Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2020–2021

35 602 EU-voorstel: Commissiemededeling over de EU-strategie voor de Veiligheidsunie (COM(2020)605)[1]

B

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 3 november 2020

De leden van de vaste commissies voor Immigratie & Asiel/JBZ-Raad[2] en voor Justitie en Veiligheid[3] hebben kennisgenomen van de op 24 juli 2020 door de Europese Commissie gepubliceerde Commissiemededeling: De EU-strategie voor de veiligheidsunie[4] en het bijbehorende BNC-fiche. Naar aanleiding hiervan hebben deze leden op 14 oktober 2020 een brief gestuurd aan de Minister van Justitie en Veiligheid met vragen van de GroenLinks-fractie.

De Minister heeft op 3 november 2020 gereageerd.

De commissies brengen bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier voor dit verslag,
Van Dooren

---

[1] Zie dossier E200012 op www.europapoort.nl

[2] Samenstelling **Immigratie en Asiel/JBZ-Raad**:
Kox (SP), Faber-van de Klashorst (PVV), (voorzitter), De Boer (GL), Van Dijk (SGP), Van Hattem (PVV), Jorritsma-Lebbink (VVD), Nooren (PvdA), Oomen-Ruijten (CDA), Rombouts (CDA), Stienen (D66), Teunissen (PvdD), Van Rooijen (50PLUS), Adriaansens (VVD), De Blécourt-Wouterse (VVD), Cliteur (FVD), Doornhof (CDA), Gerbrandy (OSF), Huizinga-Heringa (CU), Karimi (GL), Van Pareren (FVD), (ondervoorzitter), Veldhoen (GL), Vos (PvdA), De Vries (Fractie-Otten), Berkhout (FVD) en Keunen (VVD).

[3] Samenstelling **Justitie en Veiligheid**:
Backer (D66), De Boer (GL), (voorzitter), Van Dijk (SGP), Van Hattem (PVV), Nooren (PvdA), Rombouts (CDA), Bikker (CU), Baay-Timmerman (50PLUS), Adriaansens (VVD), Arbouw (VVD), Bezaan (PVV), De Blécourt-Wouterse (VVD), Cliteur (FVD), Dittrich (D66), Doornhof (D66), Gerbrandy (OSF), Janssen (SP), Karimi (GL), Meijer (VVD), Nicolaï (PvdD), Otten (Fractie-Otten), (ondervoorzitter), Van Pareren (FVD), Recourt (PvdA), Rietkerk (CDA), Veldhoen (GL) en Van Wely (FVD).

[4] COM(2020)605 final.

kst-35602-B
ISSN 0921 - 7371
's-Gravenhage 2020

BRIEF VAN DE VOORZITTERS VAN DE VASTE COMMISSIES VOOR IMMIGRATIE EN ASIEL/JBZ-RAAD EN VOOR JUSTITIE EN VEILIGHEID

Aan de Minister van Justitie en Veiligheid

Den Haag, 14 oktober 2020

De leden van de vaste commissies voor Immigratie & Asiel/JBZ-Raad en voor Justitie en Veiligheid van de Eerste Kamer hebben met belangstelling kennisgenomen van de op 24 juli 2020 door de Europese Commissie gepubliceerde Commissiemededeling: De EU-strategie voor de veiligheidsunie[5] en het bijbehorende BNC-fiche. De leden van de GroenLinks-fractie wensen de regering over deze mededeling enkele vragen te stellen.

De leden van de GroenLinks-fractie onderschrijven de doelen en begrijpen de aanpak van de Europese Commissie omtrent het aanpakken van mensenhandel, cybercriminaliteit, georganiseerde misdaad en pogingen om radicalisering tegen te gaan. De keuze van de Europese Commissie om een sterke focus te leggen op het onderwerp digitalisering in relatie tot veiligheid en criminaliteit onderschrijven deze leden evenzeer. Aan het slot van deze brief treft u enkele vragen op dit punt. Eerst zouden de aan het woord zijnde leden graag een fundamenteler gesprek aangaan met de regering over de gepresenteerde EU-strategie voor de veiligheidsunie.

