BD/DRC/CV 10.2.e@minjenv.nl>
Sent: 18 February 2020 13:13
To: 10.2.e <10.2.e@fco.gov.uk>
Subject: RE: Facebook end-to-end encryption

Dear 10.2.e,

I am sorry, I forgot to mention the main reason for traveling. I want to underline that lawful access to encrypted data is still very much at the core of our visit. We would just like to learn more on the UK approach to the other issues as well.

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
.....

Van: 10.2.e - BD/DRC/CV
Verzonden: dinsdag 18 februari 2020 13:06
Aan: 10.2.e <10.2.e@fco.gov.uk>
cc: 10.2.e (Sensitive) <10.2.e@fco.gov.uk>; 10.2.e - BD/DEIA/EU
<10.2.e@minjenv.nl>; 10.2.e @minbuza.nl; 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Onderwerp: RE: Facebook end-to-end encryption

Dear 10.2.e,

Thank you for your email and the offer to visit The Hague. However, 10.2.e and I would like to visit our counterparts in London and take the opportunity to discuss a broader array of issues. Would that be possible? Ideally we would combine the visit with the following discussions:

- interception of OTT-services
- bad-hosting, the hosting of illegal content in datacentre's
- consequences of 5G for law enforcement (for example the negative effect on our interception capacity)

I hope this doesn't demand too much of your time or the time of your colleagues in London.

10.2.e and I would be able to visit London either on the 28th of February or the 2nd of March. Is that convenient for our counterparts?

Thank you again very much for your efforts to liaise between us.

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

.....

Van: 10.2.e <10.2.e@fco.gov.uk>
Verzonden: vrijdag 14 februari 2020 16:36
Aan: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>; 10.2.e - BD/DRC/CV
10.2.e @minjenv.nl
cc: 10.2.e <10.2.e@fco.gov.uk>; 10.2.e - BD/DEIA/EU
10.2.e @minjenv.nl
Onderwerp: RE: Facebook end-to-end encryption

10.2.a & 10.2.e

[REDACTED]

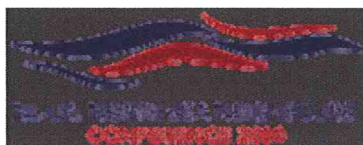
[REDACTED]

[REDACTED]

[REDACTED]

10.2.e Foreign and Security Policy | The Hague
British Embassy | Lange Voorhout 10 | 2514 ED | The Hague | The Netherlands
10.2.e | 10.2.e @fco.gov.uk

UK in the Netherlands: GOV.UK | [Facebook](https://www.facebook.com/GOV.UK) | [Twitter](https://twitter.com/GOV_UK) | [LinkedIn](https://www.linkedin.com/company/GOV.UK)



From: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Sent: 12 February 2020 15:34
To: 10.2.e <10.2.e@fco.gov.uk>; 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Cc: 10.2.e 10.2.e @fco.gov.uk; 10.2.e - BD/DEIA/EU
10.2.e @minjenv.nl
Subject: RE: Facebook end-to-end encryption

Dear 10.2.e

Thank you very much for the information and the initiative to formulate a statement on this issue. I very much look forward to the upcoming draft.

Furthermore, we would gladly accept your invitation to discuss this issue in more detail with the Home Office. We are currently forming an itinerary to visit several capitals and discuss the issue of lawful access more in-depth. Shall I come back to you with a more concrete proposal regarding possible dates?

Yours sincerely,

10.2.e

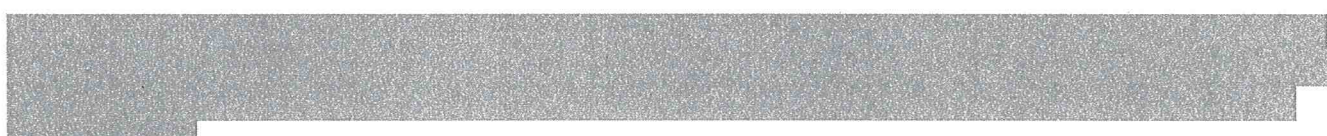
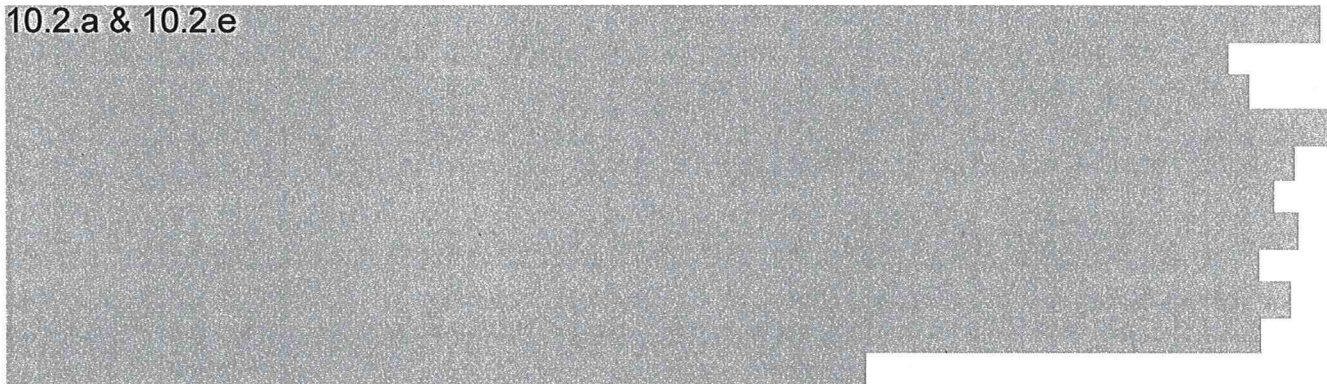
.....
Ministry of Justice and Security
Law Enforcement Department
Cybercrime unit
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands
P.O. Box 20301 | 2500 EH | The Hague | The Netherlands
.....

M10.2.e
@minvenj.nl
www.government.nl/venj
.....

Van: 10.2.e <10.2.e@fco.gov.uk>
Verzonden: woensdag 12 februari 2020 15:06
Aan: 10.2.e <10.2.e@minjenv.nl>; 10.2.e - BD/DRC/CV
<10.2.e@minjenv.nl>
CC: 10.2.e <10.2.e@fco.gov.uk>
Onderwerp: Facebook end-to-end encryption

10.2.a & 10.2.e

10.2.a & 10.2.e



10.2.e, Foreign and Security Policy | The Hague
British Embassy | Lange Voorhout 10 | 2514 ED | The Hague | The Netherlands

10.2.e | 10.2.e @fco.gov.uk

UK in the Netherlands: [GOV.UK](https://www.gov.uk) | [Facebook](#) | [Twitter](#) | [LinkedIn](#)

This email is intended for the addressee(s) only. All messages sent and received by the Foreign & Commonwealth Office may be monitored in line with relevant [UK legislation](#)

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

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 has been scanned by the Symantec Email Security.cloud service.
For more information please visit <http://www.symanteccloud.com>

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 has been scanned by the Symantec Email Security.cloud service.
For more information please visit <http://www.symanteccloud.com>

10.2.e - BD/DRC/FO

Van: 10.2.e <10.2.e@homeoffice.gov.uk>
Verzonden: donderdag 9 juli 2020 12:41
Aan: 10.2.e - BD/DRC/CV
CC: 10.2.e - BD/DEIA/EU; 10.2.e BD/DRC/CV; 10.2.e (OSCT); 10.2.e (Sensitive); 10.2.e - BD/DRC/CV; 10.2.e@minbuza.nl;
OSCTEncryptionPolicy
Onderwerp: RE: Encryption statement

Hi 10.2.e

10.2.a

10.2.e

10.2.e

Encryption and Online Safety,
Investigatory Powers Unit,
Office for Security and Counter Terrorism

Home Office

2 Marsham Street, London, SW1P 4DF

T: 10.2.e 72

E: 10.2.e@homeoffice.gov.uk

From: 10.2.e - BD/DRC/CV

Sent: 07 July 2020 16:41

To: 10.2.e

Cc: 10.2.e - BD/DEIA/EU; 10.2.e - BD/DRC/CV; 10.2.e (FCO); 10.2.e; 10.2.e; 10.2.e (OSCT); 10.2.e (Sensitive); 10.2.e - BD/DRC/CV;

10.2.e@minbuza.nl

Subject: RE: Encryption statement

Dear 10.2.e,

Thank you again for inviting us to join the statement. Addressing the need for lawful access to encrypted data is a priority in the Ministry and will remain to be so in the foreseeable future.

However, I regret to inform you that The Netherlands will not be able to join the statement at this time. I thank you for your patience and commend you for your efforts in the past few months. I hope that we can keep in touch on possible developments in our pursuits to find acceptable solutions.

I will be on holiday until the 21st of July, we could discuss the issue over the phone after that date.

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

Van 10.2.e
Verzonden: maandag 22 juni 2020 17:20
Aan: 10.2.e - BD/DRC/CV
cc: 10.2.e BD/DEIA/EU ; 10.2.e - BD/DRC/CV ; 10.2.e ; 10.2.e ; 10.2.e
10.2.e ; 10.2.e (OSCT) ; 10.2.e (Sensitive)
Onderwerp: RE: Encryption statement

Hi 10.2.e

10.2.a, 10.2.g

• 10.2.a

10.2.a

10.2.e

10.2.e

Encryption 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

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

Sent: 15 June 2020 16:13

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

Cc: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>; 10.2.e . - BD/DRC/CV <10.2.e @minjenv.nl>

Subject: Encryption statement

Hello 10.2.e

I hope you are doing well. I heard your Permanent Secretary and my Secretary-General had an introductory meeting in which the encryption statement also came up. If I understood correctly you are finishing up a new draft based on the suggestions made by Germany. Do you have an idea on when you can share a new draft?

Kind regards,

10.2.e

Met vriendelijke groet,

10.2.e

M 10.2.e

10.2.e @minjenv.nl

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

Ministerie van Justitie en Veiligheid

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 has been scanned by the Symantec Email Security.cloud service.
For more information please visit <http://www.symanteccloud.com>

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 has been scanned by the Symantec Email Security.cloud service.
For more information please visit <http://www.symanteccloud.com>

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: vrijdag 18 september 2020 14:32
Aan: 10.2.e @bmi.bund.de
Onderwerp: RE: Paper CIE - COSI

Dear 10.2.e

Thank you very much! I see that your paper is circulated now, thank you for that. 10.2.a



Thank you very much for the possibility to propose two questions! Thank you for considering these questions. If I do not see them back in the upcoming document, no worries ☺.

-1. In what kind of criminal investigations do you experience a considerable negative impact because of encryption (eg. Drugs, terrorism, fraude, moneylondering, computercrimes, CSA, criminal investigations on the whole)?

→ I would propose this question to solidify claims that decisions in the development in new technologies affect safety in the 'real world'.

-2a. How would you describe the impact of encryption in these criminal investigations? (access to evidence is restricted, delayed or impossible in its entirety)

-2b. In circumstances when access to evidence was delayed, what are examples of existing investigatory powers that were used to effectively obtain the evidence?

→ A question to check whether alternative existing powers are effective.

A big compliment of all your work in preparation of COSI! I hope you have a relaxing 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
10.2.e @minvenj.nl
www.government.nl/venj
.....

Van: 10.2.e @bmi.bund.de
Verzonden: vrijdag 18 september 2020 10:23

Aan: 10.2.e - BD/DRC/CV
Onderwerp: AW: Paper CIE - COSI

10.2.a & 10.2.e

10.2.a

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

Von: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>
Gesendet: Donnerstag, 17. September 2020 15:50
An: 10.2.e <10.2.e @bmi.bund.de>
Betreff: Paper CIE - COSI

Hello 10.2.e

For your eyes only, this is a summary of the input that I circulated for interdepartmental consultation. By the way, I have only received the CTC paper for COSI. The input below regards the CIE paper.

Essence:

We recognize the problem. We support the research into technical solutions together with ISP's. We urge not to exclude possibilities beforehand in order to adequately assess the impact of the solutions on fundamental rights and secure communications, and balance this impact against the advantages of law enforcement.

NL is 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. This is based on the available solutions in 2016 and the assessment of the negative- en positive consequences of encryption. It is to be encouraged that we research way's into which we can ease the negative consequences for law enforcement whilst the positive characteristics of encryption like fundamental rights and safe communications are sufficiently uphold.

We do think that the focus on E2EE is somewhat premature. We would like to hear the reasoning behind this. The different applications of encryption as mentioned by the CTC may require different solutions.

We support te initiative to formulate a statement on this subject from the Council.

As you know, after interdepartmental consultations the input may vary.

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
.....

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

Voor een veilige en rechtvaardige samenleving
.....

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: donderdag 15 oktober 2020 11:31
Aan: 10.2.e; 10.2.e @bmi.bund.de; 10.2.e
Onderwerp: Sovereignty and ISP's

Dear colleagues,

You might have heard about the non-paper of France and The Netherlands to regulate the tech industry in order to improve competition.

In the coverage in the Financial Times I read the comment of mr. O that his regulation is also important from a sovereignty point of view. I feel that this is also relevant in our discussions.

We have stressed the importance that ISP's take into consideration the offline consequences of their decisions in the development of technologies. I feel that this also touches on the sovereignty principle. In our countries we are faced with the effects of policies that are made in a boardroom in Silicon Valley, without public debate or democratic control. Those decisions are a 'fait accompli' with real life consequences in how we can protect the rule of law and public order.

I just wanted to share this thought with you.

<https://www.ft.com/content/4a9ed79e-c8c8-4b47-8055-1cd029541c32>

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

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: dinsdag 27 oktober 2020 18:34
Aan: 10.2.e @bmi.bund.de
Onderwerp: Encryption Vedome 30 October

Hello 10.2.e

I hope everything is well. We are finalizing our comments on the statement you circulated.

Are you aware of the 'Vendome group'? it is a group of ministers from the founding countries of the EU. Amongst which NL en GER of course.

On the 30th of October there will be an emergency Vendome group because of the murder of the French teacher by an islamist radical.

Three topics are on the agenda: Terrorist Content Online, E-evidence and Hate speech. I plan to advise my minister to bring up the issue of lawfull access to encryption under the bullet of E-evidence and voice support of the initiative of the German Presidency.

During this Vendome group also Commissioners Reynders, Johannsson and Breton will be present and the chairwomen of the LIBE-committee of the European Parliament.

I thought this might be good to know for you.

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

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: maandag 2 november 2020 11:20
Aan: 10.2.e BD/DRC/GC; 10.2.e - BD/DRC/FO; 10.2.e BD/DRC/GC; 10.2.e - BD/DRC
CC: 10.2.e - BD/DCOM/WS&O; 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
Onderwerp: FW: Extra meeting of the Vendôme Group - 30 Octobre
Bijlagen: CP - Groupe Vendôme.pdf; Draft Declaration (english) Version consolidée.docx

Ter informatie de uitkomsten van de Vendome groep van vrijdag.

