EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 13.9.2017
JOIN(2017) 450 final

# GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD

## Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU

## 1. INLEIDING

Cyberbeveiliging is van cruciaal belang voor onze welvaart en onze veiligheid. Naarmate ons dagelijks leven en onze economieën meer vervlochten raken met digitale technologieën, worden we kwetsbaarder. Cyberincidenten worden steeds diverser, zowel als je kijkt naar wie er achter zit als wat zij willen bereiken. Kwaadwillige cyberactiviteiten vormen niet alleen een bedreiging voor onze economieën en de ontwikkeling van de digitale eengemaakte markt, maar ook voor onze democratieën, onze vrijheden en onze waarden. Onze veiligheid zal in de toekomst afhangen van ons vermogen om de EU te beschermen tegen cyberaanvallen: zowel de civiele infrastructuur als de militaire capaciteit steunen op veilige digitale systemen. Dit is erkend door de Europese Raad van juni 2017[1] en ook in de integrale strategie voor het buitenland- en veiligheidsbeleid van de Europese Unie[2].

De risico's nemen exponentieel toe. Uit studies blijkt dat de economische impact van cybercriminaliteit tussen 2013 en 2017 vervijfvoudigd is en tegen 2019 nog eens viermaal zo groot zou kunnen worden[3]. Met name ransomware[4] wordt meer gebruikt en de recente aanvallen[5] wijzen op een dramatische toename van deze vorm van cybercriminaliteit. Het gevaar komt evenwel niet alleen uit die hoek.

De cyberdreigingen komen zowel van statelijke als niet-statelijke actoren: ze zijn vaak crimineel gemotiveerd, gedreven door winstbejag, maar kunnen ook een politieke en strategische inslag hebben. De criminele dreiging wordt versterkt nu de grens tussen cybercriminaliteit en "traditionele" misdaad vervaagt: criminelen gebruiken het internet niet alleen voor de uitbreiding van hun bestaande activiteiten, maar ook in hun zoektocht naar nieuwe methoden en instrumenten om misdaden te plegen[6]. In het merendeel van de gevallen is de kans echter miniem dat de criminelen kunnen worden opgespoord, en is de kans op vervolging nog kleiner.

Tegelijkertijd bereiken statelijke actoren hun geopolitieke doelen steeds vaker niet alleen met traditionele middelen, zoals militair geweld, maar ook met discretere cyberinstrumenten, bijvoorbeeld door binnenlandse democratische processen te beïnvloeden. Dat de cyberspace gebruikt wordt voor oorlogsvoering, op zichzelf staand of als onderdeel van een hybride benadering, wordt nu algemeen erkend. Desinformatiecampagnes, fakenieuws en cyberaanvallen op kritieke infrastructuurvoorzieningen komen steeds vaker voor en hiertegen moet worden opgetreden. Om deze reden heeft de Commissie in haar discussienota over de toekomst van de Europese defensie[7] het belang van samenwerking op het gebied van cyberdefensie benadrukt.

Als we onze cyberbeveiliging niet gevoelig versterken, zullen de risico's toenemen naarmate de digitale transformatie zich voltrekt. Verwacht wordt dat in 2020 tientallen miljarden toestellen zullen zijn aangesloten op het internet der dingen, maar toch is cyberbeveiliging bij

---

1 http://www.consilium.europa.eu/nl/press/press-releases/2017/06/23-euco-conclusions/

2 http://europa.eu/globalstrategy/

3 Zie bijvoorbeeld McAfee & Centre for Strategic and International Studies "Net losses: Estimating the Global Cost of Cybercrime" 2014.

4 Ransomware is een soort malware die de toegang tot het computersysteem van de gebruiker blokkeert of beperkt door het scherm te vergrendelen of door bestanden te vergrendelen totdat er losgeld ("*ransom*") is betaald.

5 In mei 2017 werden meer dan 400 000 computers in meer dan 150 landen getroffen door een aanval met WannaCry-ransomware. Een maand later werden Oekraïne en een aantal bedrijven over de hele wereld het slachtoffer van de aanval met Petya-ransomware

6 Dreigingsevaluatie van de zware en georganiseerde criminaliteit voor 2017 van Europol.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_nl.pdf

het ontwerp van die apparaten op dit ogenblik nog geen prioriteit[8]. Als we de toestellen die onze elektriciteitsnetten, auto's, wegennetten, fabrieken, financiën, ziekenhuizen en huizen gaan aansturen, niet kunnen beveiligen, kan dit desastreuze gevolgen hebben en het vertrouwen van de consument in nieuwe technologieën enorm beschadigen. Het risico dat politiek gemotiveerde aanvallen zouden worden uitgevoerd op burgerdoelen en dat de militaire cyberbeveiliging tekort zou schieten, maakt dit gevaar alleen maar groter.

De in deze gezamenlijke mededeling uiteengezette aanpak zal de EU beter wapenen tegen deze gevaren. De weerbaarheid en strategische autonomie zouden vergroten, de vermogens op het gebied van technologie en vaardigheden zouden worden versterkt en de bouw van een sterke eengemaakte markt zou worden bevorderd. Dit vraagt om de juiste structuren, zodat een sterke cyberbeveiliging kan worden uitgebouwd en waar nodig kan worden gereageerd, met volledige betrokkenheid van alle belangrijke actoren. Door de verantwoordelijken intensiever op te sporen, te traceren en ter verantwoording te roepen, zou deze aanpak cyberaanvallen ook sterker ontmoedigen. Deze aanpak houdt ook rekening met de mondiale dimensie, aangezien de ontwikkeling van internationale samenwerking de basis zou vormen waarop de EU een leidende rol op het gebied van cyberbeveiliging zou kunnen spelen. Met deze stappen wordt voortgebouwd op de benaderingen van de digitale eengemaakte markt, de integrale EU-strategie, de Europese Veiligheidsagenda[9], het gezamenlijk kader voor de bestrijding van hybride bedreigingen[10] en de mededeling over de oprichting van het Europees Defensiefonds[11][12].

De EU werkt reeds aan veel van deze kwesties, maar nu moeten de verschillende werkzaamheden worden samengebracht. In 2013 heeft de EU een cyberbeveiligingsstrategie uitgetekend waarin een aantal belangrijke activiteiten ter verbetering van de cyberweerbaarheid werden gelanceerd[13]. De belangrijkste doelstellingen en beginselen van deze strategie voor een betrouwbaar, veilig en open cyber-ecosysteem zijn nog altijd valabel. Maar door de voortdurend veranderende en toenemende cyberdreiging zijn er meer maatregelen nodig om aanvallen in de toekomst te weerstaan en af te slaan[14].

De reikwijdte van haar beleid en de instrumenten, structuren en vermogens waarover ze beschikt, maken dat de EU goed geplaatst is om het probleem van cyberbeveiliging aan te pakken. Hoewel de lidstaten verantwoordelijk blijven voor hun nationale veiligheid, vormen de schaal en de grensoverschrijdende aard van deze dreiging sterke argumenten voor EU-maatregelen waarmee de lidstaten zouden worden gestimuleerd en ondersteund om meer en betere nationale vermogens op het gebied van cyberbeveiliging te ontwikkelen en te handhaven en tegelijkertijd capaciteit op te bouwen op EU-niveau. Deze aanpak is erop gericht alle actoren – de EU, de lidstaten, het bedrijfsleven en de burgers – aan te sporen om aan cyberbeveiliging de prioriteit te geven die nodig is om de weerbaarheid aan te scherpen en

---

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, studie in opdracht van de Europese Commissie.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295 final

12 Deze benadering is ook onderbouwd met onafhankelijke wetenschappelijke adviezen van de groep op hoog niveau van wetenschappelijk adviseurs van het mechanisme voor wetenschappelijk advies van de Europese Commissie (zie verwijzingen hieronder).