De leden van de GroenLinks-fractie vragen zich af wat er zou moeten gebeuren op klimatologisch gebied voordat de gevolgen van klimaatverandering een integraal onderdeel zouden moeten vormen van de EU-strategie voor de veiligheidsunie? Klimaatverandering wordt nu genoemd in de derde zin van de inleiding, maar verder in zijn geheel niet. Hoe kijkt de regering hier tegenaan?

De Europese Commissie schrijft: «*Terrorisme, georganiseerde criminaliteit, drugshandel en mensenhandel vormen rechtstreekse bedreigingen voor de burgers en onze Europese manier van leven*»[6]. De Europese Commissie schrijft dat er sprake is van een neerwaarts spiraal van aanslagen. Kan de regering de cijfers opvragen bij de Europese Commissie van deze neerwaartse spiraal in de laatste tien jaar?
De leden steunen de Europese Commissie inzake maatregelen om de publieke ruimte in steden veiliger te maken door objecten slim te plaatsen in de publieke ruimte, zodat er minder met voertuigen aanslagen kunnen worden gepleegd. Deelt de regering deze visie van de Europese Commissie en is zij het met de leden van de GroenLinks-fractie en de Europese Commissie eens dat plekken waar auto's en vrachtwagen niet kunnen komen, veiligere publieke ruimten worden? Weet de regering wat de Europese Commissie op dit punt concreet wil doen en gaat de regering hier proactief op handelen, ook gelet op de rapporten van de NCTV? Graag verzoeken de aan het woord zijnde leden om een reactie van de regering op het gebied van veiligheid voor burgers en onze manier van leven, en een reflectie over de voordelen van deze integrale aanpak voor de publieke ruimte.

Zou het volgens de regering kunnen zijn dat de Europese Commissie ten onterechte klimaatverandering níet als rechtstreekse dan wel indirecte bedreiging ziet? Is het immers niet zo, dat zowel het aantal slachtoffers, als de impact op onze manier van leven door klimaatverandering veel

[5] COM(2020)605 final.
[6] COM(2020)605 final, p. 1.

groter is dan dat terrorisme in potentie is? De genoemde leden onderschrijven de inspanningen van de Europese Commissie op het terrein van terrorisme en het bestrijden van terroristische inhoud op internet ten zeerste. De Europese Commissie schrijft: «*De lidstaten behouden de primaire verantwoordelijkheid voor de bestrijding van terrorisme en radicalisering*»[7]. Is de regering van mening dat het klimaat- en pandemievraagstuk niet bij uitstek een bij de EU passend vraagstuk betreft, ook wat betreft veiligheid? En is de regering bereid hierover met de Europese Commissie in gesprek te treden?

«*De COVID-19-crisis heeft er ook toe geleid dat wij onze notie van veiligheidsbedreigingen en de bijbehorende beleidsmaatregelen hebben herzien*»[8], aldus de Europese Commissie. In totaal schrijft de Europese Commissie negen keer over COVID-19 in haar strategie. Negen keer is dit in relatie tot het digitale domein. Zo schrijft de Europese Commissie zowel over de oplossingen om door te kunnen blijven werken vanuit thuis dankzij technologie, waardoor men tegelijkertijd digitaal kwetsbaarder wordt voor desinformatie, als over pogingen om het politiek narratief te beïnvloeden en over de online zwendel in gezondheidsproducten. Hoe beoordeelt de regering dit en weet de regering of COVID-19 nog tot andere inzichten heeft geleid in de notie qua veiligheidsbedreigingen en mogelijk bijbehorende beleidsmaatregelen? Zo ja, zou de regering deze inzichten willen delen, inclusief de *lessons learned*? Zo niet, zou de regering deze inzichten bij de Europese Commissie willen opvragen?