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>
Datum: vrijdag 30 okt. 2020 7:53 PM
Aan: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV
10.2.e @minjenv.nl, 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>, 10.2.e - BD/PNI
10.2.e @nctv.minjenv.nl, 10.2.e - BD/DEIA/PVEU-NAVO <10.2.e @minjenv.nl>,
10.2.e @minbuza.nl <10.2.e @minbuza.nl>, 10.2.e - BD/PACT
10.2.e @nctv.minjenv.nl
Kopie: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e - BD/DEIA/EU
10.2.e @minjenv.nl, 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>, 10.2.e
- BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e @minbuza.nl <10.2.e @minbuza.nl>,
10.2.e - BD/DEIA <10.2.e @minjenv.nl>
Onderwerp: RE: Extra meeting of the Vendôme Group - 30 Octobre

Beste mensen,
De Vendome groupe is goed verlopen. Dank voor al jullie snelle en goede bijdragen. Zie bijgaand de persberichten
Heel goed weekend
Groet 10.2.e

<https://www.rijksoverheid.nl/actueel/nieuws/2020/10/30/grapperhaus-terreurdaden-frankrijk-vragen-alertheid-in-heel-europa>

Van: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>
Datum: vrijdag 30 okt. 2020 9:28 AM
Aan: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>, 10.2.e - BD/DRC/CV
<10.2.e @minjenv.nl>, 10.2.e - BD/PNI 10.2.e @nctv.minjenv.nl, 10.2.e -
BD/DEIA/PVEU-NAVO 10.2.e @minjenv.nl, 10.2.e @minbuza.nl 10.2.e @minbuza.nl, 10.2.e
Van de - BD/PACT <10.2.e @nctv.minjenv.nl>
Kopie: 10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e - BD/DEIA/EU
10.2.e @minjenv.nl, 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl, 10.2.e
10.2.e - BD/DEIA/EU <10.2.e @minjenv.nl>, 10.2.e - BD/DEIA/EU 10.2.e @minjenv.nl, 10.2.e
@minbuza.nl <10.2.e @minbuza.nl>

Onderwerp: FW: Extra meeting of the Vendôme Group - 30 Octobre

Beste mensen, bijgaand de aangepaste versie n.a.v. aanslag Nice gisteren. Met groet 10.2.e

Van: 10.2.e <10.2.e@justice.gouv.fr>

Datum: donderdag 29 okt. 2020 6:17 PM

Aan: 10.2.e 10.2.e @mjusticia.es>, 10.2.e 10.2.e @mj.etat.lu>, 10.2.e BD/DEIA/EU 10.2.e @minjenv.nl>, 10.2.e @bmjv.bund.de 10.2.e @bmjv.bund.de>, 10.2.e @just.fgov.be <10.2.e@just.fgov.be>, 10.2.e <10.2.e@giustizia.it>, 10.2.e @ec.europa.eu <10.2.e@ec.europa.eu>, 10.2.e @ec.europa.eu <10.2.e@ec.europa.eu> 10.2.e @ec.europa.eu <10.2.e@ec.europa.eu>, 10.2.e @europarl.europa.eu>

Kopie: 10.2.e <10.2.e@justice.gouv.fr>, 10.2.e 10.2.e @justice.gouv.fr>, 10.2.e <10.2.e@justice.gouv.fr>, 10.2.e 10.2.e @justice.gouv.fr>, 10.2.e <10.2.e@justice.gouv.fr>, 10.2.e @bmjv.bund.de <10.2.e@bmjv.bund.de>, 10.2.e @diplomatie.gouv.fr>, 10.2.e <10.2.e@mjusticia.es>, 10.2.e @giustizia.it>, 10.2.e <10.2.e@diplomatie.gouv.fr>, 10.2.e @sgae.gouv.fr>, 10.2.e @diplomatie.gouv.fr <10.2.e@diplomatie.gouv.fr>, 10.2.e @diplomatie.gouv.fr <10.2.e@diplomatie.gouv.fr>, 10.2.e @diplomatie.gouv.fr <10.2.e@diplomatie.gouv.fr>, 10.2.e @diplomatie.gouv.fr <10.2.e@diplomatie.gouv.fr>, CAB/DIPLOMATIQUE/SECRETARIAT <10.2.e@justice.gouv.fr>, 10.2.e 10.2.e @justice.gouv.fr>

Onderwerp: RE: Extra meeting of the Vendôme Group - 30 Octobre

Dear colleagues

10.2.a

10.2.e

De: 10.2.e

Envoyé : mercredi 28 octobre 2020 17:05

À: 10.2.e <10.2.e@mjusticia.es>, 10.2.e <10.2.e@mjusticia.es>, 10.2.e @mj.etat.lu>; 10.2.e @minjenv.nl' 10.2.e @minjenv.nl>; 10.2.e @bmjv.bund.de' 10.2.e @bmjv.bund.de>; 10.2.e @just.fgov.be' 10.2.e @just.fgov.be>; 10.2.e '10.2.e @giustizia.it>; 10.2.e @ec.europa.eu' <10.2.e@ec.europa.eu>; 10.2.e @ec.europa.eu' 10.2.e @ec.europa.eu' <10.2.e@ec.europa.eu>; 10.2.e @europarl.europa.eu> Cc: 10.2.e 10.2.e @justice.gouv.fr>; 10.2.e 10.2.e @justice.gouv.fr>; 10.2.e @justice.gouv.fr>; 10.2.e @justice.gouv.fr>; 10.2.e @bmjv.bund.de' <10.2.e@bmjv.bund.de>; 10.2.e @diplomatie.gouv.fr>; 10.2.e <10.2.e@mjusticia.es>; 10.2.e @giustizia.it>; 10.2.e <10.2.e@diplomatie.gouv.fr>; 10.2.e

<10.2.e @sgae.gouv.fr>; 10.2.e @diplomatie.gouv.fr' 10.2.e
@diplomatie.gouv.fr>; 10.2.e @diplomatie.gouv.fr' <10.2.e @diplomatie.gouv.fr>;
10.2.e @diplomatie.gouv.fr' 10.2.e @diplomatie.gouv.fr>; 10.2.e @diplomatie.gouv.fr'
<a 10.2.e @diplomatie.gouv.fr>; CAB/DIPLOMATIQUE/SECRETARIAT 10.2.e @justice.gouv.fr>;
10.2.e 10.2.e @justice.gouv.fr>

Objet : RE: Extra meeting of the Vendôme Group - 30 Octobre

10.2.a

10.2.e

De : 10.2.e

Envoyé : mardi 27 octobre 2020 12:23

À : 10.2.e '10.2.e @mjusticia.es>; 10.2.e '10.2.e @mj.etat.lu>;
10.2.e @minjenv.nl' <10.2.e @minjenv.nl>; 10.2.e @bmjv.bund.de' 10.2.e @bmjv.bund.de>;
10.2.e @just.fgov.be' 10.2.e @just.fgov.be>; 10.2.e <10.2.e @giustizia.it>;
10.2.e @ec.europa.eu' 10.2.e @ec.europa.eu>; 10.2.e @ec.europa.eu'
<10.2.e @ec.europa.eu>; 10.2.e @ec.europa.eu' <10.2.e @ec.europa.eu>; 10.2.e
10.2.e ' <10.2.e @europarl.europa.eu>
cc : 10.2.e 10.2.e @justice.gouv.fr>; 10.2.e <10.2.e
10.2.e @justice.gouv.fr>; 10.2.e 10.2.e @justice.gouv.fr>; 10.2.e
10.2.e n@justice.gouv.fr>; 10.2.e <10.2.e @justice.gouv.fr>; 10.2.e
10.2.e @justice.gouv.fr>; 10.2.e @bmjv.bund.de' 10.2.e @bmjv.bund.de>; 10.2.e
10.2.e @diplomatie.gouv.fr>; 10.2.e ' <10.2.e @mjusticia.es>; 10.2.e
10.2.e @giustizia.it>; 10.2.e '10.2.e @diplomatie.gouv.fr>; 10.2.e
10.2.e @sgae.gouv.fr>; 10.2.e @diplomatie.gouv.fr>;
10.2.e @diplomatie.gouv.fr>; 10.2.e @diplomatie.gouv.fr>; 10.2.e @diplomatie.gouv.fr>;
CAB/DIPLOMATIQUE/SECRETARIAT 10.2.e @justice.gouv.fr>

Objet : Extra meeting of the Vendôme Group - 30 Octobre

Dear All,

10.2.a

10.2.e

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 26 november 2020 17:08
Aan: 10.2.e @bmi.bund.de
Onderwerp: RE: Encryption declaration

Hello 10.2.e

Thank you for your quick reply. Your acceptance of our suggestions is greatly appreciated!

I totally share your points on the follow-up of the resolution. The follow-up should be expeditious and ambitious. I gladly cooperate with you on that. 10.2.a

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

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 10.2.e @minjenv.nl>
Gesendet: Montag, 23. November 2020 10:32
An: 10.2.e <10.2.e @bmi.bund.de>
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

.....
M 10.2.e
10.2.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

Van: 10.2.e @bmi.bund.de
Verzonden: woensdag 16 december 2020 17:42
Aan: 10.2.e BD/DRC/CV
Onderwerp: AW: Council resolution

10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV
Gesendet: Montag, 14. Dezember 2020 16:38
An: 10.2.e
Betreff: Council resolution

Dear 10.2.e

I see that the resolution has been published since 10 am this morning. Congratulations! A balanced resolution on lawful access to encrypted data negotiated in 4 months in the Council is an impressive achievement.

I wish you a lot of rest, happy holidays and a good New Year despite the lock down. Let's catch up in 2021 on the way forward.

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

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 29 januari 2021 14:47

Aan:

10.2.e @bmi.bund.de'

Onderwerp:

Encryption follow-up

Dear 10.2.e

I hope you are doing well! I thought it might be a good time to catch-up and talk about the upcoming process after the council resolution. For example, this week we spoke with the Commission on their ideas about the resolution. It might also be a good idea to invite our perm. rep. colleagues from Brussels. Also, in The Netherlands the question of lawful access to encrypted data becomes increasingly pressing because of the possible interception of OTT's. Colleagues of mine have sent out a questionnaire and a colleague of yours was very kind to answer our questions. In addition to our colleagues from Brussels we could also ask the interception colleagues to join. Would you be in favour of that? The name from BMI that I see is: 10.2.a, 10.2.e

Have a good weekend and I look forward to speaking with you again.

Mit freundlichen Grüßen,

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

10.2.e @minvenj.nl

www.government.nl/venj
.....

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: donderdag 25 februari 2021 18:00
Aan: 10.2.e @bmi.bund.de
CC: 10.2.e - BD/DRC/FO
Onderwerp: RE: NDL TelKo hier: link
Bijlagen: NL paper - roaming statement EU_20201204.docx; CCIII.pdf

Dear 10.2.e

Thank you very much, also to 10.2.e ! And likewise, always a pleasure!

Please find attached the paper that 10.2.e was talking about which he will present upcoming Monday.

Attached you find the law (ComputerCrime III), it actually arranges a wide range of issues. The articles that deal with covert intrusion are: 126nba (regular crime), 126uba (organized crime), 126zpa (terrorism), and I already sent you the article that deals with zero days (126ffa). If you want a translation of 126nba, please let me know. I can run it through Google Translate and review if they have the nuances right. No trouble at all. As regards to the three different articles, different types of crime have different levels of suspicion on which basis you can use investigatory powers.

This is the link with the whole legislative procedure, but it is quite hard to navigate if you do not speak dutch: [Eerste Kamer der Staten-Generaal - Computercriminaliteit III \(34.372\)](#).

If there is anything else you need please let me know.

Met vriendelijke groet,

10.2.e

M 10.2.e
10.2.e @minvenl.nl

Van: 10.2.e @bmi.bund.de
Verzonden: donderdag 25 februari 2021 15:58
Aan: 10.2.e - BD/DRC/CV
Onderwerp: WG: NDL TelKo hier: link

10.2.e

10.2.a

10.2.e

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: vrijdag 12 maart 2021 11:45
Aan: 10.2.e @bmi.bund.de
Onderwerp: RE: Lawful access

Hi 10.2.e

That would be very nice. In the morning, somewhere between 09:00-11:00?

Kind regards,

10.2.e

Van: 10.2.e @bmi.bund.de
Verzonden: vrijdag 12 maart 2021 08:50
Aan: 10.2.e - BD/DRC/CV
Onderwerp: AW: Lawful access

10.2.e

10.2.a

10.2.e

Von: 10.2.e - BD/DRC/CV 10.2.e @minjenv.nl>
Gesendet: Donnerstag, 11. März 2021 10:45
An: 10.2.e <10.2.e @bmi.bund.de>
Cc: 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>
Betreff: Lawful access

Dear 10.2.e

Recently our work in intercepting OTT-services was met with a coalition of civil society, academia en tech companies criticizing the initiative and calling on a new cabinet to support strong encryption.

10.2.a

My apologies if I am too curious, but have your conversations in Brussels last week been fruitful? Also in contacts with our experts the 2018 initiative of GCHQ ([https://www.lawfareblog.com/...](https://www.lawfareblog.com/)) was mentioned, just letting you know we have reached out to our British colleagues for some more background on this initiative and the backlash it received at the time.

Always happy to call.

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/...>)
.....

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 14 april 2021 09:14
Aan: 10.2.e @bmi.bund.de'
Onderwerp: RE: Lawfull access to encrypted data
Bijlagen: 2021.02 Proposition for 10.2.g - an alternative approach NOT HMG POLICY.pdf

Thank you 10.2.e

I will start setting up the meeting. Please find the paper attached and the disclaimer the British sent with it. Please share the document to a limited number.

During the meeting last week, we also talked about a paper that has been written here setting out first steps towards a way for 10.2.g to provide access to content within a broadly end-to-end encrypted environment. We said we would share it with you; I have attached it – please forgive me for pointing out the following necessary caveats:

- This is not a statement of UK Government policy.
- Please do not share this beyond government officials and advisers.
- It is designed to outline at a high level a potential approach, and thus begin a discussion with 10.2.g

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

Van: 10.2.e @bmi.bund.de
Verzonden: woensdag 14 april 2021 07:52
Aan: 10.2.e - BD/DRC/CV
Onderwerp: WG: Lawfull access to encrypted data

10.2.e

10.2.a

10.2.a

Von: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>
Gesendet: Montag, 5. April 2021 16:42
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

We have had a good conversation with the British colleagues. Have you received the 10.2.g paper already from them?

I plan to propose a stock-taking meeting in the first week of May and invite Germany, UK, US(FBI) and Portugal. The UK reportedly had good conversations with the French. I must say that I haven't that contact with France since our last trilateral meeting, but they are welcome to join.

If you agree with this approach I shall send the email below to the UK and propose a meeting. The attendees should be (senior) policyadvisors and technical colleagues.

Of course I'm happy to talk about setting-up this meeting during a call if necessary.

Dear 10.2.e

Thank you very much for sharing the paper and the names of the German colleagues. We have discussed the issue with Germany before. The paper shall be treated with great confidentiality. Regarding the stock-taking meeting we wanted to keep the circle close at this point and limit the meeting to partners with whom we discussed this issue previously, for us that would be the UK, Germany and the FBI. If I remember correctly you also had conversations with French colleagues right? Would it be possible to provide me with their contact details? In addition we talked about the possibility of inviting the occupant of Councils' Presidency (Portugal) for the European dimension. Do you agree with this approach?

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: donderdag 1 april 2021 22:29
Aan: 10.2.e - BD/DRC/CV <10.2.e@minjenv.nl>

cc: 10.2.e - BD/DRC/FO 10.2.e @minienv.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.e

10.2.a, 10.2.e, 10.2.g

10.2.e

10.2.e
10.2.e Encryption Policy Team
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/...>)
[@ukhomeoffice](https://twitter.com/ukhomeoffice) (<https://twitter.com/...>)



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

Sent: 17 March 2021 15:28

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

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

Subject: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

10.2.e

10.2.e

Investigatory Powers Unit

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

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

Subject: RE: Lawfull access to encrypted data

Hi 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

10.2.e @minvenj.nl

Van: 10.2.e <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
<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>

Onderwerp: RE: Lawfull access to encrypted data

10.2.e

10.2.a

10.2.e

10.2.e

Investigatory Powers Unit

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 in the 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.e

10.2.a, 10.2.e

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

10.2.e

From: 10.2.e - BD/DRC/CV

Sent: 17 December 2020 10:17

To: 10.2.e ; 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 ; 10.2.e
Onderwerp: Contacts

10.2.e

10.2.a

10.2.e

10.2.e
Encryption 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

Van: 10.2.e - BD/DRC/CV
Aan: 10.2.e @bmi.bund.de
Onderwerp: RE: Question
Datum: donderdag 22 april 2021 09:44:22
Bijlagen: RE Lawfull access to encrypted data.msg

Hi 10.2.e

Unfortunately, we tried to obtain such an insight when the E-evidence regulation was published, but such information was not available... There is only the transparency reports by the companies themselves. I can arrange some information on the types of data and how we can obtain it, that comes from our procedural law.

Regarding the call, did you want to join the possible call with the UK tomorrow? I haven't heard a confirmation from 10.2.e yet. I will see if I can get in touch with him today and set a time... You and me have a call planned Tuesday next week (which we could also do tomorrow by the way).

Kind regards,

10.2.e

Met vriendelijke groet,

10.2.e

M 10.2.e

@minventi.nl

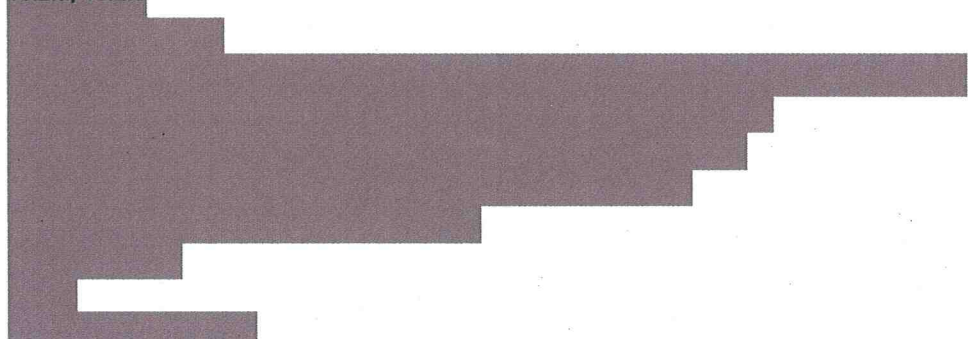
Van: 10.2.e @bmi.bund.de

Verzonden: donderdag 22 april 2021 07:09

Aan: 10.2.e - BD/DRC/CV

Onderwerp: Question

10.2.a, 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

Van: 10.2.e - BD/DRC/CV
Aan: 10.2.e
Cc: 10.2.e - BD/DRC/FO; 10.2.e; 10.2.e (OSCT); 10.2.e @minbuza.nl; 10.2.e
10.2.e 10.2.e
Onderwerp: RE: Lawfull access to encrypted data
Datum: dinsdag 20 april 2021 15:24:44
Bijlagen: image001.jpg

Dear 10.2.e

Thank you very much for this detailed proposal, it looks very promising. At this moment I would propose to take it one step at the time. I think the different sessions that you propose benefit greatly if policy, technical experts and operational leads participate jointly. This would take longer, but we hopefully get more out of the meetings. Also during the process needs or goals might develop or change. With a more prolonged process we can be more adaptable.