13 JOIN(2013) 1 final. In SWD(2017) 295 wordt deze strategie geëvalueerd.

14 Tenzij anders is aangegeven, zijn de voorstellen in deze mededeling begrotingsneutraal. Voor ieder initiatief met gevolgen voor de begroting zullen de jaarlijkse begrotingsprocedures worden gevolgd en kan er niet vooruit worden gelopen op het meerjarig financieel kader voor de periode na 2020.

te zorgen voor een betere EU-respons op cyberaanvallen. Er zullen concrete stappen worden gezet om iedere cyberaanval tegen de EU en haar lidstaten op te sporen en te onderzoeken, en om passend te reageren, onder meer door de criminelen te vervolgen. Zo kan het externe optreden van de EU daadwerkelijk de cyberbeveiliging op het wereldtoneel bevorderen. Op die manier zal de EU de omslag maken van een reactieve naar een proactieve benadering en niet alleen de Europese welvaart, maatschappij en waarden, maar ook de grondrechten en fundamentele vrijheden beschermen door bestaande en toekomstige dreigingen te pareren.

## 2. DE EU WEERBAARDER MAKEN TEGEN CYBERAANVALLEN

Sterke cyberweerbaarheid vraagt om een collectieve en brede aanpak. Hiervoor zijn robuustere en doeltreffendere structuren nodig om de cyberbeveiliging te bevorderen en om te reageren op cyberaanvallen in de lidstaten, maar ook tegen de instellingen, agentschappen en organen van de EU. Met het oog hierop dient de versterking van de cyberweerbaarheid en de strategische autonomie ook breder en beleidsoverschrijdend te worden benaderd, met een sterke eengemaakte markt, grote vooruitgang op het vlak van het technologische vermogen van de EU en een veel groter aantal deskundigen. Centraal hierbij staat de ruimere acceptatie dat cyberbeveiliging een gezamenlijk maatschappelijk probleem is, waarbij alle geledingen van de overheid, het bedrijfsleven en de maatschappij moeten worden betrokken.

### 2.1 Versterking van het Agentschap van de Europese Unie voor cyberbeveiliging

Het **Agentschap van de Europese Unie voor cyberbeveiliging** (Enisa) speelt een sleutelrol bij de versterking van de cyberweerbaarheid en de reactiviteit van de EU, maar wordt hierin beperkt door zijn huidige mandaat. Daarom doet de Commissie een ambitieus hervormingsvoorstel, dat onder meer een **permanent mandaat voor het Agentschap**[15] omvat. Hierdoor zal het Enisa de lidstaten, EU-instellingen en bedrijven kunnen ondersteunen op cruciale terreinen, zoals bij de uitvoering van de richtlijn voor de beveiliging van netwerk- en informatiesystemen[16] ("NIS-richtlijn") en het voorgestelde kader voor cyberbeveiligingscertificering.

Het hervormde Enisa zal een belangrijke adviserende rol spelen bij de ontwikkeling en uitvoering van het beleid, onder meer door samenhang te bevorderen tussen de NIS-richtlijn en sectorale initiatieven en door te helpen centra voor informatie-uitwisseling en -analyse op te zetten in kritieke sectoren. Het Enisa zal de lat hoger leggen en ervoor zorgen dat Europa beter voorbereid is dankzij de jaarlijkse organisatie van Europabrede cyberbeveiligingsoefeningen waarbij de respons op verschillende niveaus wordt gecombineerd. Het Agentschap zal ook steun verlenen aan de ontwikkeling van het EU-beleid inzake cyberbeveiligingscertificering van informatie- en communicatietechnologie (ICT) en een belangrijke rol spelen in de versterking van de operationele samenwerking en crisisbeheersing in de hele EU. Het zal in de cybergemeenschap ook dienstdoen als centraal kennis- en informatiepunt.

Het is noodzakelijk om snel en gezamenlijk inzicht te krijgen in dreigingen en incidenten terwijl deze zich voordoen, om te kunnen besluiten of een gezamenlijke corrigerende actie of

[15] COM(2017) 477 final

[16] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

respons met steun van de EU nodig is. Om informatie op een dergelijke manier uit te wisselen moeten alle relevante actoren – de organen en agentschappen van de EU, alsook de lidstaten – betrokken zijn op technisch, operationeel en strategisch niveau. Ook zal het Enisa bijdragen aan het situationeel bewustzijn op EU-niveau, in samenwerking met de betrokken organen van de lidstaten en de EU, en met name het netwerk van computer security incident response teams[17], CERT-EU, Europol en het Centrum van de Europese Unie voor de analyse van inlichtingen (EU-Intcen). Dit kan waardevol zijn voor de inlichtingen over dreigingen en voor de beleidsvorming inzake de regelmatige monitoring van de dreiging en inzake effectieve operationele samenwerking, maar ook voor de respons op grootschalige grensoverschrijdende incidenten.

## 2.2 Naar een eengemaakte markt voor cyberbeveiliging

De groei van de markt voor cyberbeveiliging in de EU wordt, als het gaat om producten, diensten en processen, in diverse opzichten afgeremd. Een belangrijk aspect is het gebrek aan regelingen voor cyberbeveiligingscertificering die in de hele EU worden erkend, waardoor de producten aan hogere cyberbeveiligingsnormen zouden voldoen en het marktvertrouwen in de gehele EU zou worden ondersteund. De Commissie dient daarom een voorstel in tot oprichting van een **Europees kader voor cyberbeveiligingscertificering**[18]. Dit kader zou de procedure omvatten voor de creatie van EU-brede regelingen voor cyberbeveiligingscertificering van producten, diensten en/of systemen, waarbij het zekerheidsniveau afhangt van het beoogde gebruik (of het nu om kritieke infrastructuur of consumentenproducten gaat)[19]. Het zou bedrijven die grensoverschrijdend handel drijven, duidelijk ten goede komen als ze niet langer verschillende certificeringsprocedures zouden moeten doorlopen en dus hun administratieve en financiële kosten zouden kunnen beperken. De in dit kader ontwikkelde regelingen zou ook het consumentenvertrouwen helpen vergroten: een conformiteitscertificaat zou de kopers en gebruikers informeren en geruststellen over de beveiligingseigenschappen van de producten en diensten die zij kopen en gebruiken. Hoge normen voor cyberbeveiliging zouden zo een concurrentievoordeel opleveren. Dit zou leiden tot een hogere weerbaarheid omdat de ICT-producten en -diensten formeel zouden worden beoordeeld aan de hand van een reeks welomschreven cyberbeveiligingsnormen die zouden kunnen worden ontwikkeld in nauwe samenhang met de bredere werkzaamheden die lopende zijn op het gebied van ICT-normen[20].