Weet de regering of de Europese Commissie de conclusie trekt dat COVID-19 ook een gevolg is ván onze manier van leven, of dat straks een ander virus dit kan zijn? Zo ja, hoe verhouden pandemieën zich dan tot veiligheidsvraagstukken? En welke conclusies op veiligheidsgebied moet je verbinden aan de vaststelling dat «onze manier van leven» een bedreiging vormt voor «onze manier van het leven?» Zo nee, zou de regering dit bij de Europese Commissie willen bepleiten?

De leden van de GroenLinks-fractie constateren dat de Europese Commissie eerder bereid is haar notie van veiligheidsbedreigingen en de bijbehorende beleidsmaatregelen te herzien. Is de regering in dat licht bereid het voorgaande omtrent klimaatverandering en COVID-19 te adresseren bij de Europese Commissie?

Tot slot hebben de leden van de GroenLinks-fractie nog de volgende vragen:
- Welke drukmiddelen zijn er ten opzichte van de private sector om relevante informatie te verkrijgen in het kader van de bestrijding van cybercriminaliteit, witwassen, georganiseerde misdaad, die deze bedrijven vanuit concurrentieoverwegingen niet willen delen?
- Kan de regering bij de Europese Commissie opvragen om inzichtelijk te maken op welke wijze artificiële intelligentie (AI) wordt toegepast binnen de Europese Unie om veiligheidsissues te adresseren? Zowel door overheden als bedrijven? Hoe zit het met digitale aanvallen vanuit de Verenigde Staten in de laatste tien jaar?
- Welke dreiging gaat er uit van drones die vanaf de andere kant van de wereld dankzij 5G kunnen worden bestuurd? Heeft de regering hier analyses van gemaakt?
- De Europese Commissie schrijft *«Huishoudens, banken, financiële diensten en ondernemingen (met name in het midden- en kleinbedrijf) worden zwaar getroffen door cyberaanvallen»*.[9] Weet de regering hoe

[7] COM(2020)605 final, p. 19.
[8] COM(2020)605 final, p. 1.
[9] COM(2020)605 final, p. 3.

groot deze schade is? Is hier onderzoek naar gedaan? Welke sectoren worden het meeste getroffen?

De leden van de vaste commissies voor Immigratie & Asiel/JBZ-Raad en voor Justitie en Veiligheid zien uw beantwoording met belangstelling tegemoet en ontvangen deze graag binnen vier weken na dagtekening van deze brief.

De voorzitter van de vaste commissie voor Immigratie en Asiel/JBZ-Raad,
Faber-van de Klashorst

De voorzitter van de vaste commissie voor Justitie en Veiligheid,
De Boer

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 3 november 2020

Hierbij zend ik u de antwoorden op de vragen van de leden van de GroenLinks-fractie over de op 24 juli 2020 door de Europese Commissie gepubliceerde mededeling: De EU-strategie voor de veiligheidsunie (167682u).

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De leden van de GroenLinks-fractie onderschrijven de doelen en begrijpen de aanpak van de Europese Commissie omtrent het aanpakken van mensenhandel, cybercriminaliteit, georganiseerde misdaad en pogingen om radicalisering tegen te gaan. De keuze van de Europese Commissie om een sterke focus te leggen op het onderwerp digitalisering in relatie tot veiligheid en criminaliteit onderschrijven deze leden evenzeer. Aan het slot van deze brief treft u enkele vragen op dit punt. Eerst zouden de aan het woord zijnde leden graag een fundamenteler gesprek aangaan met de regering over de gepresenteerde EU-strategie voor de veiligheidsunie.

De leden van de GroenLinks-fractie vragen zich af wat er zou moeten gebeuren op klimatologisch gebied voordat de gevolgen van klimaatverandering een integraal onderdeel zouden moeten vormen van de EU-strategie voor de veiligheidsunie? Klimaatverandering wordt nu genoemd in de derde zin van de inleiding, maar verder in zijn geheel niet. Hoe kijkt de regering hier tegenaan?