I propose we set a meeting in the beginning of May where the agenda is largely in line with Session 1: latest developments, goals, future sessions and opportunities for multilateral action.

Of course I am happy to discuss this on Friday, but wanted to let you know my thoughts in advance. Are you comfortable enough with this approach that I can go ahead with setting a date and we can discuss further details upcoming Friday?

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
.....

Van: 10.2.e

Verzonden: dinsdag 20 april 2021 10:39

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

cc: 10.2.e - BD/DRC/FO; 10.2.e; 10.2.e (OSCT); 10.2.e

(Sensitive); 10.2.e (Sensitive); 10.2.e (Sensitive)

Onderwerp: RE: Lawfull access to encrypted data

10.2.a, 10.2.e

[Large redacted block]

• 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

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

From: 10.2.e - BD/DRC/CV <10.2.e@minienv.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@minienv.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
10.2.e @minjenv.nl
www.government.nl/venj

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@minjenv.nl>

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>

Onderwerp: RE: Lawfull access to encrypted data

10.2.e

10.2.a, 10.2.e

[REDACTED]

10.2.e

Encryption Policy Team
National Security Directorate
Home Office
2 Marsham Street, London SW1P 4DF

T: 10.2.e
M: 10.2.e
[@ukhomeoffice](http://www.gov.uk/home-office)
C218F56A



From: 10.2.e 10.2.e @homeoffice.gov.uk>
Sent: 17 March 2021 15:28
To: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>; 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>
Cc: 10.2.e - BD/DRC/FO <10.2.e @minjenv.nl>
Subject: RE: Lawfull access to encrypted data
10.2.a, 10.2.e

10.2.e
Investigatory Powers Unit
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 <10.2.e @homeoffice.gov.uk>; 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>
Cc: 10.2.e - BD/DRC/FO 10.2.e @minjenv.nl>
Subject: RE: Lawfull access to encrypted data
Hi 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
10.2.e @minjenv.nl
Van: 10.2.e 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
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>
Onderwerp: RE: Lawfull access to encrypted data
10.2.e
10.2.a

10.2.a

10.2.e

10.2.e

Investigatory Powers Unit

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 in the 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

10.2.e @minvenj.nl

www.government.nl/venj
.....

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.e

10.2.a, 10.2.e

10.2.e

From: 10.2.e - BD/DRC/CV

Sent: 17 December 2020 10:17

To: 10.2.e ; 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

10.2.e @minvenj.nl

www.government.nl/venj

Van: 10.2.e

Verzonden: donderdag 15 oktober 2020 15:30

Aan: 10.2.e BD/DRC/CV

cc: 10.2.e ; 10.2.e

Onderwerp: Contacts

10.2.e

10.2.a, 10.2.e

[Redacted text block]

10.2.e

[Redacted text block]

[Redacted] Encryption 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.

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: vrijdag 23 april 2021 10:37
Aan: 10.2.e @bmi.bund.de'
Onderwerp: Data sources 2015 Manhattan District Attorney's office
Bijlagen: Literatuuronderzoek.pdf; 11.18.15 Report on Smartphone Encryption and Public Safety.pdf

Hi 10.2.e

I thought the table on p. 7 of the '11.18.15 Report on Smartphone Encryption' might be interesting to you. In my concept-literature study there are other statistics, mainly from the US, which might be helpful. Please disregard the text in the study, it is a concept that was never finalized.

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
.....

Inhoudsopgave

1. Inleiding	2
2. Ontwikkelingen	3
2.1 Digitale revolutie	3
2.1.1 Toename van het belang van digitaal bewijs	3
2.1.2 Toename van de dreiging	4
2.1.3 Toename van versleuteling, beter versleuteld en vaker standaard	4
2.2 Internationale dimensie	5
2.3 Conclusie voor de criminaliteitsbestrijding	6
3. De problematiek van de criminaliteitsbestrijding nader toegelicht	6
3.1 Aftappen	7
3.2 Opgeslagen data: The golden age of surveillance	8
3.3 Kinderporno	11
3.4 Conclusie	11
4. Oplossingen	12
4.1 Reguleren encryptietechnologie	13
4.2 Rekenkracht van de opsporing	14
4.3 Samenwerking met een derde partij 'Vendor Unlock'	15
4.4 Alternatieven	16
5. Afweging	19
6. Conclusie	20
Literatuurlijst	21

Concept

1. Inleiding

Beleidsstukken over encryptie beginnen traditioneel met het onderschrijven van het belang van encryptie voor de bescherming van data, cybersecurity, privacy van personen en vertrouwelijkheid van communicatie. Vervolgens wordt uiteengezet hoe criminelen deze bescherming misbruiken en opsporingsonderzoeken frustreren of in het geheel onmogelijk maken. Beide belangen zijn zwaarwegend en legitiem. Het debat is al jaren oud en wordt gekenmerkt door zijn paradoxale karakter, encryptie zou niet structureel moeten worden verzwakt, maar om de problematiek in de opsporing op te lossen wordt aangegeven dat verzwakking nodig is. Voor het doorbreken van deze cirkel zijn twee vragen te stellen: 1) Is de problematiek bij de opsporing en Inlichtingen en Veiligheidsdiensten dermate dat het op terreinen het verzwakken van encryptie legitimeert, en 2) is er een manier waarop rechtmatige toegang kan worden verkregen zonder encryptie structureel te verzwakken?

In 2016 heeft het toenmalige kabinet dit paradoxale karakter verwoord in een kabinetsstandpunt dat het: “op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland”.¹ Tegelijkertijd wordt in het standpunt de noodzaak voor rechtmatige toegang tot gegevens en communicatie onderstreept. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld.² Er is overleg nodig met aanbieders van ICT-producten en –diensten over effectieve gegevens verstrekking bij gebruik van hun diensten door kwaadwillenden.³

Toegang tot versleutelde data wordt in het maatschappelijk debat snel een ‘achterdeur’ genoemd. Een achterdeur houdt in dat men heimelijk en ongebreidelde toegang krijgt door data.⁴ Waar de opsporing naar zoekt is versleuteling waarbij de gegevens herstelbaar zijn en gepaard gaat met het benodigde toezicht.⁵ Er wordt ook wel gesproken over ‘uitzonderlijke toegang’, het is uitzonderlijk omdat de inzet gericht is, andere gebruikers zouden niet noemenswaardig moeten worden geraakt, de inzet is niet veel voorkomend wanneer met het vergelijkt op de schaal van het totaal aantal apparaten en communicatie op een platform.⁶

Hieronder leest men de uitkomsten van een literatuuronderzoek met een breed scala aan opties, van achterdeur tot herstelbare encryptie tot alternatieven. De focus van het onderzoek ligt specifiek op de mogelijkheden tot rechtmatige toegang, het is geen uitputtende appreciatie van het nut van encryptie of de dreiging die daaruit voortkomt voor de opsporing. De waarde van encryptie voor cybersecurity, de digitale economie en burgerlijke vrijheden wordt onderschreven, maar is geen onderdeel van dit onderzoek. Voor een uitvoerige studie naar de rol van encryptie in deze belangen zijn er in veelvoud, er kan bijvoorbeeld worden verwezen naar ‘Shining a light on the encryption debate: a Canadian field guide.’⁷ Of lees voor de noodzaak van sterke encryptie voor mensenrechten het rapport van Special Rapporteur on freedom of expression⁸ of het vervolgrapport⁹. Naast de

¹ Kamerstukken 2015/16, 26 649, nr. 383, p.4

² Kamerstukken 2015/16, 26 649, nr. 383, p. 3

³ Kamerstukken 2015/16, 26 649, nr. 383, p.4

⁴ Lewis et al 2017, p. 3

⁵ Lewis et al 2017, p. 3

⁶ Levy & Robinson 2018

⁷ Gill et al 2018

⁸ Kaye 2015

⁹ United Nations 2018

Concept

aanbeveling om wetgeving aan te nemen die encryptie beschermd, is een van de aanbevelingen die de rapporteur doet:

48. Laws should be established or amended to specify clearly that restrictions on encryption and anonymity tools, including government hacking measures, are permitted only in exceptional circumstances; i.e. when they satisfy the requirements of legality, necessity and proportionality, and legitimacy of objective. Government authorities should refrain from relying on generic or antiquated laws to justify restrictions on encryption and anonymity tools that do not satisfy these criteria.

50. When proposing restrictions on encryption and anonymity tools, States should engage in a meaningful and transparent consultations with a representative cross-section of civil society, corporations, the general public, and relevant stakeholders concerning the appropriate scope of those restrictions.

In hoofdstuk 5 wordt verder ingegaan op mogelijke afwegingen bij mogelijke regelgeving omtrent de rechtmatige toegang tot versleutelde data. Dit literatuuronderzoek beoogt een bescheiden bijdrage te leveren aan de inventarisatie naar de legitimiteit van dergelijke regelgeving.

2. Ontwikkelingen

2.1 Digitale revolutie

Het paradoxale karakter van het nut van encryptie en de negatieve effecten ervan wordt versterkt door de steeds grotere afhankelijkheid van technologische processen en digitale systemen. Des te meer technologie een centraal onderdeel vormt van ons persoonlijk leven en de maatschappelijke ontwikkeling, des te groter de behoefte aan beveiligende maatregelen. Tegelijkertijd is de negatieve impact des te groter bij de opsporing- en inlichtingen en veiligheidsdiensten.

2.1.1 Toename van het belang van digitaal bewijs

Een eerste gevolg van de digitale revolutie is de toename van elektronische gegevens, of in stafzaken: elektronisch bewijs.¹⁰ Er wordt steeds meer digitaal gecommuniceerd en opgeslagen, hierdoor heeft digitale informatie een steeds belangrijkere rol in opsporingsonderzoeken¹¹, terwijl tegelijkertijd steeds meer informatie buiten het bereik van de publieke autoriteiten valt doordat deze informatie steeds beter wordt beveiligd. Ter illustratie, het aantal Nederlandse gebruikers van WhatsApp, een populaire vorm van digitale communicatie, is in december 2014 gegroeid tot 10 miljoen.¹² In 2017 is voorspeld dat in de komende jaren 'Instant Messaging' door WhatsApp, Facebook Messenger, iMessage, Telegram, Skype en anderen uitgroeit tot 63% van het wereldwijde berichtenverkeer in daarop volgende komende jaren, met een toename van rond de 20% per jaar na 2019. Wereldwijd maken 1.5 miljard individuen gebruik van end-to-end encrypted Instant Messagingapps.¹³

¹⁰ Congressional Research Service 2016, p. 3 en 4

¹¹ Kamerstukken 2017/18, 22 112, nr. 2593, p. 13

¹² European Commission 2016, p. 40

¹³ Lewis et al 2017, p. 6, 8

Concept

2.1.2 Toename van de dreiging

Een tweede gevolg van de digitale revolutie is de centrale rol van technologie en dat het domein steeds aantrekkelijker wordt voor kwaadwillende actoren. De schaalvoordelen die de digitale revolutie biedt gelden ook voor criminelen. Beroepscriminelen en statelijke actoren vormen al enkele jaren de grootste dreiging voor de veiligheid in de digitale wereld. Bovendien richten zij de meeste schade aan.¹⁴ Beroepscriminelen richten zich onder andere op private organisaties en burgers met het oog op de diefstal van gegevens die vervolgens kunnen worden doorverkocht of gepubliceerd.¹⁵ In 2016 had 20 procent van de bedrijven met 10 of meer werknemers te maken met de gevolgen van een cyberaanval.¹⁶ Daarnaast was 1 op de 9 personen in 2017 slachtoffer van cybercrime.¹⁷ Daarbovenop is via *cybercrime-as-a-service*, een omvangrijke cybercriminele dienstensector, geen hoogwaardige technologische expertise vereist voor digitale criminele activiteiten.¹⁸ Deze grotere dreiging kan zowel pleiten voor de noodzaak voor betere beveiliging, als voor de noodzaak voor rechtmatige toegang voor de opsporing. De Korpschef heeft in de jaarverantwoording 2018 van de Nationale Politie benoemd dat naar verwachting de helft van alle strafzaken een link heeft met cybercriminaliteit.¹⁹ Dat betekent dat steeds meer wordt verwacht van de opsporings- en IenV diensten in het digitale domein.

2.1.3 Toename van versleuteling, beter versleuteld en vaker standaard

Een derde gevolg van de digitale revolutie is de technologische afhankelijkheid en de roep om betere bescherming. Consumentenbescherming en privacywaarborgen worden steeds meer een competitief voordeel van technologiebedrijven. De maatregelen die bedrijven vervolgens nemen leiden ertoe dat steeds meer bevelen vanuit de opsporing voor informatie steeds vaker ineffectief worden.²⁰ Informatiesystemen en software zijn dikwijls standaard ingesteld op versleutelde vormen van communicatie.²¹ Deze standaardinstellingen worden door de gebruikers vrijwel nooit gewijzigd, waardoor zij – dikwijls zonder dat zelf te weten of na te streven – steeds beter zijn beveiligd tegen het aftappen en opnemen van hun communicatie.²² In het verlengde hiervan ligt de verbetering van encryptie.²³ Bedrijven hebben hun inzet geïntensiveerd om data zwaar te versleutelen, zowel op servers als wanneer data wordt gewisseld tussen servers.²⁴ In beginsel zou deze ontwikkeling moeten worden ondersteund vanuit de overheid. Encryptie beoogt de betrouwbaarheid van (vertrouwelijke) communicatie te beschermen door de boodschap te versleutelen. Tegelijkertijd is het in toenemende mate voor bedrijven zelf onmogelijk om toegang te krijgen tot deze data.²⁵ Het resultaat is dat een derde partij die deze informatie opvraagt een onleesbare brij van letters, cijfers en tekens krijgt en de boodschap slechts kan ontcijferen met een sleutel. Traditioneel wordt de sleutel gegenereerd door een communicatie- of netwerkaanbieder en wordt deze verstrekt aan de gebruiker. Men kan zich voorstellen dat de capaciteit om deze sleutels te dupliceren of af te vangen aantrekkelijk is voor een kwaadwillende. In het streven naar het beperken van het aantal actoren die kennis hebben van een sleutel is end-to-end encryptie ontwikkeld. Bij end-to-end encryptie wordt het bericht op device

¹⁴ Kamerstukken 2017/18, 28 684, nr. 522, p. 2

¹⁵ Cyber Security Beeld Nederland 2017

¹⁶ CBS.nl 25 september 2017

¹⁷ Veiligheidsmonitor 2017, p.10

¹⁸ Cyber Security Beeld Nederland 2019, p. 7

¹⁹ Jaarverantwoording Politie 2018, p. 15

²⁰ Shah 2015, p. 544; Lewis et al 2017, p. 3

²¹ Lewis et al 2017, p. 6

²² Kamerstukken 2015/16, 34 372. Nr. 3, p. 8; Internet Society 2017, p. 5

²³ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 12

²⁴ Shah 2015, p. 553, 554; Lewis et al 2017, p. 5, 6

²⁵ Shah 2015, p. 553, 554; Lewis et al 2017, p. 5

Concept

versleuteld op het apparaat zodra het is verstuurd. Afhankelijk van de applicatie wordt het vervolgens tijdelijk opgeslagen, bijvoorbeeld in de CLOUD, totdat de ontvanger bereikbaar is.²⁶ Het ontsleuteld aanleveren van communicatie, zoals bijvoorbeeld geldt bij de aftapverplichting, is hierdoor niet mogelijk.²⁷

2.2 Internationale dimensie

Een tweede ontwikkeling is de internationale dimensie. Nederland is niet de enige die met dit dilemma speelt. In 2016 is reeds op Europees niveau geïnventariseerd naar een Europese oplossing voor de problematiek die de opsporing ervaart door encryptie. Door middel van een enquête heeft de toenmalig Voorzitter van de Raad bij de lidstaten (25 respondenten) en Europol geïnventariseerd naar de problematiek van encryptie voor de criminaliteitsbestrijding. Daarin heeft een groot deel van de respondenten aangegeven vaak of bijna altijd een vorm van encryptie tegenkomen in strafrechtelijke onderzoeken.²⁸ Tegelijkertijd werd de noodzaak voor Europese wetgeving niet onderkend, maar werden praktische maatregelen wel aangemoedigd. Het Voorzitterschap stelde onder andere voor een reflectieproces ter zake te starten om praktische oplossingen te definiëren en de mogelijkheden te bezien om technische expertise op nationaal en Europees niveau te versterken, onder andere in samenwerking met Europol en ENISA. Nederland kon instemmen met deze aanpak.²⁹ Dit heeft geleid tot een initiatief om onder andere Europol de ontwikkelingen van encryptie voor de opsporing te monitoren.³⁰