De regelingen van het kader zouden vrijwillige regelingen zijn en geen onmiddellijke regelgevende verplichtingen voor de verkopers of dienstverleners met zich meebrengen. De regelingen zouden niet in strijd zijn met de toepasselijke wettelijke voorschriften, zoals de Europese wetgeving inzake gegevensbescherming.

Zodra het kader is vastgesteld, zal de Commissie de belanghebbenden vragen zich op drie prioritaire gebieden te concentreren:

- Beveiliging van kritieke of risicovolle toepassingen[21]: systemen waar we in ons dagelijkse leven afhankelijk van zijn – van auto's tot fabrieksmachines, van grote systemen zoals vliegtuigen of elektriciteitscentrales tot kleine systemen zoals medische hulpmiddelen: ze

[17] Zoals bepaald bij artikel 9 van de NIS-richtlijn.
[18] COM(2017) 477 final.
[19] Een zekerheidsniveau geeft aan hoe strikt de beveiliging is gecontroleerd en is gewoonlijk evenredig met het risiconiveau van de toepassingsgebieden of -functies (d.w.z. dat een hoger zekerheidsniveau vereist is voor ICT-producten en -diensten die worden gebruikt in toepassingsgebieden of -functies met een hoog risico).
[20] COM(2016) 176 final.
[21] Met uitzondering van verplichte of vrijwillige certificering op grond van andere handelingen van de Unie.

worden steeds digitaler en vaker onderling verbonden. Daarom zouden de essentiële ICT-componenten van dergelijke producten en systemen streng moeten worden beoordeeld op hun beveiliging.

- De cyberbeveiliging van wijdverbreide digitale producten, netwerken, systemen en diensten die door de particuliere en publieke sector worden gebruikt om aanvallen af te slaan en regelgevende verplichtingen na te komen[22] — zoals e-mailversleuteling, firewalls en virtuele particuliere netwerken (VPN); het is van essentieel belang dat het toenemende gebruik van dergelijke hulpmiddelen niet tot nieuwe risico's of nieuwe kwetsbaarheden leidt.

- Het gebruik van ingebouwde-beveiligingsmethoden ("security by design") in goedkope, digitale, onderling verbonden toestellen voor massaconsumptie die deel uitmaken van het internet van de dingen: de regelingen van dit kader zouden kunnen worden gebruikt om aan te geven dat de producten gemaakt zijn volgens geavanceerde, veilige ontwikkelingsmethoden, dat zij afdoende getest zijn en dat de verkopers zich ertoe verbinden hun software te updaten indien nieuwe kwetsbaarheden of dreigingen aan het licht komen.

Deze prioriteiten moeten in het bijzonder rekening houden met het evoluerende cyberdreigingslandschap en met het belang van essentiële diensten zoals vervoer, energie, gezondheidszorg, het bankwezen, financiëlemarktinfrastructuren, drinkwater en digitale infrastructuur[23].

Er bestaan weliswaar geen ICT-producten, -systemen of -diensten waarvan kan worden gegarandeerd dat ze 100 % veilig zijn, maar er zijn verschillende bekende en goed gedocumenteerde gebreken in het ontwerp van ICT-producten die kunnen worden benut voor aanvallen. Indien de benadering van "ingebouwde beveiliging" door producenten van geconnecteerde toestellen, software en IT-apparatuur wordt toegepast, zorgt dit ervoor dat het probleem van de cyberbeveiliging al wordt aangepakt nog vóór nieuwe producten op de markt worden gebracht. Dit zou deel kunnen uitmaken van het zorgplichtbeginsel, dat samen met de industrie verder moet worden ontwikkeld en dat de producten/software minder kwetsbaar zou kunnen maken dankzij de toepassing, vanaf de ontwerpfase tot de keuring en de controle, van een reeks methoden, zoals, indien van toepassing, formele verificatie, onderhoud op lange termijn, het gebruik van veilige processen in de ontwikkelingscyclus en de ontwikkeling van updates en patches om nieuw ontdekte kwetsbaarheden aan te pakken en snel updates en herstellingen uit te voeren[24]. Dit zou de consument meer vertrouwen in digitale producten geven.

Ook moet worden erkend dat derden die onderzoek doen naar beveiliging een belangrijke rol spelen bij het opsporen van kwetsbaarheden in bestaande producten en diensten en moeten in

---

[22] Volgens Richtlijn (EU) 2016/1148, Verordening (EU) 2016/679, Richtlijn (EU) 2015/2366 en andere wetgevingsvoorstellen zoals het Europees wetboek voor elektronische communicatie, bijvoorbeeld, moeten organisaties passende veiligheidsmaatregelen treffen om relevante cyberbeveiligingsrisico's aan te pakken.

[23] De sectoren binnen de werkingssfeer van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

[24] "Cybersecurity in the European Digital Single Market" (cyberbeveiliging op de Europese eengemaakte digitale markt), groep op hoog niveau van wetenschappelijk adviseurs, maart 2017

alle lidstaten voorwaarden worden vastgesteld voor de gecoördineerde bekendmaking van kwetsbaarheden[25], voortbouwend op beste praktijken[26] en toepasselijke normen[27].

Tegelijk worden **specifieke sectoren** geconfronteerd met specifieke problemen en moeten zij worden aangemoedigd om hun eigen aanpak te ontwikkelen. Op die manier zouden algemene cyberbeveiligingsstrategieën worden aangevuld met sectorspecifieke cyberbeveiligingsstrategieën, bijvoorbeeld op het gebied van financiële diensten[28], energie, vervoer en gezondheid[29].

De Commissie heeft reeds gewezen op de specifieke vraagstukken met betrekking tot **aansprakelijkheid** die nieuwe digitale technologieën met zich meebrengen[30] en er wordt gewerkt aan een analyse van de implicaties; in juni 2018 zullen volgende stappen worden gezet. Cyberbeveiliging doet voor bedrijven en toeleveringsketens vragen rijzen over de toewijzing van de schade en indien deze vragen niet worden beantwoord, zal dit de ontwikkeling van een sterke eengemaakte markt voor cyberbeveiligingsproducten en -diensten belemmeren.

Tot slot is het voor de succesvolle ontwikkeling van de eengemaakte EU-markt ook van belang dat er bij het handels- en investeringsbeleid rekening wordt gehouden met cyberbeveiliging. De gevolgen van buitenlandse verwervingen van kritieke technologieën – waarvan cyberbeveiliging een belangrijk voorbeeld is – vormen een cruciaal onderdeel van het kader voor de **screening van directe buitenlandse investeringen in de Europese Unie**[31], dat het mogelijk moet maken om investeringen uit derde landen te screenen om redenen van veiligheid en openbare orde. Bovendien zijn er door vereisten inzake cyberbeveiliging reeds handelsbelemmeringen ontstaan voor goederen en diensten uit de EU in belangrijke sectoren op een aantal markten van derde landen. Het Europees kader voor cyberbeveiligingscertificering zal de internationale positie van Europa verder versterken en moet gepaard gaan met blijvende inspanningen voor de ontwikkeling van mondiale normen voor zware beveiliging en overeenkomsten inzake wederzijdse erkenning.

