Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2345

Vragen van de leden **Van Ginneken**, **Dekker-Abdulaziz** (beiden D66) en **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *de beantwoording van de schriftelijke vragen inzake de vacature «Senior beleidsmedewerker interceptie en digitale opsporing» bij het Ministerie van Justitie en Veiligheid* (ingezonden 29 maart 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 6 april 2022).

Vraag 1
Wat vindt u van de stelling dat een interessante focus van onderzoek zou kunnen zijn dat de inlichtingen-en veiligheidsdiensten effectief hun wettelijk taak kunnen blijven uitvoeren zonder een achterdeur die versleutelde communicatie via OTT(over-the-top)-diensten onveilig maakt?[1]

Antwoord 1
Ik kan niet voor de inlichtingen- en veiligheidsdiensten (IenV-diensten) spreken, deze diensten vallen onder de portefeuille van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie. Met deze diensten wordt wel goed samengewerkt. Binnen de termijn die in vraag 6 is gesteld was het niet mogelijk om bij vragen 1 en 4 de toepassing op de IenV-diensten na afstemming met hen toe te voegen, aangezien het opsporings- en IenV domein verschillend zijn gereguleerd.
Op dit moment wordt onderzocht hoe de uitdagingen in de opsporing als gevolg van encryptie kunnen worden geadresseerd. Er is een inventarisatie gaande om de technische mogelijkheden voor rechtmatige toegang tot versleutelde informatie te onderzoeken, om vervolgens de voor- en nadelen van die mogelijkheden voor alle betrokken (zwaarwegende) belangen te analyseren.
Het doel van deze inventarisatie is om geïnformeerde en zorgvuldige besluitvorming mogelijk te maken door dit kabinet en uw Kamer. Indien tot wetgeving wordt besloten wordt een duidelijke wettelijke basis voorgesteld die via een transparant wetgevingsproces aan uw Kamer wordt voorgelegd. Of en hoe dit exact vorm krijgt is afhankelijk van het EU-traject dat nu loopt. Een technische oplossing moet adequaat en evenwichtig zijn. Belangrijk hierbij zijn de principes van proportionaliteit en subsidiariteit. Ten eerste moet

[1] Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 2095

ah-tk-20212022-2345
ISSN 0921 - 7398
's-Gravenhage 2022

de technische oplossing proportioneel zijn en bijdragen aan een veilige maatschappij of de bescherming van kwetsbaren in onze samenleving. Het middel moet aanvaardbaar zijn, dit betekent dat er geen onverantwoorde beslissingen worden genomen wanneer het de (digitale) veiligheid van burgers, het bedrijfsleven en de overheid aangaat. Deze inventarisatie zal ik niet vooraf beperken, omdat alle mogelijkheden eerst in kaart gebracht moeten zijn voordat een zorgvuldige keuze voor eventuele maatregelen kan worden genomen.

Vraag 2
Zou u het onderzoek kunnen verbreden naar het onderzoeken van een grotere dreiging voor onze digitale veiligheid en verdienvermogen, namelijk het doorbreken van veilige versleutelde communicatie door nieuwe technologie zoals kwantumtechnologie in de nabije toekomst?

Antwoord 2
Zie het antwoord op vraag 3.

Vraag 3
Bent u het met de partijen eens dat het kwantumproof maken van onze communicatie en netwerken een urgente uitdaging is die nu moet worden aangepakt?

Antwoord 3
Het effect van kwantumtechnologie op de veiligheid van versleutelde communicatie past niet binnen de reikwijdte van de inventarisatie naar mogelijkheden en voor- en nadelen van de rechtmatige toegang tot versleutelde informatie. Eventuele dreigingen voor versleutelde communicatie is niet de focus van de inventarisatie die is gestart. Gegeven de complexiteit van de inventarisatie die in deze beantwoording wordt geschetst bestaat de voorkeur om de focus te behouden tot mogelijkheden voor rechtmatige toegang tot versleuteld bewijs.
Het NCSC adviseert organisaties nu al na te denken over de gevolgen van de komst van de kwantumcomputer voor hun organisatie en een actieplan op te stellen dat duidelijk maakt binnen welke tijdlijn er maatregelen genomen moeten worden.[2] Gegevens die vandaag al bestaan en die ook na de komst van kwantumcomputers beschermd moeten blijven, moeten namelijk nu al aanvullend worden beschermd.
Versleuteling is van belang voor de veiligheid. Daarnaast is rechtmatige toegang tot versleutelde communicatie is ook van belang voor de veiligheid van de maatschappij en burgers doordat illegale inhoud en activiteiten beter worden onderkend, onderschept en verwijderd, en slachtofferschap wordt voorkomen of geminimaliseerd, ook in het digitale domein.
In mijn beantwoording leest u dat in de inventarisatie verschillende grote belangen worden meegewogen. Bijvoorbeeld, cybersecurity en de bescherming van fundamentele rechten zijn zwaarwegende onderdelen die worden meegenomen in afwegingen of maatregelen proportioneel zijn. Dit is ook vice versa van belang. Ook bij toekomstige technologieën vind ik een integrale benadering belangrijk en is het goed dat ook het opsporingsbelang wordt meegenomen.

Vraag 4
Ziet u interceptie van versleutelde communicatie via OTT-diensten als een nieuwe bevoegdheid voor de inlichtingen-en veiligheidsdiensten? Op welk artikel in de Wet op de inlichtingen-en veiligheidsdiensten 2017 baseert u zich?

Antwoord 4
In lijn met de beantwoording op vraag 1 relateer ik deze vraag aan de wettelijke bevoegdheden van de opsporingsdiensten en het Openbaar Ministerie. Hierbij moet onderscheid worden gemaakt tussen het Wetboek van Strafvordering (Sv) en de Telecommunicatiewet.

---

[2] Factsheet Postkwantumcryptografie | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl)

De in hoofdstuk 13 Telecommunicatiewet en onderliggende lagere regelgeving vastgelegde medewerkings- en ontsleutelverplichtingen zijn beperkt tot (klassieke) aanbieders van openbare telecommunicatiediensten en –netwerken. Aanbieders van OTT-communicatiediensten – nummeronafhankelijke interpersoonlijke communicatiedienten volgens de definitie van de Telecommunicatiewet – vallen niet onder deze verplichtingen. Ondanks het feit dat het de officier van justitie is toegestaan op basis van artikel 126m jo. 138g Sv, na een daartoe verkregen machtiging van de rechter-commissaris, een opsporingsambtenaar te bevelen versleutelde communicatie via OTT-communicatiediensten af te tappen kan.vanwege de ontbrekende medewerkings- en ontsleutelverplichtingen geen inzicht worden verkregen in de inhoud van de versleutelde communicatie.

Vraag 5
Wat is de huidige stand van zaken van het in de beantwoording genoemde EU traject met betrekking tot veilige digitale communicatie?

Antwoord 5
De Europese Commissie beraadt zich op dit moment op een «way forward» voor de inventarisatie naar rechtmatige toegang tot versleuteld bewijs en deze wordt in 2022 gepubliceerd. Dit doet zij op basis van beantwoorde vragenlijsten en de Commissie heeft enkele ambtelijke gesprekken georganiseerd. Uiteraard zal ik uw Kamer over de uitkomsten informeren.

Vraag 6
Kunt u deze vragen afzonderlijk beantwoorden voorafgaand het commissiedebat online veiligheid en cybersecurity op 7 april 2022?

Antwoord 6
Ja.