Klimaatverandering door de opwarming van de aarde stelt ons voor nieuwe uitdagingen. Het leidt steeds vaker tot extreem weer, van heftige neerslag tot hoge temperaturen. Klimaatverandering kan leiden tot nieuwe dimensies bij veiligheidsvraagstukken. Een inzet op het voorkomen of mitigeren van dreigingen als het gevolg van klimaatverandering is daarbij het meest effectief. Nederland steunt in dat kader een ambitieuze inzet in EU verband in het kader van de Green Deal. Andere instrumenten, zoals de Veiligheidsuniestrategie, kunnen daar ook aan bijdragen.

Het doel van de EU-Strategie voor de Veiligheidsunie is om dreigingen op het gebied van criminaliteit, terrorisme, racisme en vreemdelingenhaat aan te pakken en daartoe de samenwerking tussen politiële en justitiële autoriteiten en andere autoriteiten en organisaties te bevorderen. Dreigingen ten gevolge van klimaatverandering horen slechts in deze strategie voor zover zij de onderwerpen raken die onder het veiligheidsaspect van de ruimte van vrijheid, veiligheid en recht vallen (zie artikel 67 lid 3 VWEU).

De Commissie noemt in de Veiligheidsuniestrategie diverse vormen van milieucriminaliteit, zoals illegale mijnbouw, illegale houtkap en illegale verwijdering en vervoer van afval. Ook geeft de Commissie aan dat er sprake is van criminele exploitatie van regelingen voor de handel in emissierechten en systemen voor energiecertificaten, en van misbruik van de financiering voor ecologische veerkracht en duurzame ontwikkeling. Naast het bevorderen van maatregelen van de EU, de lidstaten en de internationale gemeenschap om de inspanningen ter bestrijding van milieucriminaliteit op te voeren, onder andere via de Green Deal, geeft de Commissie aan de richtlijn milieucriminaliteit te willen beoordelen om te bezien of deze nog steeds geschikt is voor het beoogde doel.

De Europese Commissie schrijft: «Terrorisme, georganiseerde criminaliteit, drugshandel en mensenhandel vormen rechtstreekse bedreigingen voor de burgers en onze Europese manier van leven». De Europese Commissie schrijft dat er sprake is van een neerwaarts spiraal van aanslagen. Kan de regering de cijfers opvragen bij de Europese Commissie van deze neerwaartse spiraal in de laatste tien jaar?

De Commissie geeft in de Veiligheidsuniestrategie aan dat er in 2019 een neerwaartse trend waar te nemen was waar het ging om terroristische aanslagen in de EU. De Commissie verwijst hierbij naar een publiek beschikbaar rapport van Europol, het European Union Terrorism Situation and Trend Report, 2020. Cijfers over aanslagen met een terroristisch

oogmerk in de laatste tien jaar zijn beschikbaar in dit jaarlijks gepubliceerde rapport van Europol.[10] In het overzicht van 2009 wordt het hoogste aantal verijdelde, mislukte en volbrachte aanslagen gerapporteerd in de EU met 294 en in 2019 het laagste aantal met 119. De daling verloopt overigens niet in een rechte lijn – het ene jaar daalt het wat meer en het andere stijgt het weer iets. De achtergrond achter de gerapporteerde verijdelde, mislukte en volbrachte aanslagen loopt sterk uiteen van bijvoorbeeld jihadistisme, rechts-extremisme en linksextremisme. Ook wordt separatisme meegenomen. Van de 119 verijdelde, mislukte en volbrachte aanslagen in 2019 zien bijvoorbeeld 56 op veiligheidsincidenten in Noord-Ierland.