### 2.3 Volledige uitvoering van de richtlijn voor de beveiliging van netwerk- en informatiesystemen

Aangezien de belangrijkste instrumenten voor cyberbeveiliging zich vandaag op het nationale niveau bevinden, heeft de EU erkend dat de normen moeten worden aangescherpt. Grootschalige cyberincidenten treffen zelden slechts één lidstaat, aangezien belangrijke sectoren (bv. bankwezen, energie of vervoer) in toenemende mate mondiaal actief zijn, afhankelijk zijn van digitale technologie en onderling verbonden zijn.

---

[25] De gecoördineerde bekendmaking van kwetsbaarheden is een vorm van samenwerking waardoor beveiligingsonderzoekers kwetsbaarheden (gemakkelijker) kunnen melden aan de eigenaar of verkoper van het informatiesysteem, zodat de organisatie de zwakke plek correct en op tijd kan opsporen en verhelpen voordat gedetailleerde informatie hierover wordt vrijgegeven aan derden of het grote publiek.

[26] Bijvoorbeeld: Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, Enisa, 2016.

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure.

[28] Bij de komende werkzaamheden van de Commissie met betrekking tot financiële technologie zal ook aandacht worden besteed aan cyberbeveiliging in de financiële sector.

[29] Bijvoorbeeld in de energiesector, waar enerzijds zeer oude en anderzijds geavanceerde informatietechnologieën worden gebruikt, met name met het oog op de realtimevereisten van het elektriciteitsnet.

[30] COM(2017) 228 final.

[31] COM(2017) 478 final.

De richtlijn voor de beveiliging van netwerk- en informatiesystemen (de "NIS-richtlijn") is het eerste stuk EU-wetgeving betreffende cyberbeveiliging[32]. Met deze richtlijn moet de weerbaarheid worden vergroot door de nationale vermogens inzake cyberbeveiliging te verbeteren, de samenwerking tussen de lidstaten aan te zwengelen en ondernemingen in belangrijke economische sectoren te verplichten doeltreffende risicobeheerspraktijken toe te passen en ernstige incidenten aan de nationale autoriteiten te melden. Deze verplichtingen gelden ook voor aanbieders van drie essentiële soorten internetdiensten: cloudcomputing, zoekmachines en onlinemarktplaatsen. Het doel is om tot een sterkere en systematischere aanpak te komen en de doorstroming van informatie te verbeteren.

Voor de cyberweerbaarheid van de EU is het van essentieel belang dat de richtlijn uiterlijk in mei 2018 door alle lidstaten volledig is uitgevoerd. Het proces steunt op de gezamenlijke inspanningen van de lidstaten, wat in het najaar van 2017 zal resulteren in richtsnoeren voor een meer geharmoniseerde uitvoering, met name met betrekking tot aanbieders van essentiële internetdiensten. Als onderdeel van dit cyberbeveiligingspakket komt de Commissie ook met een mededeling[33] om de lidstaten bij hun inspanningen te ondersteunen door goede praktijken uit de lidstaten aan te reiken voor de uitvoering van de richtlijn en richtsnoeren te verstrekken over de wijze waarop de richtlijn in de praktijk moet functioneren.

Op het gebied van informatiedoorstroming moet de richtlijn nog worden aangevuld. Zo heeft de richtlijn alleen betrekking op de belangrijkste strategische sectoren, maar zou een soortgelijke aanpak logischerwijze ook moeten worden toegepast door alle belanghebbenden die door cyberaanvallen worden getroffen, zodat de kwetsbaarheden en toegangspunten voor cyberaanvallen systematisch kunnen worden beoordeeld. Bovendien liggen er nog een aantal obstakels op de weg naar samenwerking en informatie-uitwisseling tussen de publieke en particuliere sectoren. Regeringen en overheden staan weigerachtig tegenover het delen van informatie over cyberbeveiliging uit angst dat ze op die manier de nationale veiligheid of het concurrentievermogen in het gedrang zouden brengen. Particuliere ondernemingen zijn dan weer huiverig om informatie over de gebreken in hun cyberbeveiliging en de daaruit voortvloeiende verliezen te delen uit angst dat ze zo gevoelige bedrijfsinformatie prijsgeven, hun reputatie op het spel zetten of de regels inzake gegevensbescherming zouden schenden[34]. Er is voor publiek-private partnerschappen meer onderling vertrouwen nodig zodat er nauwer kan worden samengewerkt en informatie kan worden uitgewisseld in een groter aantal sectoren. De centra voor informatie-uitwisseling en -analyse spelen een bijzonder belangrijke rol om het nodige vertrouwen te wekken met het oog op informatie-uitwisseling tussen de particuliere en de publieke sectoren. Er zijn al enkele eerste stappen gezet met betrekking tot specifieke kritieke sectoren, zoals de luchtvaart (oprichting van het Europees centrum voor cyberbeveiliging in de luchtvaart)[35] en de energiesector (ontwikkeling van centra voor informatie-uitwisseling en -analyse)[36]. De Commissie zal, met de steun van het Enisa, ten

---

[32] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

[33] COM (2017)476 final.

[34] "Cybersecurity in the European Digital Single Market" (cyberbeveiliging op de Europese eengemaakte digitale markt), groep op hoog niveau van wetenschappelijk adviseurs, maart 2017 Een specifiek vraagstuk is dat van de bedrijfsgeheimen, met betrekking waartoe in de mededeling van juli 2016 over het versterken van het Europese cyberbeveiligingssysteem wordt gewezen op de bestaande terughoudendheid om cyberdiefstal van bedrijfsgeheimen te melden en op het belang van betrouwbare rapportagekanalen die de vertrouwelijkheid waarborgen.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa

[36] Er bestaan organisaties zonder winstoogmerk die door hun leden worden gedragen en uit private en publieke entiteiten bestaan, en die tot doel hebben informatie uit te wisselen over cyberdreigingen, -risico's, -

volle bijdragen aan deze aanpak en noodzakelijkerwijs een versnelling hoger schakelen met betrekking tot sectoren die essentiële diensten leveren, zoals vastgesteld in de NIS-richtlijn.

### 2.4 Weerbaarheid door snelle noodrespons

De schade door een cyberaanval kan worden beperkt als er snel en doeltreffend wordt gereageerd. Dit toont ook aan dat overheidsinstanties niet machteloos staan tegenover cyberaanvallen en versterkt het vertrouwen. Wat de respons van de EU-instellingen zelf betreft, moeten de cyberbeveiligingsaspecten worden geïntegreerd in de bestaande crisisbeheersingsmechanismen van de EU: de geïntegreerde EU-regeling politieke crisisrespons, gecoördineerd door het voorzitterschap van de Raad[37], en de algemene systemen voor snelle waarschuwing van de EU[38]. Als een lidstaat moet reageren op een cyberincident of -aanval van bijzonder ernstige aard, kan dit voldoende reden zijn om een beroep te doen op de solidariteitsclausule van de EU[39].