De internationale dialoog kreeg een nieuwe impuls na het versturen van een open brief aan Facebook door de Amerikaanse, Britse en Australische ministers van justitie.³¹ De brief is een reactie op het voornemen van Facebook om Messenger end-to-end te versleutelen. De ministeres van justitie roepen Facebook op om met hen in gesprek te gaan om samen te werken aan een oplossing die werkt voor beide partijen. De Nederlandse minister van Justitie en Veiligheid heeft begrip getoond voor de zorgen die in de brief worden geuit.³² Hij heeft bij zijn bezoek aan zijn Amerikaanse collega aangegeven deze problematiek ook bij zijn Europese collega's aan te kaarten.³³ Daarnaast is hij een inventarisatie gestart naar oplossingen waarbij wordt gestreefd om binnen de kaders van het kabinetsstandpunt te blijven en recht te doen aan belangen van de opsporing en de nationale veiligheid.³⁴ Hierbij wordt tevens bezien of een internationale oplossing mogelijk is.³⁵

Verder zijn er al enkele landen met wetten die een ontsleutelmogelijkheid verplichten, zoals China, India, Brazilië, Rusland, het Verenigd Koninkrijk(VK), Frankrijk en Zuid Korea. China en Rusland hebben meerdere wetten die leveranciers van encryptieproducten onder een evaluatie-regime plaatsen en bedrijven verplichten om medewerking te verlenen aan het installeren van hard- en software om toegang tot de apparaten te krijgen. Daarnaast staan er boetes op het niet kunnen ontsleutelen van data. Rusland verplicht dienstverleners om achterdeuren te bieden en consumentencommunicatie zes maanden op te slaan.³⁶ China verplicht inzicht in de broncode en de data die in dat land wordt geproduceerd in dat land op te slaan.³⁷ Bedrijven moeten verder

²⁶ Europol 2019, p. 19

²⁷ Art. 2(e) van het Besluit Aftappen openbare netwerken en –diensten dat telecommunicatie

²⁸ Council of the European Union 2016, p. 3

²⁹ Kamerstukken 2016/17, 32 317, nr. 450, p. 9

³⁰ European Commission 2017

³¹ US Justice Department 2019

³² NOS 2019a

³³ Politico 2019

³⁴ Kamerstukken 2019/20, nr. 759, Aangangsel van de Handelingen

³⁵ Kamerstukken 2019/20, nr. 1095, Aangangsel van de Handelingen

³⁶ Lewis et al 2017, p. 19, 20

³⁷ Lewis et al 2017, p. 24

Concept

'cryptography schemes' rapporteren aan de overheid of 'technical interfaces' installeren voor de overheid.³⁸ In Frankrijk geldt voor leveranciers die zaken doen met de overheid toegang tot data te faciliteren. In het VK heeft de minister van Binnenlandse Zaken de bevoegdheid om communicatiediensten te bevelen een interceptiecapaciteit te behouden. Daarnaast kunnen decryptiebevelen worden gegeven aan iedereen in bezit van versleutelde data en de sleutels. Een bevel, een 'technical capability notice', kan worden geweigerd indien dit onredelijk kostbaar of technisch onmogelijk is.³⁹ In de VK zijn in de meeste jaren sinds inwerkingtreding minder dan tien mensen vervolgd voor het weigeren om invulling te geven aan de decryptieplicht. In de periode tussen 2008-2013 zijn tussen de één en drie personen per jaar zijn veroordeeld. Daarnaast heeft iemand in 2008 een beroep gedaan op het recht niet te mogen worden gedwongen om aan de eigen veroordeling mee te werken (het nemo-teneturbeginsel) en is in het gelijk gesteld.⁴⁰ In Frankrijk is echter geoordeeld door het Constitutioneel Hof dat er geen sprake is van het nemo-teneturbeginsel aangezien het geen bekentenis betreft, maar slechts data betreft die al ergens is opgeslagen en daardoor bestaat onafhankelijk van de wil van de verdachte.⁴¹

2.3 Conclusie voor de criminaliteitsbestrijding

Vanuit het perspectief van de criminaliteitsbestrijding kan worden geconcludeerd dat elektronisch bewijs steeds belangrijker wordt in strafzaken, de dreiging vanuit het digitale domein wordt steeds groter, en er wordt steeds meer van de digitale opsporing verwacht. Tegelijkertijd wordt de drempel om aan deze behoefte te kunnen voldoen steeds hoger. Dit komt mede omdat het (tijdig) inzicht verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten wordt bemoeilijkt, vertraagt, of onmogelijk wordt gemaakt.⁴² Om deze reden wordt vanuit de opsporing-, inlichtingen- en veiligheidsdiensten gevraagd om een betrouwbare, snelle en schaalbare toegang tot versleutelde data.⁴³

3. De problematiek van de criminaliteitsbestrijding nader toegelicht

Voor de beantwoording van de eerste onderzoeksvraag, 'Is de problematiek bij de opsporing en Inlichtingen en Veiligheidsdiensten dermate dat het op terreinen het verzwakken van encryptie legitimeert' is de impact van encryptie op aftappen, toegang tot opgeslagen data en kinderporno onderzocht. In 2018 heeft de Commissie modernisering opsporingsonderzoek in het digitale tijdperk gesignaleerd dat dataversleuteling van een laptop of harde schijf problemen oplevert bij bijvoorbeeld kinderporno en computervredebreukonderzoeken. Daarnaast vindt communicatie steeds minder in spraak en steeds meer in tekst en beelden plaats via data in transit. Tappen is daarmee in de afgelopen jaren steeds minder succesvol geworden. De commissie geeft aan dat ook onderzoeken met de hoogste prioriteit, allerlei communicatie van en naar verdachten kan plaatsvinden zonder dat de opsporingsdienst er kennis van kan nemen.⁴⁴

De reactie vanuit Nederland op bovengenoemde enquête vanuit de Raad van de Europese Unie inzake encryptie en criminaliteitsbestrijding is in november 2016 naar de Kamer verstuurd.⁴⁵ In het antwoord geeft Nederland aan dat de encryptieproblematiek per zaak afhankelijk is, maar dat in zaken naar cybercrime, kinderporno of georganiseerde misdaad in bijna elke zaak een vorm van

³⁸ Lewis et al 2017, p. 20

³⁹ Lewis et al 2017, p. 20, 21, Walden, 2018, p. 903

⁴⁰ Koops & Kosta 2018, p. 895

⁴¹ Koops & Kosta 2018, p. 895

⁴² Kamerstukken 2015/16, 26 643, nr. 383, p. 3

⁴³ NAS 2018, p.1

⁴⁴ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 12

⁴⁵ Kamerstukken 2016/17, 32 317 of 26 643, nr. 429

Concept

encryptie is betrokken. Daarnaast wordt ook opgeslagen data steeds vaker versleuteld en wordt toegang tot data op inbeslaggenomen hardware steeds moeilijker. Deze conclusie wordt gedeeld door Europol.⁴⁶ In de beantwoording wordt aangegeven dat nationale wetgeving niet afdoende is om voldoende effectief bewijs te vergaren wanneer deze is versleuteld. Toentertijd was geen bevoegdheid om toegang te verkrijgen tot het apparaat voordat het bericht werd versleuteld, noch een mogelijkheid om de dataflow om te leiden om toegang te verkrijgen. Ook is het breken van encryptie (via brute force) niet mogelijk. De consequenties op een breed scala aan criminele feiten wordt hier erkent. Meer concreet in de opsporing kan worden gewezen op de effectiviteit van een bevel tot aftappen en de aanpak van kinderporno.

3.1 Aftappen

Indicatoren Unit Landelijke Interceptie ⁴⁷						
	2013	2014	2015	2016	2017	2018
Aantal nummers waarvoor een bevel tot aftappen is gegeven	26.150	25.181	24.063	24.850	24.900	23.458
Gemiddeld aantal taps per dag	1.391	1.386	1.415	1.423	1.421	1.397
IP-taps*	17.806					
Gemiddeld aantal IP- taps per dag	829					
Aantal aanvragen op historische gegevens**	62.554	62.533	56.100	58.985	59.434	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.						

Table 1 Indicatoren Unit Landelijke Interceptie

Tappen is een belangrijke opsporingsmethode in de strijd tegen zware criminaliteit. Reeds in 2012 is geconcludeerd dat de internettap (of IP-tap) sterk aan effectiviteit heeft ingeboet.⁴⁸ Dit komt doordat communicatiediensten steeds vaker standaard gebruik maken van encryptie, deze diensten een ander bedrijf inschakelen om encryptie toe te passen, of gebruikers aanvullend encryptie toepassen (bijvoorbeeld Pretty Good Privacy). Het is niet alleen encryptie die effectiviteit van de interceptie schaadt, ook het gebruik van wifi netwerken of hotspots is hier onderdeel van. Dit komt omdat wifi netwerken in een restaurant, trein of café van verschillende aanbieders zijn en bij al deze aanbieders een tap moet worden geplaatst. Aangezien ook steeds vaker via internet wordt gebeld (Skype, WhatsAppgesprek) boet ook de telefoontap aan effectiviteit in.

In de Verenigde Staten worden jaarlijks statistieken gepubliceerd over tappen. Deze tapstatistieken zijn verre van volledig, aanzien veel wetgeving waarvoor interceptie zou kunnen worden ingezet wordt uitgezonderd in de rapportage.⁴⁹ Het gaat hier om: 'interception of wire, oral, or electronic communications' In 2018 zijn 2.937 toegestaan door de rechter. In 2018 werd in 96% van de gevallen een tap geplaatst op een mobiel apparaat. Dit betreft bijvoorbeeld mobiele communicatie, tekst berichten en applicatie software (apps). In 46% van de gevallen was de tap nodig in een onderzoek

⁴⁶ Europol 2019, p. 23

⁴⁷ VI Justitie en Veiligheid – Rijksjaarsverslag 2018, p. 49

⁴⁸ Oerlemans 2012, p. 30

⁴⁹ SECTION 1. EXEMPTION OF CERTAIN REPORTS FROM AUTOMATIC ELIMINATION AND SUNSET, S. 1769 — 106th Congress: Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act.

Concept

naar drugscriminaliteit, samenzwering vertegenwoordigt 13% van de taps en moord en mishandeling 4%.⁵⁰

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

Table 2 'interception of wire, oral, or electronic communications'

In totaal ging het in Amerika in 2018 om 2.937 taps waar in 220 gevallen men te maken kreeg met encryptie, dit is in een kleine 5% van de gevallen. Van de 220 gevallen kon 192 keer (87%) geen toegang worden verkregen tot de data. De groei van het aantal keer dat men encryptie tegenkomt en niet kan breken was als volgt:

Tap statistieken in de VS ⁵¹			
	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

Table 3 Tap statistieken in de VS

In Amerika zijn de tapcijfers relatief gering, maar de statistieken laten zien dat in steeds vaker encryptie een rol speelt, van 102 in 2017 naar 220 in 2018, en dat steeds vaker geen inzicht kan worden verkregen, van 97 keer in 2017 naar 192 in 2018. Ook worden opsporingsonderzoeken naar vele verschillende strafbare geraakt.

3.2 Opgeslagen data: The golden age of surveillance

De informatiemaatschappij waarin wij leven heeft een positief effect op de beschikbare data voor de opsporing.⁵² Met een tap ontvangt de opsporing niet alleen spraak communicatie, maar kan ook de belgeschiedenis, locatiegegevens en contactgegevens worden verkregen. Verder kan opgeslagen data op een telefoon of in een cloud in beheer zijn bij een dienstverlener en worden gevorderd of worden verkregen na inbeslagname. Met de hoeveelheid data die tegenwoordig wordt geproduceerd wordt wel eens gesproken van de 'de golden age of surveillance'.⁵³ Hier wordt vanuit de Amerikaanse opsporing tegenin gebracht dat er geen sprake is van deze gouden eeuw, aangezien sprake is van toenemende versleuteling en dat de beschikbaarheid van deze informatie afhankelijk is van de databron. Verschillende typen data staan exclusief op het apparaat, in de cloud of zijn alleen in bezit van de dienstverlener.

De manier waarop de ontwikkeling van encryptie een effect heeft op de beschikbaarheid van data kan worden geïllustreerd door de mogelijkheid van de opsporing om toegang te verkrijgen tot iPhones. In de iPhone 4 en eerdere modellen kon het wachtwoord via *brute force* worden achterhaald. Met *brute force* wordt geautomatiseerd alle mogelijk combinaties geprobeerd. Vanaf

⁵⁰ US Courts 2018

⁵¹ US Courts 2020

⁵² NAS 2018, p. 7

⁵³ Walden 2018, p. 906

Concept

de iPhone4s en met telefoons die het besturingssysteem van Apple, IOS 7, gebruiken was *brute force* niet meer mogelijk en moest de telefoon naar Apple worden verstuurd waarna een kopie van de data werd verkregen. Data werd bij deze telefoons ontoegankelijk wanneer een maximum aantal pogingen onsuccesvol was. Vanaf versie 8 van het besturingssysteem, IOS 8, kon Apple de telefoons niet langer ontsleutelen.⁵⁴

Daarnaast is de beschikbaarheid van data afhankelijk van de databron. In onderstaande tabel wordt de beschikbaarheid van opgeslagen data geanalyseerd en bij aangegeven bij welke databronnen deze beschikbaar is. Uit deze analyse van de Amerikaanse opsporing blijkt dat veel opgeslagen data beperkt is tot het apparaat zelf, of men is afhankelijk van instellingen van de gebruiker en beleid van de dienstverlener rond de bewaring van de informatie. Verschillende bedrijven houden verschillende termijnen aan voor het bewaren van bel of chatgeschiedenis.⁵⁵

Vergelijking van databronnen				
	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

(1) Apple's website states that it can provide this information (http://images.apple.com/privacy/docs/us_le_guidelines_final_20150916.pdf, p. 8). In response to search warrants, however, Apple has not provided such information for backups of phones running IOS 8.

(2) The information would be available to law enforcement only if the device user chose to back up to the cloud and included this type of data. See discussion immediately following chart.

(3) Most carriers do not retain content. Some that do, retain for only a short period (e.g., 3-5 days).

(4) This data can be obtained by law enforcement while the data is retained by the phone service provider. There is no requirement, however, that wireless carriers maintain this type of data at all or for any particular length of time. In addition, cell site data is not retained by certain phone carriers for text messages. Given that many people now primarily communicate through text messages, this limits the amount of location information investigators can learn through cell site data.

(5) May be available for only certain devices.

(6) Forensic analysts are able to extract this information from devices. When Apple provides device data pursuant to an unlock order, however, they do not include this data.

(7) May be available from Google when stored in its servers. This type of data does not appear to be stored in Google's cloud.

(8) Certain types (e.g., GPS EXIF data) may be available, but not all (e.g., Google Maps data).

⁵⁴ Manhattan District Attorney's Office 2015, p. 4; Lewis et al 2017, p. 8

⁵⁵ Congressional Research Service 2017, p. 7

Concept

Table 4 Bron Manhattan District Attorney's Office 2015, p. 7

Ook al is de trend dat veel data wordt opgeslagen in de cloud is de politie nog allerm minst zeker van toegang tot de data. In het algemeen stelt de Commissie modernisering opsporingsonderzoek in het digitale tijdperk dat steeds vaker data wordt opgeslagen en versleuteld op een wijze waardoor de aanbieder er zelf ook niet meer bij kan.⁵⁶ Maar ook wanneer data wél beschikbaar is, is succes van meerdere factoren afhankelijk. Ten eerste moet hier onderscheid worden gemaakt of de politie weet van welke cloud-dienst de verdachte gebruik maakt, bijvoorbeeld Apple, Google, Microsoft, Amazon, Dropbox, etc. Indien de politie dit weet zou deze de informatie kunnen vorderen en is men afhankelijk of de cloud-dienst een sleutel bewaart. Indien de politie niet weet welke cloud-dienst wordt gebruikt kan de telefoon in beslag worden genomen, maar is men afhankelijk van toegang tot het apparaat. Data kan zijn verwijderd indien niet snel genoeg toegang wordt verkregen tot het apparaat of de juiste cloud-dienst niet snel genoeg wordt geïdentificeerd. Een dergelijk 'wiscommando' is bijvoorbeeld ook de reden dat verbindingen van in beslaggenomen geautomatiseerde werken onmiddellijk moeten worden verbroken.⁵⁷ Daarnaast is de opsporing afhankelijk van de instellingen van de gebruiker om data op te slaan in de cloud en van de instellingen van de cloud-dienst. Een cloud-dienst kan vereisen dat een Wifi-verbinding nodig is of juist een netwerkverbinding voor het synchroniseren van de telefoon met de cloud. Gegevens die voor die tijd zijn geproduceerd staan alleen op het apparaat. Ook kan verwijderd materiaal van een apparaat in gevallen worden teruggezet, terwijl dit bij de cloud niet mogelijk kan zijn.⁵⁸

Over de problematiek met toegang tot een smartphone wordt sinds 2015 gepubliceerd door het bureau van de Officier van Justitie van het Manhattan District in New York. In de eerste 10 maanden van 2017 zijn daar voor 1.200 apparaten een machtiging van de rechtbank verkregen of is toestemming verkregen om het apparaat te doorzoeken. Rond de helft was vergrendeld bij ontvangst (72% Apple, 37% Android). In 2019 is het aantal vergrendelde ontvangen telefoons gegroeid tot 64% (82.2% Apple, 50.1% Android).⁵⁹ Het ontvangen van vergrendelde telefoons betekend dat er een beveiliging moet worden doorbroken voor toegang, bijvoorbeeld de toegangscode. Gegeven hetgeen dat aan het begin van deze paragraaf is gezegd, is dit in toenemende mate problematisch.