De leden steunen de Europese Commissie inzake maatregelen om de publieke ruimte in steden veiliger te maken door objecten slim te plaatsen in de publieke ruimte, zodat er minder met voertuigen aanslagen kunnen worden gepleegd. Deelt de regering deze visie van de Europese Commissie en is zij het met de leden van de GroenLinks-fractie en de Europese Commissie eens dat plekken waar auto's en vrachtwagen niet kunnen komen, veiligere publieke ruimten worden? Weet de regering wat de Europese Commissie op dit punt concreet wil doen en gaat de regering hier proactief op handelen, ook gelet op de rapporten van de NCTV? Graag verzoeken de aan het woord zijnde leden om een reactie van de regering op het gebied van veiligheid voor burgers en onze manier van leven, en een reflectie over de voordelen van deze integrale aanpak voor de publieke ruimte.

Zoals verwoord in de Veiligheidsuniestrategie zet de Commissie zich in het kader van een toekomstbestendige veiligheidsomgeving in om de bescherming van publieke ruimten verder te verbeteren. «Publieke ruimte» is daarbij een ruim begrip. Het kabinet acht het van belang om eerst helder te hebben welke ruimte dat exact is en welke onderdelen binnen die ruimte beter fysiek beveiligd zouden moeten worden. Daarbij wordt ook gehecht aan aandacht voor de (betere) samenwerking tussen publiek en privaat. Onder andere wordt bekeken hoe de beproefde aanpak voor bijvoorbeeld luchthavens toepasbaar kan zijn voor andere publieke ruimten. Het kabinet hecht in dit kader veel waarde aan uitwisseling van beproefde praktijken in EU verband, zoals de aanpak van het misbruik van drones. De stappen die de Commissie reeds in dat verband heeft gezet worden daarin sterk gewaardeerd.

Zou het volgens de regering kunnen zijn dat de Europese Commissie ten onterechte klimaatverandering níet als rechtstreekse dan wel indirecte bedreiging ziet? Is het immers niet zo, dat zowel het aantal slachtoffers, als de impact op onze manier van leven door klimaatverandering veel groter is dan dat terrorisme in potentie is? De genoemde leden onderschrijven de inspanningen van de Europese Commissie op het terrein van terrorisme en het bestrijden van terroristische inhoud op internet ten zeerste. De Europese Commissie schrijft: «De lidstaten behouden de primaire verantwoordelijkheid voor de bestrijding van terrorisme en radicalisering». Is de regering van mening dat het klimaat- en pandemievraagstuk niet bij uitstek een bij de EU passend vraagstuk betreft, ook wat betreft veiligheid? En is de regering bereid hierover met de Europese Commissie in gesprek te treden?

Zoals ook hierboven beschreven, richt de Veiligheidsuniestrategie zich slechts op dreigingen op het gebied van criminaliteit, terrorisme, racisme en vreemdelingenhaat. Het feit dat klimaatverandering niet als dreiging

[10] https://www.europol.europa.eu/tesat-report

genoemd wordt in deze strategie, betekent daarom niet dat de Commissie deze dreiging niet ziet.

Zoals bij u bekend is, is bijvoorbeeld de Green Deal erop gericht klimaatbeleid voor de langere termijn te beïnvloeden. Deze strategie is gebaseerd op de vaststelling van de Commissie dat klimaatverandering een existentiële bedreiging voor Europa en de wereld vormt. De Green Deal sluit op hoofdlijnen goed aan bij het nationale Klimaatakkoord. Hierbij acht het kabinet het van belang dat Nederland deze grote uitdagingen samen in EU-verband aanpakt.

Hetzelfde geldt voor de aanpak het pandemievraagstuk, dat zowel in nationale context als op EU-niveau wordt geadresseerd.