Om snel en doeltreffend te kunnen reageren is er ook een snel mechanisme voor informatie-uitwisseling tussen alle belangrijke actoren op nationaal en EU-niveau nodig, wat dan weer betekent dat er duidelijkheid moet bestaan over hun respectieve taken en verantwoordelijkheden. De Commissie heeft instellingen en lidstaten geraadpleegd over een "blauwdruk" voor een doeltreffend proces om in geval van een grootschalig cyberincident operationeel te reageren op Unie- en lidstaatniveau. In de **blauwdruk** – die in een mededeling[40] van dit pakket wordt gepresenteerd – wordt uitgelegd hoe cyberbeveiliging wordt opgenomen in de bestaande crisisbeheersingsmechanismen op EU-niveau en worden de doelstellingen en samenwerkingsvormen tussen de lidstaten onderling en tussen de lidstaten en de betrokken instellingen, diensten, agentschappen en organen van de EU[41] beschreven om op grootschalige cyberincidenten en -crises te reageren. In de aanbeveling wordt de lidstaten en de EU-instellingen ook verzocht een EU-kader voor respons op cybercrises vast te stellen om de blauwdruk in praktijk te brengen. De blauwdruk zal regelmatig worden getest bij cyberbeveiligings- en andere crisisbeheersingsoefeningen[42] en zo nodig worden bijgewerkt.

Aangezien cyberincidenten aanzienlijke gevolgen kunnen hebben voor de werking van de economie en voor het dagelijkse leven van mensen, zou de optie van een **cyberbeveiligingsnoodfonds** kunnen worden onderzocht, naar het voorbeeld van dergelijke crisismechanismen op andere beleidsterreinen van de EU. Zo zouden lidstaten tijdens of na een ernstig incident hulp kunnen zoeken op EU-niveau, op voorwaarde dat de lidstaat voorafgaand aan het incident een solide cyberbeveiligingssysteem heeft ingesteld, met inbegrip van de volledige uitvoering van de NIS-richtlijn en beproefde risicobeheersings- en toezichtskaders op nationaal niveau. Met een dergelijk fonds – dat de bestaande mechanismen voor crisismanagement op EU-niveau zou aanvullen – kan snelle-responsvermogen worden

---

preventie, -schadebeperking en -respons. Zie bv. de European Energy Information Sharing and Analysis Centres (Europese centra voor informatie-uitwisseling en -analyse in de energiesector – http://www.ee-isac.eu).

37 Hierdoor kan de respons op grote sectoroverschrijdende crises worden gecoördineerd op het hoogste politieke niveau.

38 Deze maken het mogelijk om intern informatie uit te wisselen en coördinatie tot stand te brengen met betrekking tot nieuwe multisectorale crises of voorspelbare of onmiddellijke dreigingen die een optreden op EU-niveau vereisen.

39 Krachtens artikel 222 van het Verdrag betreffende de werking van de Europese Unie.

40 C(2017) 6100 final.

41 Met inbegrip van Europol, Enisa, het computercrisisteam voor de EU-instellingen en -agentschappen (CERT-EU) en het Centrum van de Europese Unie voor de analyse van inlichtingen (EU-Intcen).

42 Zoals de door het Enisa georganiseerde oefeningen: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

ingezet en kunnen specifieke noodmaatregelen worden gefinancierd, zoals de vervanging van gekraakte apparatuur of het gebruik van beperkings- of responsinstrumenten, waarbij kan worden geput uit nationale expertise zoals gebeurt voor het Uniemechanisme voor civiele bescherming.

### 2.5 Een kennisnetwerk voor cyberbeveiliging met een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging

Technologische cyberbeveiligingsinstrumenten zijn strategische troeven, maar ook essentiële groeitechnologieën voor de toekomst. In het strategische belang van de EU moet ervoor worden gezorgd dat de Unie de essentiële capaciteiten behoudt en ontwikkelt om haar digitale economie, maatschappij en democratie veilig te stellen, de kritieke hardware en software te beschermen en essentiële cyberbeveiligingsdiensten te verstrekken.

Het in 2016 opgezette publiek-private partnerschap voor cyberbeveiliging[43] was een belangrijke eerste stap en zal tegen 2020 tot een totale investering van maximaal 1,8 miljard EUR leiden. De omvang van de investeringen die er in andere delen van de wereld zitten aan te komen[44], wijzen er echter op dat de EU ervoor moet zorgen dat er meer wordt geïnvesteerd en dat de capaciteiten niet versnipperd worden over de hele EU.

De EU kan een meerwaarde bieden gezien de complexiteit van cyberbeveiligingstechnologie, de vereiste grootschalige investeringen en de behoefte aan oplossingen die in heel de EU werken. Voortbouwend op de werkzaamheden van de lidstaten en het publiek-private partnerschap, zou in een volgende fase het cyberbeveiligingsvermogen van de EU worden versterkt met een **netwerk van kenniscentra voor cyberbeveiliging**[45], waarin een **Europees onderzoeks- en kenniscentrum voor cyberbeveiliging** centraal zou staan. Dit netwerk en het bijbehorende centrum zouden de ontwikkeling en inzet van cyberbeveiligingstechnologie bevorderen en een aanvulling vormen op de inspanningen inzake capaciteitsopbouw die op dit gebied zowel op EU- als nationaal niveau worden geleverd. De Commissie zal een effectbeoordeling uitvoeren om de beschikbare opties te onderzoeken, zoals de mogelijkheid om een gemeenschappelijke onderneming op te richten, met het oog op de creatie van deze structuur in 2018.

Als eerste stap – en als bijdrage aan het toekomstige denkproces – zal de Commissie voorstellen een proeffase op te starten in het kader van Horizon 2020 om de nationale centra samen te brengen in een netwerk en zo een nieuwe impuls te geven aan de ontwikkeling van cyberbeveiligingscompetentie en -technologie. Hiertoe is zij voornemens op korte termijn een kapitaalsinjectie van 50 miljoen EUR voor te stellen. Deze activiteit zal een aanvulling vormen op de lopende uitvoering van het publiek-private partnerschap voor cyberbeveiliging.

In eerste instantie zouden het netwerk en het centrum erop gericht zijn de onderzoeksinspanningen te bundelen en vorm te geven. Om de ontwikkeling van industriële vermogens te ondersteunen, zou het centrum als beheerder van projecten inzake vermogen kunnen optreden en multinationale projecten kunnen behandelen. Dit zou ook een extra impuls geven aan de innovatie en het concurrentievermogen van de Europese industrie op het wereldtoneel als het gaat om de ontwikkeling van digitale technologieën van de volgende generatie (bijv. artificiële intelligentie, quantumcomputing, blockchain en beveiligde digitale

[43] C(2016) 4400 final.

[44] Alleen al in 2017 investeert de VS 19 miljard dollar in cyberbeveiliging, een stijging met 35 % ten opzichte van 2016. Het Witte Huis, kabinet van de perschef: 'Fact Sheet: Cybersecurity National Action Plan', 9 februari 2016.

[45] Het netwerk zou bestaan uit huidige en toekomstige cyberbeveiligingscentra in de lidstaten, waarvan de leden meestal openbare onderzoeksinstellingen en laboratoria zijn.

identiteiten) en ervoor zorgen dat in de EU gevestigde ondernemingen toegang hebben tot massagegevens – allemaal belangrijk voor de cyberbeveiliging van de toekomst. Het centrum zou ook voortbouwen op het werk van de EU om de infrastructuur voor high performance computing op te schalen: dit is van essentieel belang voor de analyse van grote hoeveelheden gegevens, snelle encryptie en decryptie van gegevens, identiteitscontrole, de simulatie van cyberaanvallen en de analyse van videomateriaal[46].