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

Table 5 Bron: Manhattan District Attorney's Office 2017, p.5

In de ongeveer eerste elf maanden van 2017 ging het op federaal niveau bij de FBI om 6.900 mobiele apparaten waarbij in over de helft van de gevallen geen toegang werd verkregen tot data.⁶⁰ In 2019 is in het Manhattan district een tabel gemaakt van het type misdrijven waarbij een mobiel apparaat is verkregen, versleuteld of toegankelijk.

⁵⁶ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 121

⁵⁷ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 14

⁵⁸ Manhattan District Attorney's Office 2015, p. 8

⁵⁹ Manhattan District Attorney's Office 2019, p. 4

⁶⁰ Business Insider 2017

Concept

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%

Table 6 Bron: Manhattan Distric Attorney's Office 2019, p. 5

3.3 Kinderporno

Voor de aanpak van kinderporno hebben de VS, samen met het VK en Australië, recent het belang van Facebook in deze aanpak aangegeven. Deze cijfers zijn vrijgegeven nadat Facebook had besloten om Messenger end-to-end te versleutelen waarbij deze meldingen praktisch zouden verdwijnen. In 2018 heeft Facebook 16.8 miljoen meldingen gedaan aan het National Center for Missing & Exploited Children (NCMEC) (90% van het totaal aantal ontvangen meldingen). Hierbij waren 8.000 pogingen tot grooming, sexting of ontmoetingen. In het VK heeft dit geleid tot 2.500 arrestaties en 3.000 kinderen zijn veiliggesteld.⁶¹

In de laatste jaren nam in Nederland het aantal meldingen van online seksueel misbruik en kinderpornografie explosief toe: van ruim 5000 in 2015 naar ruim 30.000 in 2018. Ten opzichte van 2017 is de instroom van het aantal meldingen gestegen met 69%. Ook in Nederland wordt het beeld herkend dat verschillende chat en messenger applicaties worden gebruikt voor het delen van strafbaar materiaal. Een ruime meerderheid van de meldingen die bij de Nederlandse politie in 2019 zijn binnengekomen is afkomstig van Facebook of Instagram. Hiervan is overigens ook een groot percentage beeldmateriaal dat, ondanks een bloot kind, niet kinderpornografisch van aard is. Facebook is daarmee geen platform vol verderfelijk materiaal, de huidige hoeveelheid meldingen bewijst juist het belang van samenwerken met (grote) platforms.⁶²

Daarnaast wordt er ook proactief opgespoord, want een opsporingstraject door OM en politie, al dan niet naar aanleiding van een melding, blijft essentieel. Daarbij helpt het als bij een aanhouding een profiel met chatgeschiedenis wordt bevroren, zodat alle (belastende) informatie voor politie en OM beschikbaar blijft. Dit geeft namelijk inzicht in het netwerk van een verdachte en daarmee in slachtoffers en medeverdachten. Dat bevroren kan een Platform op verzoek van OM/politie doen, maar encryptievoornemens kunnen de leesbaarheid van het materiaal schaden.

3.4 Conclusie

In dit hoofdstuk is het effect van encryptie op de opsporing bij vier verschillende toepassingen toegelicht. Bij stromende data (tappen), opgeslagen data (Cloud en apparaat), en de scancapaciteit van social media. In Amerika heeft men reeds jaren ervaring met de vergaring van data, de analyse ervan en het inzichtelijk maken van de wijze waarop de toepassing problematisch kan zijn. Helaas verschilt het aggregatieniveau zodanig dat het lastig is om een vergelijking te maken tussen de toepassingen van encryptie. Dat wil zeggen, de cijfers inzake stromende data wordt op federaalniveau gemeld, terwijl de cijfers over opgeslagen data voornamelijk op lokaal niveau is gepresenteerd. Een conclusie dat, gegeven tabellen 2 en 6, drugsonderzoeken meer gebaat zijn bij een oplossing bij stromende data en diefstal en cybercrime-gerelateerde zaken bij opgeslagen data is

⁶¹ US Justice departement 2019

⁶² Wijk et al 2019, p. 7

Concept

niet mogelijk. Ook wanneer men de aantallen van tabellen 1, 3 en 5 vergelijkt is de Amerikaanse situatie door verschil in definitie en transparantie niet vergelijkbaar met de Nederlandse.

De cijfers zijn echter wel in algemene zin tekenend voor de ervaren problematiek. Apparaten en/of digitaal bewijs worden steeds vaker geraadpleegd in opsporingsonderzoeken. Ondanks de groeiende rol van apparaten en digitaal bewijs is deze steeds vaker beveiligd en is de beveiliging minder vaak te doorbreken. Daarnaast wordt de problematiek niet alleen ervaren bij terroristen, technisch kundige criminelen of criminele hoofdrolspelers, maar wordt de problematiek in vele typen onderzoek gevoeld.

Zoals uit bovenstaande blijkt zijn er vier toepassingen van encryptie waardoor de opsporing wordt belemmerd. 1) het apparaat is versleuteld, waardoor inbeslaggenomen hardware niet of ten dele kunnen worden uitgelezen, 2) de communicatiestroom is versleuteld, waardoor ondanks een tapbevel geen inzicht wordt verkregen in de stromende data, 3) opgeslagen data is versleuteld, waardoor niet of lastiger toegang verkregen kan worden tot bijvoorbeeld de cloud, en 4) versleuteling maakt het werk van derden onmogelijk om mee te werken aan de opsporing. Een vijfde categorie, e-mail encryptie, is volgens de literatuur nog geen groot probleem. Dit komt mogelijk door de wens van gebruikers om makkelijk bij e-mails te kunnen komen, makkelijk wachtwoordherstel in te schakelen en de kosteloze toegang tot deze dienst waarbij bedrijven de inhoud voor commerciële doeleinden benutten.⁶³

Dit onderscheid in de toepassingen van encryptie is belangrijk voor de beoogde oplossing. De Nederlandse minister heeft in Nieuwsuur een voorstel gedaan voor een sleutelrecht waarbij via internetpartijen, in het geval er sprake is van verdacht verkeer, toegang hiertoe kan worden verkregen.⁶⁴ Bij dit type toegang moet dus sprake zijn van een verdachte situatie. Deze vorm van 'toegang in het concrete geval' kan effectief zijn in de gevallen waarin een apparaat is versleuteld, de communicatiestroom is versleuteld of indien opgeslagen data is versleuteld. Er is een andere oplossing nodig voor de problematiek die aanleiding is voor de brief van de Amerikaanse, Britse en Australische minister van Justitie. Met de voorgestelde end-to-end encryptie van Facebook kan dit verdachte verkeer niet meer worden herkend.

4. Oplossingen

In antwoord op de tweede onderzoeksvraag 'Is er een manier waarop rechtmatige toegang kan worden verkregen zonder encryptie structureel te verzwakken' is zijn diverse oplossingen geïnventariseerd. Men kan onderscheid maken tussen het stellen van eisen aan encryptietechnologie, rekenkracht van de opsporing, en samenwerking met een derde partij. Daarnaast zijn er alternatieven beschreven die encryptie zelf ongemoeid laten, maar deze omzeilen.

In dit rapport worden theoretische oplossingen geïnventariseerd en wet- of regelgeving waarin wordt vereist dat bedrijven een decryptie mogelijkheid te hebben. Dit zou gepaard kunnen gaan met boetes voor bedrijven die niet meewerken.⁶⁵ In plaats van bedrijven dwingen om openingen in hun technologie in te bouwen ten behoeve van de overheid kunnen systemen worden ontworpen waar bedrijven zelf wel toegang tot hebben. Bij eventuele wet- en regelgeving wordt gewaarschuwd dat een langere implementatietijd van minimaal 12 maanden nodig kan zijn voor bedrijven om systemen te ontwerpen waar risico's die voortkomen uit deze mogelijkheid worden ondervangen.⁶⁶

⁶³ Lewis et al 2017, p. 10

⁶⁴ NOS 2019b

⁶⁵ Shah 2015, p. 555

⁶⁶ Shah 2015, p. 557

Concept

Bij de beslissing over een oplossing zou moeten worden nagedacht over waar de problematiek het meest urgent is. Zoals onder paragraaf drie is aangegeven is het maken van onderscheid tussen de verschillende toepassingen van encryptie belangrijk. Men kan kiezen voor een oplossing voor opgeslagen data op telefoons, wanneer de behoefte naar rechtmatige toegang hiervoor het grootst is.⁶⁷ De markt voor mobiele telefonie wordt gedomineerd door enkele bedrijven hetgeen het regulerend kader overzichtelijk maakt. De onderstaande inventarisatie is breed van aard en er is beoogd om geen mogelijkheid onbesproken te laten. De bezwaren die worden genoemd bij de oplossingen zijn illustrerend bedoeld. Het is niet het doel geweest uitputtend te zijn in de mogelijke bezwaren die bestaan.

4.1 Reguleren encryptietechnologie

Verzwak encryptie

Het is mogelijk om het algoritme van encryptie aan te passen zodat dit te breken is door de opsporing. Bijvoorbeeld door het verkorten van sleutels.⁶⁸ Indien deze oplossing in zijn algemeenheid wordt doorgevoerd zou dit kunnen worden misbruikt door kwaadwillende actoren.⁶⁹ Daarnaast stelt de AVG eisen om de nodige technische en organisatorische veiligheidsmaatregelen te nemen bij de gegevensverwerking.⁷⁰

Een andere mogelijkheid is om gevonden kwetsbaarheden in encryptiesoftware door de opsporing niet te melden aan de producent van de software.⁷¹ In software die veelvuldig wordt gebruikt in de maatschappij zou dit tevens risico's kunnen opleveren voor onschuldige burgers. Deze kwetsbaarheid kan immers ook worden uitgewonnen door kwaadwillenden.⁷²

Versimpel het verzamelen of volgen van sleutels

Dit is onder andere mogelijk bij inzicht verkrijgen in zowel opgeslagen als stromende data. Mogelijkheden hiervoor zijn het koppelen van sleutels aan andere sleutels of het opslaan van sleutels hetzij op het apparaat of daarbuiten (key escrow).⁷³ Key escrow wil zeggen dat een partij borg staat voor de gerichte ontsleuteling. Deze partij kan een commercieel bedrijf of de overheid zijn. Indien bedrijven zelf sleutels bewaren kan elk bedrijf zijn eigen algoritme bepalen.⁷⁴ Indien een overheidsorganisatie deze rol vervult zou betekenen dat de overheid bepaalt welke algoritmes producenten gebruiken voor key escrow, of dat de producent de overheid voorziet van de vereiste code om te ontsleutelen.⁷⁵ De eerste mogelijkheid legt een zware verantwoordelijkheid bij de overheid om de best technologische oplossing te blijven creëren, terwijl de tweede mogelijkheid veel capaciteit vraagt van de overheidsorganisatie om alle sleutels bij specifieke organisaties te bevragen. Tevens kunnen derde partijen deze rol vervullen, maar des te meer leveranciers van ICT apparaten of diensten deze partij gebruiken des te aantrekkelijker de derde partij wordt voor aanvallen.⁷⁶

Een andere mogelijkheid is om de sleutel te verdelen in verschillende stukken en deze later te koppelen. Elk deel kan worden opgeslagen bij een andere organisatie waardoor de code niet kan

⁶⁷ Carnegie Endowment for International peace 2019, p.11

⁶⁸ NAS 2018, p. 65

⁶⁹ Internet society 2017, p. 4

⁷⁰ Walden, 2018, p. 905

⁷¹ Europol 2019

⁷² Internet society 2017, p. 4

⁷³ Carnegie Endowment for International peace 2019, p.10

⁷⁴ NAS 2018, p. 49

⁷⁵ NAS 2018, p. 49

⁷⁶ NAS 2018, p. 49

Concept

worden gebroken indien een bedrijf is gecompriëerd. Hierbinnen zijn tevens verschillende mogelijkheden, bijvoorbeeld dat de sleutel uit vijf onderdelen bestaat en dat bij drie uit de vijf onderdelen het bericht kan worden ontsleuteld. In de praktijk kan een onderdeel van de sleutel in beheer zijn bij een leverancier, de overheid en een derde partij. In het verleden is dit te complex beoordeeld.⁷⁷

Het opslaan van sleutels op het apparaat voorkomt dat er een centrale 'honey pot' wordt gecreëerd die aantrekkelijk is voor kwaadwillend actoren. Ook is het risico op, en het gevolg van, van een data lek kleiner. Bij een centrale opslag zijn gelijk vele telefoons kwetsbaar, terwijl hier de beveiliging per telefoon is geregeld.⁷⁸ Daarnaast kan dit op zo'n wijze worden vormgegeven dat fysieke toegang tot de telefoon nodig is voordat de sleutel kan worden verkregen.⁷⁹ Ook hier is het mogelijk om de uiteindelijke sleutel te verdelen in meerdere delen.⁸⁰ Enkele auteurs verkiezen een dergelijke oplossing boven het sturen van valse updates naar een verdachte waardoor een kwetsbaarheid in de software voor die verdachte wordt gecreëerd. Indien dit gemeengoed wordt zouden individuen terughoudend kunnen worden met het updaten.

Het bewaren van sleutels is geen nieuw gegeven voor dienstenleveranciers. Leveranciers kunnen sleutels bewaren als verificatie voor het uitvoeren van updates 'institutional-level keys' of sleutels bewaren voor klanten in het geval ze hun sleutel verliezen.⁸¹ Deze sleutels kunnen worden gelekt of aantrekkelijk zijn voor kwaadwillenden.

4.2 Rekenkracht van de opsporing

Raden van de sleutel

De kracht van encryptie wordt berekend in bits. 64-bit sleutels kunnen redelijk simpel worden gebroken via *brute force*. 80-bit sleutels vereisen een flinke computercapaciteit zoals Inlichtingen- en opsporingsdiensten kunnen organiseren. Maar 128-bit sleutels zijn praktisch buiten bereik van hedendaagse computertechnologie en 256-bit sleutels ook voor toekomstige voorzienbare technologieën. De laatste twee type sleutels worden vandaag de dag het meest gebruikt.⁸² Europol schat in dat het tot 2500 jaar kan duren met de huidige computerkracht om de sleutel te raden indien een crimineel encryptiesoftware gebruikt. Met het vergroten van de computerkracht kan deze tijd worden verlaagd tot 500 jaar. Deze tijd kan worden verkort wanneer persoonlijke gegevens bekend zijn bij de opsporing. Wachtwoorden kunnen toegang verlenen tot de encryptiesleutel Het gros van de mensen gebruikt woorden, namen of (geboorte)data en hergebruikt wachtwoorden of een kleine variatie daarop.⁸³

Zoals in paragraaf 3.2 is vermeld kan er een limitatief aantal mogelijkheden zijn in het raden van het wachtwoord. In de literatuur is geen vermelding gevonden van de mogelijkheid om het limitatief aantal pogingen om een wachtwoord in te voeren door de telefoon- of besturingssysteemfabrikant uit te schakelen en alsnog over te gaan op *brute force*.