«De COVID-19-crisis heeft er ook toe geleid dat wij onze notie van veiligheidsbedreigingen en de bijbehorende beleidsmaatregelen hebben herzien», aldus de Europese Commissie. In totaal schrijft de Europese Commissie negen keer over COVID-19 in haar strategie. Negen keer is dit in relatie tot het digitale domein. Zo schrijft de Europese Commissie zowel over de oplossingen om door te kunnen blijven werken vanuit thuis dankzij technologie, waardoor men tegelijkertijd digitaal kwetsbaarder wordt voor desinformatie, als over pogingen om het politiek narratief te beïnvloeden en over de online zwendel in gezondheidsproducten. Hoe beoordeelt de regering dit en weet de regering of COVID-19 nog tot andere inzichten heeft geleid in de notie qua veiligheidsbedreigingen en mogelijk bijbehorende beleidsmaatregelen? Zo ja, zou de regering deze inzichten willen delen, inclusief de *lessons learned*? Zo niet, zou de regering deze inzichten bij de Europese Commissie willen opvragen?

Tijdens de JBZ-Raad van 28 april jl.[11] gaf Europol een overzicht van de ontwikkelingen in criminele activiteiten sinds de uitbraak van het COVID-19 virus. De conclusie hierbij was dat de beperkende maatregelen, zoals lock downs, de georganiseerde criminaliteit niet hebben beperkt. Wel was er wel sprake van een aanpassing van criminele activiteiten.

Europol gaf daarbij aan dat er verschuivingen in criminele fenomenen zijn waargenomen, met de meeste impact op het digitale/cyber domein. Criminelen lijken hun werkmethoden snel aan te passen aan de nieuwe omstandigheden, waarbij digitale vormen van criminaliteit zoals malware en ransomware werden genoemd, maar ook fraude met beschermingsmateriaal en medicijnen. Ook waarschuwde Europol voor de risico's van een kwetsbare economie voor misbruik door de georganiseerde criminaliteit doordat het bedrijfsleven vatbaarder is voor criminele investeringen. Verder vroeg de Commissie in de voorbije maanden aandacht voor de toename van seksuele exploitatie van kinderen online, de toename van huiselijk geweld en mogelijke fraude met economische steunmaatregelen.

Het kabinet onderschrijft de analyse van Europol en de Commissie en kan de waargenomen verschuiving in criminaliteit en gesignaleerde risico's bevestigen. Er is een toename in digitaal ondersteunde criminaliteit; de bestrijding daarvan heeft prioriteit. Ook moeten diverse vormen van fraude en witwassen worden bestreden. Het kabinet stelt vast dat de COVID-19 crisis de meest kwetsbaren in de samenleving het hardst raakt. In het bijzonder maakt het kabinet zich zorgen over online seksuele uitbuiting van kinderen, verborgen misdrijven zoals huiselijk geweld en mensenhandel, evenals georganiseerde ondermijnende criminaliteit.

---

[11] Eerste Kamer, vergaderjaar 2019–2020, 32 317, nr. LB

Weet de regering of de Europese Commissie de conclusie trekt dat COVID-19 ook een gevolg is ván onze manier van leven, of dat straks een ander virus dit kan zijn? Zo ja, hoe verhouden pandemieën zich dan tot veiligheidsvraagstukken? En welke conclusies op veiligheidsgebied moet je verbinden aan de vaststelling dat «onze manier van leven» een bedreiging vormt voor «onze manier van het leven?» Zo nee, zou de regering dit bij de Europese Commissie willen bepleiten?

Een pandemie kan ook gevolgen hebben voor veiligheidsvraagstukken. Dit toont de COVID-19 pandemie aan zoals hierboven al aangegeven. De Commissie heeft aangegeven dat in EU verband de paraatheid en beheersing van grensoverschrijdende bedreigingen voor de volksgezondheid moet worden versterkt. De Commissie is voornemens om voorstellen te doen om het EU-kader voor het detecteren en reageren op grensoverschrijdende bedreigingen te verbeteren en de rol van de huidige agentschappen te versterken.

De leden van de GroenLinks-fractie constateren dat de Europese Commissie eerder bereid is haar notie van veiligheidsbedreigingen en de bijbehorende beleidsmaatregelen te herzien. Is de regering in dat licht bereid het voorgaande omtrent klimaatverandering en COVID-19 te adresseren bij de Europese Commissie?