Het netwerk van kenniscentra zou ook de vermogens moeten hebben om de industrie bij te staan met tests en simulaties ter ondersteuning van de in deel 2.2 beschreven cyberbeveiligingscertificering. Door de betrokkenheid van dit netwerk bij het volledige scala van cyberbeveiligingswerkzaamheden van de EU zouden zijn streefdoelen voortdurend worden aangepast aan de behoeften. Het centrum zou niet alleen hoge cyberbeveiligingsnormen nastreven in technologieën en systemen voor cyberbeveiliging, maar ook in de ontwikkeling van geavanceerde vaardigheden voor professionals, door oplossingen en modellen aan te reiken voor nationale inspanningen inzake digitale vaardigheden. In dat opzicht zou het centrum ook op EU-niveau de cyberbeveiligingsvermogens verhogen en voortbouwen op synergieën met onder meer het Enisa, CERT-EU, het mogelijke toekomstige cyberbeveiligingsnoodfonds en nationale CSIRT's.

Het kennisnetwerk zal in het bijzonder moeten focussen op het gebrek aan Europese capaciteit voor de beoordeling van de **encryptie** van producten en diensten die door burgers, bedrijven en overheden op de digitale eengemaakte markt worden gebruikt. Sterke encryptie vormt de grondslag voor veilige digitale identificatiesystemen die cruciaal zijn voor doeltreffende cyberbeveiliging[47], zorgt voor de beveiliging van intellectuele eigendom, voor de bescherming van grondrechten, zoals de vrijheid van meningsuiting en de bescherming van persoonsgegevens, en voor veilige e-commerce[48].

Aangezien de civiele en defensiemarkten voor cyberbeveiliging in de EU voor gemeenschappelijke uitdagingen staan[49] en gebruikmaken van dezelfde technologieën voor tweeërlei gebruik die nauwe samenwerking op kritieke gebieden vereisen, zouden het netwerk en het centrum in een tweede fase kunnen worden uitgebreid met een cyberdefensiedimensie, met volledige inachtneming van de bepalingen van het Verdrag in verband met het gemeenschappelijk veiligheids- en defensiebeleid. Naast het technologische aspect zou de defensiedimensie ook kunnen bijdragen aan de samenwerking tussen de lidstaten op het gebied van cyberdefensie, onder meer m.b.t. informatie-uitwisseling, situationeel bewustzijn, verwerving van expertise en gecoördineerde reacties, en hen ondersteunen bij de ontwikkeling van gemeenschappelijke vermogens. Het zou ook dienst kunnen doen als platform om de lidstaten toe te laten de EU-prioriteiten inzake cyberdefensie te bepalen, gemeenschappelijke oplossingen te onderzoeken, aan de ontwikkeling van gemeenschappelijke strategieën bij te dragen, gezamenlijke opleidingen, oefeningen en tests inzake cyberdefensie op Europees niveau te bevorderen en de classificatie en standaardisatie inzake cyberdefensie te ondersteunen, waarbij het centrum een ondersteunende en adviserende rol zou spelen. Met het oog op bovengenoemde activiteiten zou het centrum volledig complementair en nauw moeten samenwerken met het Europees Defensieagentschap op het gebied van cyberdefensie en met

[46] COM(2012) 45 final en COM(2016) 178 final.

[47] De Commissie zal in het kader van Horizon 2020 al een nieuwe Horizonprijs van 4 miljoen EUR uitloven voor de beste innovatieve oplossingen voor naadloze online-authenticatiemethoden.

[48] "Cybersecurity in the European Digital Single Market" (cyberbeveiliging op de Europese eengemaakte digitale markt), groep op hoog niveau van wetenschappelijk adviseurs, maart 2017

[49] "Study on synergies between the civilian and the defence cybersecurity markets"(Optimity; SMART 2014-0059).

het Enisa op het gebied van de cyberweerbaarheid. In deze defensiedimensie zou rekening worden gehouden met het proces dat op gang is gebracht door de discussienota over de toekomst van de Europese defensie.

De hoge mate van weerbaarheid die nodig is voor cyberdefensie, vraagt om specifieke gerichte onderzoeks- en technologie-inspanningen. De door ondernemingen ontwikkelde cyberdefensieprojecten of -technologieën zouden zowel in de onderzoeks- als ontwikkelingsfase in aanmerking kunnen komen voor financiering uit het Europees Defensiefonds[50]. In dit verband zouden bepaalde gebieden, zoals encryptiesystemen op basis van kwantumtechnologie, cybersituationeel bewustzijn, biometrische toegangsbeveiligingssystemen, opsporing van geavanceerde persistente dreigingen, of datamining, bijzonder relevant kunnen zijn. De hoge vertegenwoordiger, het Europees Defensieagentschap en de Commissie zullen de lidstaten ondersteunen bij het bepalen van terreinen waarop gemeenschappelijke cyberbeveiligingsprojecten in aanmerking zouden kunnen komen voor financiering uit het Europees Defensiefonds.

## 2.6 Bouwen aan solide cybervaardigheden in de EU

Cyberbeveiliging heeft een sterke onderwijskundige dimensie. Doeltreffende cyberbeveiliging is in sterke mate afhankelijk van de vaardigheden van de betrokken personen. Maar voorspeld wordt dat er in 2022 in de Europese private sector een tekort zal zijn van 350 000 werknemers met vaardigheden op het gebied van cyberbeveiliging[51]. Op alle niveaus zouden opleidingen in cyberbeveiliging moeten worden aangeboden, te beginnen met regelmatige opleidingen voor personeel in de sector van de cyberbeveiliging, aanvullende scholing over cyberbeveiliging voor alle ICT-specialisten en nieuwe specifieke studierichtingen op het gebied van cyberbeveiliging. Om aan de vraag naar versnelde onderwijs- en opleidingsmogelijkheden te voldoen, moeten sterke academische kenniscentra worden opgericht die kunnen voortbouwen op richtsnoeren van een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging en van het Enisa. Dit alles moet tot doel hebben dat het vanzelfsprekend wordt om de beveiligingsbeginselen al in de ontwerpfase in ICT-producten en -systemen in te bouwen. Cyberbeveiligingsonderwijs mag niet alleen gericht zijn op IT-professionals, maar moet ook in de leerplannen van andere studiegebieden worden geïntegreerd, zoals techniek, bedrijfsbeheer, ondernemingsrecht, en in sectorspecifieke opleidingen. Tot slot moeten leerkrachten en leerlingen in het lager en middelbaar onderwijs, bij het verwerven van digitale vaardigheden, bewust worden gemaakt van cybercriminaliteit en cyberbeveiliging.

De EU moet hier samen met de lidstaten ook toe bijdragen door voort te bouwen op de werkzaamheden van de coalitie voor digitale vaardigheden en banen[52] en door bijvoorbeeld stageregelingen met betrekking tot cyberbeveiliging op te zetten voor kleine en middelgrote ondernemingen.

## 2.7 Bevordering van cyberhygiëne en cyberbewustzijn

[50] In het ontwikkelingsprogramma voor de Europese defensie-industrie zal nu al voorrang worden gegeven aan cyberdefensieprojecten, en cyberdefensie wordt een van de thema's van de in 2018 te lanceren oproep tot het indienen van voorstellen.