⁷⁷ NAS 2018, p. 49, 50

⁷⁸ Internet society 2017, p. 4

⁷⁹ Carnegie Endowment for International peace 2019, p.12, 13

⁸⁰ NAS 2018, p. 50, 51

⁸¹ NAS 2018, p. 47, 50

⁸² Kerr & Schneier 2018, p. 6,7

⁸³ Europol 2019, p. 29; Kerr, Schneier 2018, p. 11-13

Concept

4.3 Samenwerking met een derde partij 'Vendor Unlock'

Masterkeys of achterdeuren

De houder van deze sleutel heeft toegang tot de data die is versleuteld door dat bedrijf.⁸⁴ Aangezien dit een algemene kwetsbaarheid in het systeem introduceert heeft dit dezelfde nadelen als het verzwakken van encryptie.⁸⁵

Zoals hierboven aangegeven wordt voor encryptie van opgeslagen data in de cloud vaak door organisaties toegang tot encryptiesleutels behouden om de consumenten te kunnen bedienen in geval deze toegang wenst, wilt synchroniseren, of data wilt herstellen.⁸⁶ Dit wordt door anderen genuanceerd door te stellen dat dit alleen authenticatiesleutels zijn die de identiteit van de klant verifiëren een aanvullende encryptiesleutel geeft toegang tot de versleutelde data.⁸⁷

Valse update

Software updates actualiseren het besturingssysteem van de gebruiker. Het is mogelijk om richting gebruikers individueel updates te sturen en expres een zwakte in deze versie te bouwen die kan worden uitgebuit. Tegenstanders van deze optie vrezen voor het vertrouwen van personen in het installeren van updates.⁸⁸ Ook is de opsporing afhankelijk van het tijdstip waarin de verdachte de update installeert of dat deze persoon 'automatisch updaten' ingeschakeld heeft. Voorstanders van deze mogelijkheid benadrukken het gerichte en specifieke karakter van deze oplossing.⁸⁹

Zonder voorgeschreven technische oplossing

Men kan een algemene decyptieplicht instellen zonder daarbij voor te schrijven hoe bedrijven hier invulling aan kunnen geven. Dit kan door proportionele medewerking te verlenen op een case-by-case basis.⁹⁰ De vraag is vervolgens wat redelijkerwijs van een dienstverlener kan worden verwacht. Wat is redelijk gegeven het dreigingsbeeld, de capaciteit, kosten-baten voor het niet-medewerken met de opsporing, of als verantwoording over gegevensverwerking richting de klanten.⁹¹ Daarnaast wordt door dienstenleveranciers vaak tegengeworpen dat medewerking technisch niet mogelijk is omdat ook zij geen inzicht hebben in de sleutels, bijvoorbeeld bij end-to-end versleuteling. De juridische houdbaarheid van dit argument is in de Skype-uitspraak onderuit gehaald in België:

*According to the court, there can be no question of any material impossibility to comply with the cooperation duty in respect of Skype, given the fact that Skype created this material impossibility itself by organising the supply of services to its users in such a way.*⁹²

In hoger beroep is daarnaast geoordeeld dat bij de ontwikkeling van de programmatuur geen rekening is gehouden met het vervullen van wettelijke voorschriften:

⁸⁴ NAS 2018, p. 65

⁸⁵ Internet society 2017, p. 4

⁸⁶ Carnegie Endowment for International peace 2019, p.11

⁸⁷ Internet society 2017, p. 4

⁸⁸ NAS 2018, p. 47, 48

⁸⁹ Carnegie Endowment for International peace 2019, p.11, 12

⁹⁰ NAS 2018, p. 51

⁹¹ NAS 2018, p. 51

⁹² Public Prosecutor's Office v Skype Communications SARL, Case no. ME 20.F1.105151-12, 27 October 2017, at para. 5.5.2.

Concept

*The fact that Skype did not conceive its technical infrastructure from the outset in order to be able to comply with its legal obligations...exactly constitutes the criminal offense which Skype is reproached in the present case.*⁹³

Skype is daarmee schuldig bevonden en beboet⁹⁴, echter tot een doorbraak in opsporing heeft het niet geleid.

Ontsleuteldozen

De Commissie modernisering opsporingsonderzoek in het digitale tijdperk geeft aan dat voor het vastleggen van telecommunicatie en vertrouwelijke communicatie vanwege de toename in (eind tot eind) versleutelde communicatie het wenselijk is om bij de interceptie gebruik te maken van "ontsleuteldozen" in de lawful intercept-infrastructuur van de aanbieder. Zoals aangegeven in paragraaf 2.1.3 is het ontdoen van versleuteling reeds de praktijk bij telecommunicatieaanbieders, bij de eventuele uitwerking van een oplossing kan een voorbeeld worden genomen aan deze praktijk.

4.4 Alternatieven

Decryptiebevel verdachten

In paragraaf 2.2 is reeds geschreven over de spanning van het decryptiebevel met het beginsel van nemo-tenetur. Tegelijkertijd is een decryptiebevel aan een persoon niet verboden en is dit een uitwerking van art. 19(4) van de Budapest Conventie.⁹⁵ In Nederland is de uitwerking geregeld in art. 125k Sv, waarbij iemand die vermoedelijk kennis draagt van de beveiliging van een geautomatiseerd werk kan worden bevolen om daartoe toegang te verschaffen.⁹⁶ In de herziening van het wetboek van strafvordering wordt dit bevel opgenomen in artikel 2.7.4.1.4 en uitgebreid tot een ontsleutelbevel voor geautomatiseerde werken én gegevensdragers.⁹⁷ Het is hierbij belangrijk om te bepalen of de wijze van ontsleuteling afhankelijk is van de wil van de verdachte. Een biometrisch gegeven, zoals een vingerafdruk, een iris scan of Face-ID, komt niet voort uit het brein, maar uit het lichaam. Deze kenmerken kunnen worden verkregen onafhankelijk van de wil van de verdachte en de verdachte kan worden gedwongen medewerking te verrichten.⁹⁸ De beginselen van proportionaliteit en subsidiariteit en artikel 3 EVRM begrenzen de zo nodig uit te oefenen dwang.⁹⁹

Toegang tot het device

Met het binnendringen van een device wordt de encryptie omzeild en kunnen berichten worden ingezien voordat deze worden versleuteld. Toegang tot plaintext wordt hierdoor verbeterd.¹⁰⁰ Er worden enkele voorwaarden genoemd voor de effectiviteit van deze bevoegdheid, de teams moeten voldoende financiering hebben, voldoende capaciteit hebben en het moet zijn toegestaan om een arsenaal aan exploits op te bouwen om apparatuur binnen te dringen.¹⁰¹ Toegang tot de telefoon kan ook door een verdachte te surveilleren en het apparaat ontnemen zodra het niet vergrendeld is of middels het afvangen van gebruikersnamen en wachtwoorden.¹⁰²

⁹³ Court of Appeal of Antwerp, Case no. 2016/CO/1006, 15 November 2017, at section 5.1.2.3.

⁹⁴ Walden 2018, p. 904

⁹⁵ Walden 2018, p. 903

⁹⁶ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 104

⁹⁷ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 198

⁹⁸ Koops & Kosta 2018, p. 895

⁹⁹ Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018, p. 198

¹⁰⁰ NAS 2018, p. 8

¹⁰¹ Soesanto 2018, p. 29

¹⁰² NAS 2018, p. 8; Kerr & Schneier 2018, p. 26

Concept

Indien een opsporingsdienst een *dark web market* heeft overgenomen die bezoekers via diverse nodes, zoals bij The Onion Router, kunnen bezoeken kan ook een *Network Investigative Technique*, een type malware, worden geïnstalleerd op de computers van gebruikers. Deze malware reist mee via het verkeer dat van de website naar de gebruiker gaat via de diverse nodes en wordt geïnstalleerd op het eindpunt. Waardoor de daadwerkelijke IP-adres en plaats van herkomst kunnen worden achterhaald.¹⁰³

Voeg een opsporingsdienst toe aan een app

In 2018 hebben de Britse Technische directeur van het National Cyber Security Centre en de Technische Directeur voor Cryptanalysis voor het Government Communications Headquarters, twee wiskundigen het voorstel gedaan om de opsporing toe te voegen aan een groepschat of telefoongesprek.¹⁰⁴ De dienstverlener heeft in de regel controle over de identificeringssystematiek en kan bepalen welke apparaten betrokken worden in de chat of het gesprek. De facto wordt een extra 'end' aan de end-to-end encryptie toegevoegd. Dit is de digitale vorm van het vroegere 'klipje' op de telefoondraad. Critici van deze oplossing benadrukken onder andere de technische complexiteit om berichtgeving over een derde partij in de app te onderdrukken en waarschuwen voor toenemend wantrouwen richting de aanbieder van de app.¹⁰⁵

Maak meer gebruik van data die reeds in bezit is van dienstverleners

Expertise bij de opsporing over welke data wél beschikbaar is zou al veel voordeel kunnen hebben in de opsporing.¹⁰⁶ We leven immers in het tijdperk van ongekende dataverzameling. Investeer in de opleiding van de opsporing waarin wordt aangegeven wat wél kan.¹⁰⁷ Dit kan zeker voordeel hebben, maar dit standpunt lijkt geen rekening te houden met de trend dat steeds meer wordt versleuteld.¹⁰⁸ Desalniettemin verzamelen bedrijven veel data die mogelijk van waarde kan zijn voor de opsporing. Er kunnen betere afspraken komen om deze data te ontsluiten.¹⁰⁹ Het gebruik van data die reeds in bezit is van dienstverleners wordt beperkt door de restricties rond dataretentie.¹¹⁰

Homomorphic encryption

Homomorphic encryption is op dit moment erg in ontwikkeling.¹¹¹ Dit type encryptie maakt het mogelijk dat over versleutelde opgeslagen data te analyseren zonder de data van het individu inzichtelijk te maken.¹¹² Veel literatuur richt zich nu nog op de praktische toepassingen in de civiele sector, de toegevoegde waarde voor de opsporing moet verder worden onderzocht. Voor zover nu kan worden overzien kan deze oplossing dienstig zijn bij opgeslagen data, maar wordt geen inzicht verkregen in de inhoud van data. Een zorg van de opsporing is dat dit type encryptie kan worden gezien als 'zwakker' hetgeen de aantrekkingskracht van dit type encryptie kan schaden. Aan de andere kant kan een te grote populariteit huidige toegankelijke cloud-databases versleutelen.¹¹³

¹⁰³ Kerr & Schneier 2018, p. 27

¹⁰⁴ Levy & Robinson 2018

¹⁰⁵ Europol 2020, p. 10

¹⁰⁶ Balkovich et al 2015, p. 6,7

¹⁰⁷ Lewis et al 2017, p. 17

¹⁰⁸ Balkovich et al 2015, p. 7

¹⁰⁹ Internet society 2017, p. 5

¹¹⁰ Walden 2018, p. 907

¹¹¹ NAS 2018

¹¹² Marr 2019; Europol 2020, p. 20

¹¹³ Europol 2020, p. 21

Concept

Investeer in financiële en technische mogelijkheden voor de opsporing

Neem meer personeel in dienst om slimme oplossingen te bedenken, vergroot de capaciteit voor het binnendringen in een apparaat, en verhoog de expertise over welke data wél beschikbaar is. Zet daarnaast meer in op het delen van oplossingen tussen opsporingsautoriteiten en verbeter de samenwerking met leveranciers zodat professionals meer bekend raken met de producten. Ook kan een organisatie worden opgericht waar expertise samenkomt.¹¹⁴ Daarnaast kunnen bij de leverancier gemelde kwetsbaarheden worden gedeeld met de opsporing zodat in de tijd tussen melding en de update de kwetsbaarheid kan worden uitgewonnen. Deze verplichting tot mededeling van de kwetsbaarheid kan ook voor centrale derde partijen gelden. Daarnaast zou de overheid kunnen investeren in een type encryptie dat recht doet aan alle belangen.¹¹⁵

Daarnaast kan de opsporing proberen onderdeel te worden van de beveiliging, door zich bijvoorbeeld voor te doen als een node in het netwerk.¹¹⁶

Vergemakkelijk de medewerking van Inlichtingen- en Veiligheidsdiensten

Inlichtingen- en veiligheidsdiensten kennen een minder hoge drempel voor de inzet van bevoegdheden dan opsporingsdiensten, zij kunnen meer bevoegdheden hebben als de opsporing of reikwijdte van de inzet breder zijn.¹¹⁷ De rechtsbescherming is echter ook minder in de WIV dan in het strafrecht.

Vind een plaintext kopie

In gevallen kan het mogelijk zijn dat een eindversie door de gebruiker is versleuteld. Indien de laatste versie van een Word document is versleuteld, kunnen eerdere automatisch opgeslagen versies niet versleuteld zijn. Kopieën van e-mails kunnen opgeslagen zijn in de CLOUD en inzichtelijk zijn voor de betreffende dienstverlener, hetzelfde geldt wellicht voor een back-up. Het succes van deze oplossing is afhankelijk van 1) het bestaan een kopie, 2) het kunnen vinden van de kopie, 3) wettelijk grondslag voor de vordering moet bestaan, en 4) de niet versleutelde versie moet actueel zijn en vergelijkbaar met de versleutelde versie.¹¹⁸

Stel verstrekking, bezit of gebruik strafbaar

Men kan het gebruik van encryptie voor criminele doeleinden strafbaar stellen. Dit wordt geregeld in art. 6 van de Budapest Conventie.¹¹⁹ Het probleem is dat het lastig onderscheid maken tussen legitiem en crimineel gebruik van versleutelprogramma's. Het verstrekken van dergelijke software kan worden gereguleerd in een export-controle regime. Daarnaast kan met het gebruik van encryptie bij crimineel gedrag of strafverzwarend element regelen. Dit gebeurt reeds in de VS, Frankrijk en het VK.¹²⁰

Verdere ontwikkelingen

Andere ontwikkelingen zien op het inzicht verkrijgen in data via een 'restricted key', bijvoorbeeld het toetsen of bepaalde steekwoorden of zinnen voorkomen in de versleutelde tekst.¹²¹ Het simpel

¹¹⁴ Lewis et al 2017, p. 28

¹¹⁵ NAS 2018, p. 57, 58

¹¹⁶ Walden 2018, p. 905

¹¹⁷ Lewis et al 2017, p. 28

¹¹⁸ Kerr & Schneier 2018, p. 28, 29

¹¹⁹ Walden 2018, p. 902

¹²⁰ Walden 2018, p. 902

¹²¹ NAS 2018, p. 52, 66

Concept

veranderen van de spelling kan deze mogelijkheid al frustreren. Een simplistisch voorbeeld kan zijn, b0m met het getal '0' in plaats van de letter 'o'.

5. Afweging

Initiatieven om oplossingen te inventariseren om tot rechtmatige toegang tot versleuteld bewijs te komen worden vaak verwelkomd met kritiek dat 1) dit ineffectief is, 2) dit onacceptabele risico's oplevert voor cybersecurity, 3) dat dit onacceptabele risico's voor privacy en burgerlijke vrijheden oplevert, 4) dienstverleners voor een onmogelijke opgave stelt, en 5) innovatie van encryptie schaadt.¹²² Daarnaast wordt ook naar voren gebracht dat landen met een slecht mensenrechtenbeleid ook misbruik kunnen maken van deze oplossing.

Daarom is het van belang om mogelijke oplossingen goed af te wegen. Diverse elementen worden voorgesteld. De studie van het National Academies of Sciences wordt aangegeven dat aandacht moet worden besteed aan 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.¹²³

Een andere benadering is om verschillende principes te hanteren: 1) een oplossing moet gericht zijn, 2) beveiliging niet verzwakken, 3) geen verandering brengen in het vertrouwen tussen rechtmatige gebruikers en bedrijven, 4) rechtmatige toegang tot data moet mogelijk zijn, 5) één oplossing werkt niet altijd, en 6) een oplossing is gebaseerd op samenwerking tussen bedrijven en de opsporing.¹²⁴

Weer anderen geven richtlijnen voor de discussie: 1) voorkom absolute stellingname, 2) start het debat door het vaststellen van een gezamenlijke zorg, 3) erken dat veiligheid vele vormen aanneemt en verward 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.¹²⁵

Verder hebben de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw Zeeland een 'Five Country statement' uitgebracht in 2018 waarin drie principes staan voor toegang tot bewijs en encryptie. In het statement wordt de toegevoegde waarde van encryptie voor privacy, de digitale economie, cybersecurity en het vertrouwelijk communiceren van burgers, bedrijven en overheid onderschreven. De drie principes die vervolgens worden genoemd zijn: 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 rechtswaarden staan voorop, toegang tot data moet worden gereguleerd door de bescherming voor burgers die de rechtstaat biedt. 3) vrijheid in de

¹²² NAS 2018, p. 1

¹²³ NAS 2018, p. 2

¹²⁴ Internet Society 2017, p. 6,7

¹²⁵ Carnegie Endowment for International peace 2019, p. 3-6

Concept

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.¹²⁶

Het VK heeft dit nader uitgewerkt in enkele principes¹²⁷:

- 1) Privacy and security protections are critical to public confidence. Therefore, we will only seek exceptional access to data where there's a legitimate need, that access is the least intrusive way of proceeding and there is appropriate legal authorisation
- 2) Investigative tradecraft has to evolve with technology.
- 3) Even when we have a legitimate need, we can't expect 100 percent access 100 percent of the time.
- 4) Targeted exceptional access capabilities should not give governments unfettered access to user data.
- 5) Any exceptional access solution should not fundamentally change the trust relationship between a service provider and its users.
- 6) Transparency is essential

6. Conclusie

De opsporing in het digitale domein is volop in ontwikkeling en ervaart een minder effectief opsporingsinstrumentarium in de online wereld ten opzichte van de offline wereld. Men vreest dat de opsporing steeds meer in het duister tast waardoor het digitale domein een vrijplaats wordt voor criminelen. Encryptie speelt hierin een belangrijke rol, de vraag is of er maatregelen moeten worden genomen die zien op een aanpassing van encryptie of dat meer aandacht moet uitgaan in het omzeilen van encryptie.¹²⁸ De onderzoeksvragen aan het begin van dit literatuuronderzoek waren de volgende.