Zoals aangegeven zijn zowel klimaat als COVID-19 prioritaire thema's in EU-verband en op nationaal niveau. Wat betreft klimaatverandering ziet het kabinet de Green Deal als essentieel instrument. Op het gebied van COVID-19 zet het kabinet in op betere samenwerking tussen de lidstaten.

Tot slot hebben de leden van de GroenLinks-fractie nog de volgende vragen:

Welke drukmiddelen zijn er ten opzichte van de private sector om relevante informatie te verkrijgen in het kader van de bestrijding van cybercriminaliteit, witwassen, georganiseerde misdaad, die deze bedrijven vanuit concurrentieoverwegingen niet willen delen?

Net als alle organisaties moeten bedrijven zich houden aan de wet en zal handhavend worden opgetreden in strafrechtelijke, bestuursrechtelijke zin of op een andere wijze. Gegevens kunnen door het Openbaar Ministerie worden gevorderd voor opsporing en vervolgingsdoeleinden. Inzake het digitale domein wordt in Europees verband (binnen de EU en in het kader van de Raad van Europa) gewerkt aan het versterken van de bewijsvergaringsmogelijkheden voor digitale informatie. Dit gebeurt door het realiseren van een e-evidence verordening (het standpunt van het Europees parlement wordt afgewacht) en het tweede Protocol in het Raad van Europa verdrag voor de bestrijding van cybercriminaliteit. Ik verwijs u ook naar mijn brief aan de Tweede Kamer van 29 juni 2020 inzake de voortgang van de integrale aanpak van cybercrime[12]. Voor het vorderen van bankgegevens is naar aanleiding van de gewijzigde vierde anti-witwasrichtlijn recentelijk de wet financieel toezicht gewijzigd en is een verwijzingsportaal bankgegevens voor opsporing en vervolgingsdoeleinden actief. Voor het tegengaan van illegale content online, mede voor de bestrijding van seksuele kindermisbruik online, verwijs ik u naar de brief aan de Tweede Kamer van 8 oktober 2020 inzake hostingbedrijven en kinder-pornografisch beeldmateriaal[13].

---

[12] Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 696

[13] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z18360&did=2020D39646

Kan de regering bij de Europese Commissie opvragen om inzichtelijk te maken op welke wijze artificiële intelligentie (AI) wordt toegepast binnen de Europese Unie om veiligheidsissues te adresseren? Zowel door overheden als bedrijven? Hoe zit het met digitale aanvallen vanuit de Verenigde Staten in de laatste tien jaar?

Artificiële intelligentie (AI) kan het beste worden gezien als een bouwsteen die in toenemende mate wordt gebruikt in bestaande en nieuwe cybersecuritysystemen bij zowel overheden als het bedrijfsleven. Deze ontwikkeling is ook benoemd in het Cybersecuritybeeld Nederland van 2019[14] en 2020[15]. Ook ENISA noemt in hun recentelijk gepubliceerde analyse van het dreigingslandschap[16] dat AI kan bijdragen aan het analyseren van informatie over cyberdreigingen. Een concreet voorbeeld van de mogelijkheden is dat AI, door middel van machine learning, patronen kan herkennen in omvangrijke datasets bestaande uit cyberincidenten om zo ook nieuwe dreigingen te ontdekken. Ook zou deze technologie kunnen worden gebruikt om de digitale infrastructuur van een organisatie live te monitoren op ongebruikelijke activiteit. Hierbij kan gedacht worden aan inlogpogingen die afwijken van normale situaties. Daarnaast wordt AI veelvuldig toegepast in anti-malware software.

Voor het meest actuele beeld van de digitale dreiging verwijs ik u naar het CSBN 2020, dat ik in juni aan de Tweede Kamer heb aangeboden[17]. Het CSBN 2020 biedt inzicht in de digitale dreiging en de belangen die daardoor kunnen worden aangetast. Het gaat ook in op de weerbaarheid tegen de digitale dreiging en op de digitale risico's. Het accent ligt daarbij op de nationale veiligheid.