[51] Global Information Security Workforce Study 2017. Op wereldvlak zijn er 1,8 miljoen cybervaardige werknemers te kort.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

Het feit dat zowat 95 % van de cyberincidenten mogelijk wordt gemaakt door een of andere menselijke fout, al dan niet opzettelijk,[53] wijst op een belangrijke menselijke factor. We zijn dus allemaal verantwoordelijk voor onze cyberbeveiliging. Particulieren, ondernemingen en overheidsdiensten moeten zich dus anders gaan gedragen zodat iedereen zich bewust is van de dreiging en over de nodige instrumenten en vaardigheden beschikt om aanvallen snel te herkennen en actief het hoofd te bieden. Mensen moeten een zekere cyberhygiëne in acht nemen en ondernemingen en organisaties moeten passende, op risicoanalyse gebaseerde cyberbeveiligingsprogramma's opzetten en regelmatig bijstellen naarmate het risicolandschap verandert.

De NIS-richtlijn bepaalt niet alleen dat de lidstaten verantwoordelijk zijn om op EU-niveau informatie over cyberaanvallen uit te wisselen, maar ook om beproefde nationale cyberbeveiligingsstrategieën en kaders voor de beveiliging van netwerk- en informatiesystemen op te zetten. Overheidsdiensten op EU- en nationaal niveau moeten het voortouw nemen om deze inspanningen verder te stimuleren.

Ten eerste moeten de lidstaten zorgen voor een maximale beschikbaarheid van cyberbeveiligingsinstrumenten voor burgers en bedrijven. Er moet met name meer worden gedaan om de impact van cybercriminaliteit op eindgebruikers te vermijden en te verzachten. Een bestaand voorbeeld hiervan is de "NoMoreRansom"-campagne van Europol[54], uitgewerkt in nauwe samenwerking met rechtshandhavingsinstanties en cyberbeveiligingsbedrijven, om gebruikers te helpen infecties met ransomware te voorkomen en slachtoffers van een aanval te helpen hun gegevens weer te decrypten. Dergelijke regelingen moeten ook worden ingevoerd voor andere soorten malware op andere gebieden en de EU moet **een portaalsite ontwikkelen om dergelijke instrumenten samen te brengen in een onestopshop** met advies voor gebruikers over de preventie en detectie van malware en met links naar rapporteringsmechanismen.

Ten tweede moeten de lidstaten vaart zetten achter het **gebruik van meer cyberbeveiligingsinstrumenten bij de ontwikkeling van e-overheidsdiensten** en ook het kennisnetwerk ten volle benutten. Het gebruik van beveiligde identificatiemiddelen moet worden bevorderd, voortbouwend op het EU-kader voor elektronische identificatie en vertrouwensdiensten voor elektronische transacties op de interne markt dat sinds 2016 van kracht is en dat een voorspelbaar regelgevingsklimaat voor beveiligde en naadloze elektronische interacties tussen bedrijven, burgers en overheidsinstanties schept[55]. Voorts moeten openbare instellingen, met name instellingen die essentiële diensten aanbieden, ervoor zorgen dat hun personeel opgeleid is op het gebied van cyberbeveiliging.

Ten derde moeten lidstaten in **bewustmakingscampagnes** voorrang geven aan cyberbewustzijn, onder meer in scholen, universiteiten, het bedrijfsleven en onderzoeksinstellingen. De maand van de cyberbeveiliging, een door het Enisa gecoördineerd initiatief dat ieder jaar in oktober plaatsvindt, zal worden uitgebreid om meer mensen te bereiken dankzij een gezamenlijke communicatie-inspanning op EU- en nationaal niveau. Even belangrijk is bewustmaking met betrekking tot online **desinformatiecampagnes en fakenieuws** op sociale media die specifiek bedoeld zijn om de Europese waarden en

[53] IBM "The Cybersecurity Intelligence Index" 2014, referred to in Securitymagazine.com, 19 juni 2014.

[54] https://www.nomoreransom.org/

[55] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS-verordening). Voorts draagt de Europese Commissie via het CEF-programma bouwstenen en instrumenten aan voor de interoperabiliteit van elektronische identiteitskaarten en e-handtekeningen (bv. Trusted Lists Browsers).

democratische processen te ondermijnen. Hoewel dit in de eerste plaats een nationale verantwoordelijkheid blijft – ook met betrekking tot de Europese parlementsverkiezingen – is aangetoond dat het bundelen van expertise en het delen van ervaringen op Europees niveau helpt bij het bepalen van actiepunten[56].

Ook is er een sterke rol weggelegd voor de **industrie** in het algemeen en voor fabrikanten en verleners van digitale diensten in het bijzonder. Zij moeten de gebruikers (particulieren, bedrijven en overheden) de instrumenten aanbieden om verantwoordelijkheid op te nemen voor hun eigen online gedrag en duidelijk maken dat cyberhygiëne een onmisbaar onderdeel is van het consumentenaanbod[57]. Om zwakke punten op te sporen en te verhelpen moet de industrie ernaar streven interne processen uit te werken om zwakke punten te onderzoeken, te sorteren en te verhelpen, ongeacht of de oorzaak van de potentiële kwetsbaarheid buiten of binnen de betrokken onderneming ligt.

**Kernacties**

- Volledige uitvoering van de richtlijn voor de beveiliging van netwerk- en informatiesystemen;
- Snelle vaststelling door het Europees Parlement en de Raad van de verordening tot vaststelling van een nieuw mandaat voor het Enisa en een Europees certificeringskader[58];
- Een gezamenlijk initiatief van de Commissie en de industrie ter bepaling van een "zorgplichtbeginsel" om producten/software minder kwetsbaar te maken en de toepassing van "ingebouwde beveiliging" te stimuleren;
- Snelle uitvoering van de blauwdruk voor respons op grote grensoverschrijdende incidenten;
- Door middel van een effectbeoordeling de mogelijkheid onderzoeken om in 2018, voortbouwend op een directe testfase, een Commissievoorstel in te dienen voor de oprichting van een netwerk van kenniscentra voor cyberbeveiliging en een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging;
- De lidstaten ondersteunen bij het bepalen van terreinen waarop gemeenschappelijke cyberbeveiligingsprojecten in aanmerking zouden kunnen komen voor financiering uit het Europees Defensiefonds;
- Een onestopshop voor de hele EU om slachtoffers van cyberaanvallen te helpen, informatie over de meest recente dreigingen te verstrekken en zowel praktisch advies als cyberbeveiligingsinstrumenten aan te reiken;
- Maatregelen van de lidstaten om cyberbeveiliging onder de aandacht van het brede publiek te brengen door middel van opleidingsprogramma's, e-overheidsinitiatieven en bewustmakingscampagnes;
- Maatregelen van de bedrijfswereld om personeelsleden beter te trainen met betrekking tot cyberbeveiliging en het concept van ingebouwde beveiliging toe te passen op hun producten, diensten en processen.

[56] Een voorbeeld is de East StratCom Task Force die in 2015 door de lidstaten en de hoge vertegenwoordiger is opgericht als antwoord op de aanhoudende desinformatiecampagnes uit Rusland. Het team werkt aan de ontwikkeling van communicatieproducten en -campagnes om in de regio van het Oostelijk Partnerschap het EU-beleid uit te leggen.