- 1) Is de problematiek bij de opsporing en Inlichtingen en Veiligheidsdiensten dermate dat het op terreinen het verzwakken van encryptie legitimeert, en 2) is er een manier waarop rechtmatige toegang kan worden verkregen zonder encryptie structureel te verzwakken?

Dit literatuuronderzoek geeft voldoende redenen om deze vragen verder te onderzoeken, maar vooralsnog geen adequate antwoorden.

¹²⁶ Five Country Ministerial Statement 2018

¹²⁷ Levy & Robinson 2018

¹²⁸ Kerr & Schneier 2018, p. 4,5

Concept

Literatuurlijst

Balkovich et al 2015

E. Balkovich, D. Prosnitz, A.E. Boustead, and S.C. Isley, *Electronic Surveillance of Mobile Devices: Understanding the Mobile Ecosystem and Applicable Surveillance Law*. RAND Corporation Santa Monica, CA 2015. https://www.rand.org/pubs/research_reports/RR800.html. Also available in print form.

Business Insider 2017

Business Insider, <https://www.businessinsider.com/ap-fbi-couldnt-access-nearly-7k-devices-because-of-encryption-2017-10?international=true&r=US&IR=T>, geraadpleegd op 20 februari 2020, New York 2017

Carnegie Endowment for International Peace 2019

Carnegie Endowment for International Peace, Princeton University, Centre for Information Technology Policy, *Moving the Encryption Policy Conversation Forward: Encryption Working Group*, Washington D.C. 2019

CBS.nl 2017

Centraal Bureau voor de Statistiek, <https://www.cbs.nl/nl-nl/nieuws/2017/39/een-op-vijf-bedrijven-slachtoffer-van-cyberaanval>, geraadpleegd op 20 februari 2020, Den Haag 2017

Congressional Research Service 2016

Congressional Research Service, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, Washington D.C. 2016

Congressional Research Service 2017

Congressional Research Service, *Encryption and the "Going Dark" Debate*, Washington D.C. 2017

Commissie modernisering opsporingsonderzoek in het digitale tijdperk 2018

Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018

Council of the European Union 2016

Council of the European Union, *Encryption: Challenges for criminal justice in relation to the use of encryption – future steps – progress report*, 14711/16, Brussel 2016

Cybersecuritybeeld Nederland 2017

Nationaal Coördinator Terrorismebestrijding en Veiligheid *Cybersecuritybeeld Nederland (CSBN) 2017*, Ministerie van Veiligheid en Justitie, Den Haag 2017

Cybersecuritybeeld Nederland 2019

Nationaal Coördinator Terrorismebestrijding en Veiligheid *Cybersecuritybeeld Nederland (CSBN) 2019*, Ministerie van Veiligheid en Justitie, Den Haag 2019

European Commission 2016

European Commission, *Study on future trends and business models in communication services*, uitgevoerd door Ecorys en TNO voor EU DG Home, Brussels 2016

Concept

European Commission 2017

European Commission, *Eleventh progress report towards an effective and genuine Security Union*, 608 final, Brussel 2017

Europol 2019

Europol & Eurojust, *First report of the observatory function on encryption*, Den Haag 2019

Europol 2020

Europol & Eurojust, *Second report of the observatory function on encryption*, Den Haag 2020

Five Country Ministerial Statement 2018

Five country ministerial 2018, *Statement of principles on access to evidence and encryption*, <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018>, geraadpleegd op 21 februari 2020

Marr 2019

B. Marr, *What is Homomorphic Encryption? And Why Is It So Transformative?*, Forbes magazin, <https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/#2cf80c877e93>, geraadpleegd op 20 februari 2020, New York 2019

Gill et al 2018

L. Gill, T. Israel, C. Parsons, *Shining a light on the encryption debate: a Canadian Field Guide*, a joint research publication by Citizen Lab and the Canadian Internet Policy & Public Interest Clinic 2018

Internet Society 2017

Internet Society-Chatham House, *Roundtable on Encryption and Lawful Access*, te raadplegen op <https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access/>, geraadpleegd op 20 februari 2020, Reston Virginia 2017

Jaarverantwoording Politie 2018

Nationale Politie, *Jaarverantwoording: Midden in de samenleving*, Ministerie van Justitie en Veiligheid, Den Haag 2019

Kaye 2015

D. Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, A/HRC/29/32, 22 mei 2015

Kerr & Schneier 2018

O.S. Kerr, B. Schneier, *Encryption Workarounds*, 106 Georgetown Law Journal, 989, Washington D.C. 2018

Koops & Kosta 2018

B.J. Koops & E. Kosta, *Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"*, Computer law & security review, 34, pp. 890-900 2018

Concept

Levy & Robinson 2018

I. Levy, C. Robinson, *Principles for a More Informed Exceptional Access Debate*, <https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate>, geraadpleegd op 21 februari 2020, Lawfareblog 2018,

Lewis et al 2017

J.A. Lewis, D.E. Zheng, W.A. Carter, *The effect of Encryption on Lawful Access to Communications and Data*, Center for Strategic and International Studies, A report of the CSIS Technology Policy Program 2017

Manhattan District Attorney's Office 2015

Manhattan District Attorney's Office, *Report of the Manhattan district Attorney's office on smartphone encryption and public safety*, New York november 2015

Manhattan District Attorney's Office 2017

Manhattan District Attorney's Office, *Third report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, New York november 2017

Manhattan District Attorney's Office 2019

Manhattan District Attorney's Office, *Report of the Manhattan district Attorney's office on Smartphone encryption and Public Safety: An update tot he November 2018 report*, New York 2019

NAS 2018

National Academies of Sciences, Engineering, and Medicine, *Decrypting the encryption debate: A framework for decision makers*, Washington DC: The national academies 2018

NOS 2019a

Nederlandse Omroep Stichting, <https://nos.nl/artikel/2304627-vs-wil-uitstel-encryptieplannen-facebook.html>, geraadpleegd op 20 februari 2020, Hilversum 2019

NOS 2019b

Nederlandse Omroep Stichting, <https://nos.nl/nieuwsuur/artikel/2308847-minister-grapperhaus-wil-toegang-tot-chat-en-berichtendiensten.html>, geraadpleegd op 20 februari 2020, Hilversum 2019

Oerlemans 2012

J.J. Oerlemans, *Tappen en infiltreren*, Justitiële verkenningen, jrg. 38, nr. 3 2012

Politico 2019

Politico, https://www.politico.eu/pro/ferdinand-ferd-grapperhaus-dutch-minister-justice-security-urges-eu-action-to-fight-child-pornography-online/?utm_source=POLITICO.EU&utm_campaign=f8fa9c715a-EMAIL_CAMPAIGN_2019_12_04_10_11&utm_medium=email&utm_term=0_10959edeb5-f8fa9c715a-190433209, geraadpleegd 27 januari 2020, Washington 2019

Shah 2015

R. Shah, *Law enforcement and Data Privacy: A Forward-looking Approach*, The Yale Law Journal, vol. 125, No.2, pp. 543-558, New Haven Connecticut 2015

Concept

Soesanto 2018

S. Soesanto, *No Middle Ground: Moving on From The Crypto Wars*, European Council on Foreign Relations, policy brief, Brussels 2018

United Nations 2018

Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Encryption and Anonymity follow-up report*, Research paper 1/2018, juni 2018.

US Courts 2018

United States Courts, *Wiretap Report 2018*, <https://www.uscourts.gov/statistics-reports/wiretap-report-2018>, geraadpleegd op 20 februari 2020, Washington D.C. 2018

US Courts 2020

United States Courts, *Wiretap Reports*, <https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports>, geraadpleegd op 20 februari 2020, Washington D.C. 2020

US Justice departement 2019

United States Justice departement, <https://www.justice.gov/opa/press-release/file/1207081/download>, geraadpleegd op 20 februari 2020, Washington 2019

Veiligheidsmonitor 2017

Centraal Bureau voor de Statistiek, *Veiligheidsmonitor 2017*, Ministerie van Justitie en Veiligheid, Den Haag 2018

VI Justitie en Veiligheid – Rijksjaarsverslag 2018

Rijksjaarsverslag 2018 VI Justitie en veiligheid, <https://www.rijksoverheid.nl/documenten/jaarverslagen/2019/05/15/justitie-en-veiligheid-2018>, geraadpleegd op 20 februari 2020, Den Haag 2019

Walden 2018

I. Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' problem*, computer law & security review, 34, pp 901-907 2018

Wijk et al 2019

A. van Wijk, S. Dickie, T. van Ham, *Downlaoders van kinderporno; een literatuuronderzoek*, Beke Reeks, Ministerie van Justitie en Veiligheid, Den Haag 2019

10.2.e - BD/DRC/FO

Van: 10.2.e - BD/DRC/CV
Verzonden: maandag 26 april 2021 08:37
Aan: 10.2.e @bmi.bund.de
CC: 10.2.e n@minbuza.nl
Onderwerp: RE: Encryption - way forward

Hello 10.2.e

Here you find options for a meeting with the Commission for this week. We plan to meet for half an hour.

I could meet Wednesday between 15:00-16:00 and Thursday from 13:00-15:45 and 16:45-18:00.

What time would suit you?

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
.....

Van: 10.2.e
Verzonden: zaterdag 24 april 2021 11:57
Aan: 10.2.e - BD/DRC/CV
Onderwerp: RE: Encryption - way forward
Hoi 10.2.e

Voor mij komen de volgende tijden het best uit:

- Dinsdag 16:00-17:00
- Woensdag 10:00-11:00 en 15:00-16:00
- Donderdag 13:00-18:00

Hoe zit jij? Wil jij een tijd aan 10.2.e voorleggen?

Vriendelijke groet,

10.2.e

From: 10.2.e <10.2.e @ec.europa.eu>

Sent: vrijdag 23 april 2021 17:15

To: 10.2.e <10.2.e @minbuza.nl>

Cc: 10.2.e - BD/DRC/CV <10.2.e @minjenv.nl>; 10.2.e <10.2.e @ec.europa.eu>;

10.2.e <10.2.e @ec.europa.eu>

Subject: RE: Encryption - way forward

10.2.a, 10.2.e

10.2.e

10.2.e

From: 10.2.e <10.2.e@minbuza.nl>

Sent: Friday, April 23, 2021 12:52 PM

I am contacting you in relation to encryption. We had a nice chat about this in January and we have recently seen that the organized crime strategy of the Commission makes reference to this topic. The strategy mentions that the Commission will steer a process to analyze with the relevant stakeholders existing capabilities and approaches for lawful and targeted access to encrypted information in the context of criminal investigations and prosecutions. We are very interested in this process and would like to ask you whether it is possible for us to set up a meeting to hear more about your ideas. In the Netherlands we are currently also looking into concrete options to tackle these issues (legal and technical ways) and the possibility of setting up a national expert group on encryption. We therefore think it would be good idea to exchange thoughts with each other. We are also in very good contact with Germany on this topic and if you agree to having a meeting, we think it could really help our discussion if our German colleagues could join as well.

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.

Questionnaire A

Legislation and case-law (please provide the text of the relevant national provisions and references to the case-law)

Some of these questions build on the information set out in the section covering legal developments relating to encryption in the Reports of the Observatory Function on Encryption.¹ Please feel free to consider these reports in your answers.

1. Does your **national legislation**:

- a. authorise decryption of data (at rest or in transit, stored on the device of the suspect or with the electronic communications provider)?

- i. yes
- ii. no

If yes, under which conditions – please specify if the measure is limited to a list of offenses or to crimes of a specific threshold.

- b. authorise remote data capture (before the data is encrypted/after it is encrypted)?

- i. yes
- ii. no

If yes, under which conditions – please specify if it is limited to a list of offenses or to crimes of a specific threshold. Do you encounter legal issues in implementing such solutions, e.g. in the case of cross border investigations?

- c. oblige the electronic communication service providers to give access to the encryption keys or otherwise to cooperate with law enforcement authorities to assist them to decrypt the data?

- i. yes
- ii. no

If yes, under which conditions – please specify if the measure is limited to a list of offenses or to crimes of a specific threshold.

- d. oblige the suspect to give access to the encryption keys, passwords etc. or give access to the decrypted data?

- i. yes
- ii. no

- e. provide that technologies/ tools used are authorised for use only if targeted access to specific individuals or group of individuals is enabled?

- i. yes
- ii. no

- f. provide for further conditions/safeguards (oversight, error rate of the technology used etc) in order to ensure the fundamental rights of other users' communications data?

- i. yes
- ii. no

- g. provide for an obligation for the law enforcement authorities to disclose in court proceedings the tools/methods used to decrypt the data?

- i. yes

¹ First and second reports of the observatory function on encryption.

ii. no

2. Under your national law, is it possible to intercept/monitor application-level communication providers (such as , WhatsApp, Telegram, Signal, etc.)? If so, please specify what the legal basis is.
3. How do measures such as the ones under Q1 point a) - g)_and Q2 impact on the level of cybersecurity and protection of fundamental rights, such as privacy, protection of personal data, freedom of expression?
4. If there is no specific legislation on the decryption of encrypted data, is decryption allowed based on general legislative provisions (such as an Order to obtain the data)? Please specify which measures are allowed? (force the providers to give access to the encryption keys / force the suspect to give access to passwords, keys etc. or give access to data in a decrypted form / deploy other methods, such as brute force attack, access to the data before encryption or after decryption / other)
5. Considering the impact on fundamental rights and cybersecurity, did you consult your national data protection authority, other bodies with a remit in fundamental rights and/or cybersecurity on measures relating to access by law enforcement / judicial authorities to decrypted data on adopted or planned measures? What was the opinion of those bodies? Did you follow this opinion fully or partially?
6. Is there **case-law** on the compliance of your national legislation or applied measures relating to access to data in a decrypted form with fundamental rights, i.e. the right to confidentiality of communications, the right to protection of personal data, the right to freedom of expression, the right to assembly, the right to not incriminate oneself? If so, please summarise
7. Is there **case-law** on the admissibility of decrypted data in criminal proceedings? If so, please summarise
8. Does your legal framework allow you to make tools and services available to other Member States?
 - a. yes (please specify the conditions)
 - b. no
9. Does your legal framework allow you to use tools and services offered by Europol e.g. to obtain access to data at the end points (remote data stored in the sender/recipient's devices, captured before it is encrypted/after it is encrypted)?
 - a. yes (please specify the conditions)
 - b. no
10. Does your legal framework allow you to use tools and services offered by another Member State?
 - a. yes (please specify the conditions)
 - b. no (please provide reasons)
11. Are there other legal issues that you would like to raise in relation to encryption and the possible approach to these issues (e.g. encryption challenges in the context of evolving technologies such as 5G)? Please share any relevant national experience or considerations arising from your practice that need to be taken into account.

12. Does your legal framework provide public authorities with the ability to use investigative techniques that rely on the exploitation of vulnerabilities?
- yes - provide references to the relevant legal provisions
 - no
13. In your view, would legislative measures that aim at obtaining decrypted data from seized devices adopted at EU level in the future provide added value?
- no EU measures are necessary
 - yes such measures would provide added value
- Please give reasons for your answer, including where appropriate what should be covered under EU legislation.
14. In your view, do legal measures to facilitate lawful access to encrypted data in motion need to be adopted at EU level in the future?
- yes
 - no
- Please give reasons for your answer, including where appropriate what should be covered under EU legislation.
15. In your view, would there be added value in measures at EU level to allow lawful access to data at the end-points (i.e. remote data stored on the sender and/or recipient's devices)?
- yes
 - no
- Please give reasons for your answer, including where appropriate what should be covered under EU legislation.