Welke dreiging gaat er uit van drones die vanaf de andere kant van de wereld dankzij 5G kunnen worden bestuurd? Heeft de regering hier analyses van gemaakt?

Al geruime tijd houden veiligheidspartners, zowel op nationaal als internationaal niveau, de ontwikkelingen op het gebied van drones nauwlettend in de gaten. Hierbij wordt nauw samengewerkt met kennisinstituten en het bedrijfsleven. In gezamenlijkheid worden de civiele en militaire ontwikkelingen nationaal en Europees/internationaal op de voet gevolgd. Ook de ontwikkelingen omtrent 5G worden hierin meegenomen. De ontwikkeling van 5G roept namelijk de vraag op welke veiligheidsrisico's hieraan kleven en wat de rol is van de internationale samenwerking op dit gebied.

De besturing van drones kan op verschillende wijzen plaatsvinden. Vooralsnog worden drones slechts beperkt met 4G of 5G aangestuurd. Naar verwachting zullen in de toekomst, met de uitrol van 5G, drones wel steeds meer met 5G (telecom) – signalen bestuurd kunnen gaan worden.

Om een drone te kunnen laten vliegen via een 5G netwerk moet een dekkend 5G netwerk zijn en dat is op dit moment niet het geval. In de evolutie van 4G naar 5G is er bovendien een tussenstap. In eerste instantie zal 5G non-standalone zijn. Dat wil zeggen dat de verbindingsopbouw en netwerkcontroleberichten over de bestaande 4G netwerken gaan, de (breedband) datatransmissie gaat dan over het nieuwe 5G netwerk. Pas later zal een migratie plaatsvinden naar een volledig standalone 5G netwerk.

---

[14] CSBN 2019
[15] CSBN 2020
[16] ENISA Threat Landscape – The year in review (2020)
[17] Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 695

Onder volledige 5G zal de geografische (netwerk)afstand waarop het toestel goed te besturen is naar verwachting toenemen, maar daarmee valt nog niet met zekerheid te stellen of een drone dan succesvol vanaf de andere kant van de wereld bedient kan worden. Om tijdig de consequenties van de ontwikkelingen in te kunnen schatten lopen op dit gebied verschillende initiatieven.

De Europese Commissie schrijft «Huishoudens, banken, financiële diensten en ondernemingen (met name in het midden- en kleinbedrijf) worden zwaar getroffen door cyberaanvallen». Weet de regering hoe groot deze schade is? Is hier onderzoek naar gedaan? Welke sectoren worden het meeste getroffen?

De NCTV stelt jaarlijks het Cybersecuritybeeld Nederland (CSBN) vast, dat inzicht biedt in de digitale dreiging en de belangen die daardoor kunnen worden aangetast. In het CSBN wordt onder meer vermeld dat digitale risico's voor Nederland thans onverminderd groot zijn. Vanuit het perspectief van nationale veiligheid gaat het vooral om de risico's van (voorbereidingen voor) sabotage en spionage door statelijke actoren. Ook bestaat het risico van (grootschalige) uitval van digitale diensten, processen of systemen. Verder is er het risico van cyberaanvallen door criminele actoren die het te doen is om economisch gewin. Het CSBN 2020 is in juni aan de Tweede Kamer aangeboden[18]. Eerder is door het Centraal Planbureau onderzoek gedaan naar de economische gevolgen van cyberrisico's in de Risicorapportage Cyberveiligheid, waarvan de meest recente editie in 2019 is verschenen[19]. Eén van de conclusies hiervan is dat het risico van schade door ontwrichtende incidenten waarschijnlijk niet is afgenomen, maar dat het lastig is vast te stellen wat de economische en maatschappelijke van een digitale aanval of digitale spionage is.

[18] Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 695
[19] https://www.cpb.nl/risicorapportage-cyberveiligheid-2019