Questionnaire B

Operational practices and needs, the latter also covering quantitative data, where available

Impact on investigation

1. What proportion of criminal investigations require access to encrypted data [any type of encryption]? Please specify the types of offences and indicate in what proportion of these investigations, the data has been successfully decrypted?
2. How often do you encounter **end-to-end encryption** in your operational activities and while gathering electronic evidence/evidence in cyber space in the course of criminal procedures?
 - a. almost always (> 75%)
 - b. in many cases (upward of 50%)
 - c. in some cases (0% - 50%)
 - d. never

Please provide other relevant information including possible statistical and anecdotal information that illustrates your answer:

If you have different experiences in cross-border cases, please specify here:

3. How would you assess the impact of end-to-end encryption on investigations?
 - a. significant number of investigations (> 75%) are stopped or delayed due to encryption (please provide an estimate if possible)
 - b. some investigations (upward of 50%) are stopped or delayed due to encryption (please provide an estimate if possible)
 - c. a limited number of investigations (less than 50%) are stopped or delayed due to encryption (please provide an estimate if possible)
 - d. no investigation is stopped or delayed due to encryption

Please provide other relevant information (eg. no access to the keys) including possible statistical and anecdotal information that illustrates your answer:

Decryption Capabilities

4. How are your current decryption capacities deployed?
 - a. centralised
 - b. distributed
 - c. other, please specify
5. What kind of decryption challenges is the service in charge of decryption from Q4 addressing?
 - a. data at rest only
 - b. data in motion only

- c. both
6. What kind of encryption modalities are you faced with during investigations? For each modality, please provide a technical description of the practices used.
 - a. commercial solutions, please provide details
 - b. open-source solutions, please provide details
 - c. new solutions developed by criminals, please provide details
 7. How effective are alternative methods to tackling encryption, such as the use of communications metadata?
 8. How do you assess the effectiveness of possible obligations on mainstream providers to give access to decrypted data given the existence of other possibilities to encrypt data, such as use of home-grown solutions by tech-savvy criminals or use of services offered by non-compliant service providers?

Access to data on seized devices

9. What main operational and practical issues do you typically encounter when seizing encrypted evidence on devices including computers, tablets, smartphones and decrypting it?
 - a. skills
 - b. financial
 - c. technical capability
 - d. others

Describe in more detail the issues identified above:

If you have different experiences in cross-border cases, please specify:

10. Europol offers Member States support to decrypt data on devices seized during criminal investigations through a decryption platform (as announced in the 11th Security Union Progress Report²). You may select more than one answer:
 - a. we are not aware of this facility
 - b. we are aware that the decryption platform exists but have not yet used it
 - c. we have used/are making use of the platform
 - d. our demand for the use of the platform is higher than the capacity allocated to us
 - e. in order for the platform to remain a useful resource it must be constantly developed to keep abreast of technical developments

Please provide further comments:

11. Which practical measures could provide added value to help law enforcement overcome the challenges posed by encryption in criminal investigations?

² https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

- a. not needed
- b. improve capabilities (e. g. foster the development of tools and services for police and judicial authorities at MS and/or EU level)
- c. improve technical expertise at EU level
- d. improve exchange of information and best practices between police and judicial authorities
- e. Improve and expand on existing trainings for law enforcement and the judiciary

Please give examples:

Lawful access to data in motion

12. What are the main practical/operational issues typically encountered under national lawful interception frameworks while intercepting/monitoring encrypted data in motion³ in order to obtain decrypted data?
- a. skills
 - b. financial
 - c. technical capability
 - d. others

Describe in more detail the issues identified above:
--

13. Which practical measures could provide added value to help law enforcement overcome the challenges encountered while intercepting/monitoring encrypted data flow?
- a. not needed
 - b. improve capabilities (e. g. foster the development of tools and services for police and judicial authorities at MS and/or EU level)
 - c. improve technical expertise at EU level
 - d. improve exchange of information and best practices between police and judicial authorities, including training

Please give examples:

Lawful access to data on endpoints (remote data capture before it is encrypted)

14. What main issues do you typically encounter to implement such solutions (if national legal framework allows for it)?
- a. skills
 - b. financial
 - c. technical capability
 - d. others

Describe in more detail the issues identified above:
--

³ The legally sanctioned official access to private communications intercepted whilst transiting between the sender and recipient e.g. telephone calls, e-mails and text messages. Traditionally the network operator or service provider gives law enforcement officials access. With increasing deployment of end-to-end encryption in electronic communications many service providers no longer have the possibility to support law enforcement with this type of lawful access.

If you have different experiences in cross-border cases, please specify:

15. In your view, which practical measures in this regard need to be adopted?
- not needed
 - improve capabilities (e. g. foster the development of tools and services for police and judicial authorities at MS and/or EU level)
 - improve technical expertise at EU level
 - improve exchange of information and best practices between police and judicial authorities, including training

Please give examples:

16. Are there other operational issues that you would like to raise in relation to encryption and the possible approach to these issues (e.g. encryption challenges in the context of evolving technologies such as 5G)? Please share any relevant national experience or considerations arising from your practice that need to be taken into account.
17. If encryption is limited to enable access by law enforcement / judicial authorities, how can strong encryption be preserved to ensure cybersecurity (e.g. protection against cybercrime) and the protection of fundamental rights, including in the context of international data transfers?
18. Which actors are associated to the debate on encryption in your Member State and how do you ensure an inclusive approach?

Innovative investigative capabilities⁴

The following questions explore the dimension of innovative investigative capabilities coupled with solid coordination, as underlined by the November 2020 Council Resolution⁵ on Encryption. They stem from experience gained during recent investigation cases that have demonstrated the usefulness of taking advantage, in a targeted way, of existing vulnerabilities in order to overcome the issue of encrypted data.

19. Have you implemented a dedicated mechanism, including a 'vulnerability equities process'⁶ to manage the use (from exploitation to disclosure) of vulnerabilities?
- yes, please specify the mechanism and the list of stakeholders involved
 - no
20. Do you apply this vulnerability management strategy to:
- the acquisition of data at rest?
 - the acquisition of data in motion?
 - both?

⁴ These are marked as sensitive questions.

⁵ <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf>

⁶ A vulnerability equities process serves the purpose of assessing the risk associated with exploiting any particular vulnerability rather than disclosing the vulnerability to the affected vendor

21. What operational model do you apply to exploit vulnerabilities in criminal investigations? Please describe.
22. Does the exploitation of the vulnerabilities (such as payload development, vector, control, etc.) rely on:
 - a. internal support?
 - b. external support - private provider?
 - c. external support - public provider?
23. Which parts of your operational model are currently only available outside of the EU, and would need to be developed in future within the EU?
24. Which oversight mechanisms are applied to the management of these innovative investigative capabilities?
 - a. judicial authority oversight
 - b. parliamentary oversight
 - c. other, please specify
25. Please describe the main elements of these oversight mechanisms?
26. Do you publish annual/regular reports on the use of such techniques?
 - a. yes, please provide references
 - b. no
27. Do you agree to the proposal that, in case the Commission receives a request for access to documents regarding these questionnaires, the answers to the questions marked as sensitive would not be disclosed?
 - a. yes
 - b. no

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

Country	Participant, organisation
AT	10.2.e , Ministry of Interior
	10.2.e , Ministry of Justice
	10.2.e , Federal Chancellery
BE	10.2.e
	Court of Appeal in Antwerp & 10.2.e
	public prosecutor's office on cybercrime
	B4
	10.2.e
	federal police
	10.2.e federal public service justice
BG	10.2.e
	Ministry of Justice
	10.2.e for National Security
	10.2.e
	Ministry of Interior
CY	10.2.e Councillor
CZ	10.2.e Justice and Home Affairs Unit
	10.2.e Department of the Supreme
	Prosecutor's Office
	10.2.a, 10.2.e
	10.2.e , National Organized Crime Agency CPIS
DE	10.2.e Unit Justice and Consumer Protection,
	Permanent Representation of Germany to the EU
	10.2.e Cybersecurity, Federal Ministry of the
	Interior;
	10.2.e Criminal Procedural Law, Federal
	Ministry of Justice and Consumer protection
DK	10.2.e
	10.2.e , law enforcement authorities
	10.2.e
EE	10.2.e , Ministry of Justice
	10.2.e
	10.2.e
EL	10.2.e , Public Prosecutor at Athens Court of
	Appeal
	10.2.e , Police Captain
	10.2.e , Police Second Lieutenant
	10.2.e Associate Councilor (Judge) at the Greek
	Council of State, 10.2.e
	)
	10.2.e Department of ICT
	Projects' Planning and Development of Hellenic Ministry of Justice

	10.2.e	Department of Operation and Support of Information Systems of Hellenic Ministry of Justice
ES	10.2.e	Home Affairs Counsellor
	10.2.e	
	10.2.e	Permanent Representation of Spain
FI	10.2.e	
	10.2.e	
	10.2.e	Ministry of the Interior
FR	10.2.e	
	10.2.e	
	10.2.e	l'Union-Secrétariat général des affaires européennes
HR	10.2.e	, Permanent Representation
	10.2.e	Department, Ministry of the Interior
	10.2.e	, Permanent Representation
HU	10.2.e	
	10.2.e	
	10.2.a, 10.2.e, 10.2.g	
	10.2.e	, National Police Headquarters
	10.2.a, 10.2.e, 10.2.g	
IE	10.2.e	, Department of Justice
	10.2.e	
	10.2.e	
	10.2.e	, Permanent Representation of Italy to the EU
IT	10.2.e	, Italian Ministry of the Interior
	10.2.e	Italian Ministry of the Interior
LT	10.2.e	, Prosecutor General's Office
	10.2.a, 10.2.e, 10.2.g	
	10.2.e	
LU	10.2.a, 10.2.e, 10.2.g	
LV	10.2.a, 10.2.e, 10.2.g	
	10.2.a, 10.2.e, 10.2.g	
	10.2.e	, Ministry of Foreign Affairs
MT	10.2.a, 10.2.e, 10.2.g	
	10.2.a, 10.2.e, 10.2.g	
NL	10.2.e	
	10.2.e	
	10.2.e	, Justice and Home Affairs Counsellor
PL	10.2.e	, Justice and Home Affairs Unit

	10.2.e	
		and Home Affairs Section
PT	10.2.a, 10.2.e, 10.2.g	
	10.2.a, 10.2.e, 10.2.g	
	10.2.e	Ministry of Foreign Affairs
	10.2.e	(COSI COSI-SG IXIM)
	10.2.e	
RO	10.2.e	Home Affairs
	10.2.e	
SE	10.2.e	Perm Rep
	10.2.e	, Ministry of
	Justice	
	10.2.e	Ministry of
	Justice.	
SI	10.2.e	
		Ministry of Justice of the Republic of Slovenia
	10.2.e	Ministry of Justice of the Republic of Slovenia
	10.2.e	, Ministry of Justice of the Republic of Slovenia
SK	10.2.e	Ministry of Interior

10.2.e - BD/DRC/FO

Van: 10.2.e @minbuza.nl>
Verzonden: dinsdag 25 mei 2021 16:52
Aan: 10.2.e
CC: 10.2.e @minbuza.nl; 10.2.e BD/DEIA/EU;
10.2.e - BD/DRC/CV
Onderwerp: Flits CIE vergadering encryptie 25 mei 2021

Hoi allen,

Op 25 mei 2021 heeft de Commissie een vergadering georganiseerd om de plannen op het gebied van encryptie toe te lichten:

- **Doel:** CIE verwijst 10.2.a

[Redacted content]

- **Proces:** CIE heeft 10.2.a

[Redacted content]

- **Volgende stappen:** CIE zal 10.2.a

[Redacted content]

Vriendelijke groet,

10.2.e



10.2.e

Criminal justice, data protection, e-Justice

Permanent Representation of the
Kingdom of the Netherlands to the European Union
Avenue de Cortenbergh 4-10
1040 Brussels, Belgium

M: 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.



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
T 10.2.e
E 10.2.e @minjenv.nl

Datum
22 juni 2021

Projectnaam
Encryptie

Ons kenmerk
3399620

nota

Encryptie questionnaire Europese Commissie

1 Doel nota

Accordering van de verzending van de beantwoording op de questionnaire over de inventarisatie naar mogelijkheden voor rechtmatige toegang tot versleutelde informatie (encryptie).

De Europese Commissie heeft een questionnaire verstuurd over wetgeving en jurisprudentie rondom rechtmatige toegang tot bewijs en vraagt een appreciatie op diverse mogelijkheden die de Commissie kan onderzoeken. Een tweede deel van de questionnaire dat gaat over de aard van de problematiek wordt later beantwoord.

2 Aanleiding, gevraagde actie(s) en advies

De Commissie concentreert zich op vier onderwerpen: interceptie, end-point toegang (rechtmatige hacken, CCIII), toegang tot inbeslaggenomen apparatuur, en het decryptiebevel. Voor het decryptiebevel wordt een feitelijke weergave van wetgeving en jurisprudentie gegeven.

Naast een uiteenzetting van het bestaand juridisch kader vraagt de Commissie ook naar de toegevoegde waarde van juridische instrumenten op EU-niveau. In lijn met het standpunt dat we tot nu toe hebben uitgedragen roept Nederland op om geen mogelijkheid in de inventarisatie buiten beschouwing te laten.

Inzake de vraag over toegang tot inbeslaggenomen apparaten (vraag 13) wordt geantwoord dat Europese wetgeving toegevoegde waarde zou hebben zodat internationale samenwerking met deze bedrijven kan worden verbeterd en meer documentatie kan komen over producten, zodat de opsporing dit niet zelf hoeft te 'reverse engineeren'. Dit is het achteraf achterhalen hoe een product technisch in elkaar zit nadat het product reeds is opgeleverd. Dit raakt voornamelijk het werk van het NFI.

Inzake de vraag over mogelijkheden voor interceptie via OTT-communicatiediensten (vraag 14) wordt in beginsel positief geantwoord op de vraag of Europese wetgeving toegevoegde waarde zou hebben. Echter, de voor- en nadelen van deze mogelijkheid moeten goed worden onderzocht. Ook wordt een voorbehoud gemaakt inzake de reikwijdte van Europese regelgeving. Wellicht biedt dit EU-traject al voldoende mogelijkheden om uitvoering te geven aan onze nationale interceptiebevoegdheid en zou Europese regelgeving alleen nodig zijn voor de handhaving van een bevel. Deze inschatting kan pas later in het proces worden gemaakt.

Inzake de vraag over mogelijkheden voor end-point toegang (vraag 15, rechtmatig hacken) wordt geen direct antwoord gegeven. De gevolgen voor de markt van binnendringsoftware, onbekende kwetsbaarheden, en gevaar voor geautomatiseerde systemen bij onzorgvuldige inzetten worden genoemd. Daarbovenop is betrouwbare en voorspelbare toegang wenselijk, bij een hack weet je niet of/wanneer en voor hoe lang je toegang hebt. Echter, in deze inventarisatie zouden geen mogelijkheden moeten worden uitgesloten.

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

Datum
22 juni 2021

Ons kenmerk
3399620

3 Toelichting op het advies

Nvt.

4 Dilemma's

Nvt.

5 Politieke en bestuurlijke context

Afgezien van de vragen 13, 14 en 15 zijn de vragen en beantwoording relatief feitelijk van aard. Inzake de interceptie van OTT-communicatiediensten wordt de lijn vastgehouden dat wetgeving in beginsel een toegevoegde waarde voor de opsporing hebben, maar de voor- en nadelen goed moeten worden onderzocht. Standpunten op de toegang tot inbeslaggenomen apparatuur en end-point toegang zijn nieuw. Dit laatste kan bijvoorbeeld ook resulteren in de oprichting van een unit bij Europol die op verzoek van lidstaten hacks kan zetten. In de beantwoording wordt gewezen op de risico's rondom de markt van binnendringsoftware, onbekende kwetsbaarheden en nevenschade voor apparatuur, maar wordt niets uitgesloten. Toegang tot inbeslaggenomen apparatuur lijkt in dit verband de relatief minst vergaande mogelijkheid. Als bijlage bij de questionnaire wordt het kabinetsstandpunt 2016 meegezonden.

6 Communicatie

Nvt.

7 Afstemming

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

8 Bijlagen

- Questionnaire A
- Cabinet position on encryption 2016

10.2.e - BD/DRC/FO

Van: 10.2.e <10.2.e@minbuza.nl>
Verzonden: woensdag 30 juni 2021 16:26
Aan: 10.2.g @ec.europa.eu
CC: 10.2.e - BD/DEIA/EU; 10.2.e - BD/DRC/CV; 10.2.e
10.2.e 10.2.e
Onderwerp: RE: Questionnaires on encryption_kind reminder to reply by 25/06
Bijlagen: Questionnaire A1.docx; nl-cabinet-encryption-position.pdf

Dear colleagues,

With apologies for the delay, please find attached the reply of the Netherlands to the first questionnaire. I also attach for your information our standing Government position on encryption. Should you have any questions, please don't hesitate to contact us.

Best wishes,

10.2.e

10.2.e

Criminal justice, data protection, e-Justice

Permanent Representation of the
Kingdom of the Netherlands to the European Union
Avenue de Cortenbergh 4-10
1040 Brussels, Belgium



M: 10.2.e
Email: 10.2.e @minbuza.nl

From: 10.2.g @ec.europa.eu
Sent: maandag 21 juni 2021 14:01
To: 10.2.e, 10.2.g

10.2.e, 10.2.g

Cc: 10.2.g

@ec.europa.eu

Subject: Questionnaires on encryption_kind reminder to reply by 25/06

10.2.a

From: SG SECURITY UNION <10.2.g @ec.europa.eu>

Sent: Thursday, June 3, 2021 3:09 PM

To: 10.2.e, 10.2.g