[57] Sommige fabrikanten zijn reeds bekend met dit concept aangezien een deel van de Europese productregelgeving (zoals Richtlijn 2006/42/EG betreffende machines) de beginselen van "ingebouwde beveiliging" voorschrijft.

[58] COM(2017) 477 final.

## 3. DOELTREFFENDE AFSCHRIKKING VOOR CYBERCRIMINELEN IN DE EU

Om op een doeltreffende manier afschrik te wekken, moet een kader worden opgezet met maatregelen die zowel geloofwaardig als ontradend zijn voor potentiële cybercriminelen en -aanvallers. Zolang hun eigen falen het enige is dat statelijke en niet-statelijke cyberaanvallers te vrezen hebben, zullen ze weinig reden hebben om niet te proberen. Een doeltreffendere strafrechtelijke respons met de nadruk op opsporing, traceerbaarheid en vervolging van cybercriminelen is van essentieel belang om hen op een doeltreffende manier af te schrikken. Daarbij komt nog dat de EU haar lidstaten moet ondersteunen bij de ontwikkeling van cyberbeveiligingsvermogens voor tweeërlei gebruik. Wij zullen het tij pas kunnen doen keren als er een hogere pak- en strafkans is voor cyberaanvallers. Cyberaanvallen moeten onmiddellijk worden onderzocht en de daders moeten voor de rechter worden gebracht, of er moeten maatregelen worden genomen voor een passend politiek of diplomatiek antwoord. Bij een grote crisis met een grote internationale dimensie en defensiedimensie zou de hoge vertegenwoordiger de Raad opties voor een passende respons kunnen voorleggen.

In 2013 is met de vaststelling van de Richtlijn over aanvallen op informatiesystemen[59] al een eerste stap gezet naar een betere strafrechtelijke respons op cyberaanvallen. Deze richtlijn voorzag in minimumvoorschriften voor de definitie van strafbare feiten en sancties op het gebied van aanvallen op informatiesystemen en in operationele maatregelen ter bevordering van de samenwerking tussen de autoriteiten. Dit heeft ertoe geleid dat cyberaanvallen in de lidstaten op een meer vergelijkbaar niveau strafbaar worden gesteld, wat de grensoverschrijdende samenwerking vergemakkelijkt tussen de rechtshandhavingsautoriteiten die deze strafbare feiten onderzoeken. De richtlijn beschikt echter nog over niet aangeboord potentieel dat ten volle zou kunnen worden benut als de lidstaten alle bepalingen volledig uitvoeren[60]. De Commissie zal de lidstaten blijven ondersteunen bij de uitvoering van de richtlijn en ziet momenteel geen reden om wijzigingen voor te stellen.

### 3.1 Identificatie van kwaadwillige actoren

Als we de kansen willen vergroten dat de daders voor het gerecht worden gebracht, moeten we snel onze capaciteit verbeteren om de verantwoordelijken van cyberaanvallen te identificeren. Rechtshandhavingsautoriteiten hebben een hele kluif aan het vinden van gegevens, meestal in de vorm van digitale sporen, die nuttig zijn voor onderzoeken naar cybercriminaliteit. Om doeltreffend onderzoek te kunnen voeren, moeten wij ons technologische vermogen dus opschroeven, onder meer door de eenheid cybercriminaliteit van Europol te versterken met cyberdeskundigen. Europol is een belangrijke speler geworden voor de ondersteuning van lidstaten in onderzoeken waarbij meerdere jurisdicties betrokken zijn. Het agentschap moet uitgroeien tot een centrum van expertise voor de rechtshandhaving door de lidstaten met betrekking tot online onderzoeken en digitale forensische wetenschap.

De wijdverbreide praktijk om verschillende gebruikers – soms zelfs duizenden – gebruik te laten maken van eenzelfde IP-adres, maakt het technisch zeer moeilijk om onderzoek te doen naar kwaadwillig online gedrag. Hierdoor is het soms ook nodig om, als het bijvoorbeeld om ernstige misdrijven zoals seksueel misbruik van kinderen gaat, een groot aantal gebruikers te onderzoeken om één dader te identificeren. Daarom wil de EU het gebruik van het nieuwe protocol (IPv6) aanmoedigen, aangezien hiermee één IP-adres aan één gebruiker kan worden toegekend, hetgeen duidelijke voordelen oplevert voor rechtshandhaving en onderzoeken met

[59] Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen.

[60] COM(2017) 474 final.

betrekking tot cyberbeveiliging. Als een eerste stap ter bevordering van het gebruik van dit protocol zal de Commissie de vereiste om over te stappen op IPv6 opnemen in al haar beleidsmaatregelen, inclusief in de vereisten voor aanbestedingen, project- en onderzoeksfinanciering, en zal ze ondersteuning bieden voor het noodzakelijke opleidingsmateriaal. Daarnaast moeten de lidstaten overwegen om vrijwillige overeenkomsten te sluiten met aanbieders van internetdiensten om vaart te zetten achter de invoering van IPv6.

*België is, mede dankzij publiek-private samenwerking, de nummer één ter wereld*[61] *wat betreft de invoering van IPv6: de belanghebbenden zijn overeengekomen om, als onderdeel van een vrijwillige zelfregulerende maatregel, het delen van een IP-adres te beperken tot maximaal 16 gebruikers, hetgeen de overgang naar IPv6 heeft gestimuleerd*[62].

Er moet algemeen gezien meer online verantwoordingsplicht komen. Dit betekent dat er maatregelen moeten komen ter voorkoming van misbruik van domeinnamen voor de verspreiding van spamberichten of phishing. Daartoe zal de Commissie werken aan de verbetering van de werking van de WHOIS-systemen[63] voor domeinnamen en IP-adressen en aan een grotere beschikbaarheid en juistheid van de daarin vervatte gegevens, in aansluiting op de inspanningen van de Internet Corporation for Assigned Names and Numbers[64].

### 3.2 De rechtshandhavingsrespons versterken

Doeltreffend **onderzoek** naar en **vervolging** van cybercriminaliteit zijn belangrijke afschrikmiddelen tegen cyberaanvallen. Het huidige procedurele kader moet echter beter aansluiten op het internettijdperk[65]. De snelheid van de cyberaanvallen kan een overweldigend effect hebben op onze procedures en ook bijzondere behoeften voor snelle grensoverschrijdende samenwerking creëren. Daarom zal de Commissie, zoals reeds aangekondigd in de Europese veiligheidsagenda, begin 2018 voorstellen doen om **grensoverschrijdende toegang tot elektronisch bewijsmateriaal te vergemakkelijken**. Parallel hieraan voert de Commissie praktische maatregelen in om de grensoverschrijdende toegang tot elektronisch bewijsmateriaal in strafrechtelijke onderzoeken te vergemakkelijken, met inbegrip van subsidies voor opleiding op het vlak van grensoverschrijdende samenwerking, de ontwikkeling van een elektronisch platform voor informatie-uitwisseling binnen de EU en de standaardisering van formulieren voor justitiële samenwerking tussen de lidstaten.

Ook de verschillende gerechtelijke procedures voor de vergaring van elektronisch bewijsmateriaal in onderzoeken naar cybercriminaliteit die in de verschillende lidstaten bestaan, maken een doeltreffende vervolging moeilijk. Dit kan worden verholpen door te werken aan de vaststelling van gemeenschappelijke forensische normen. Daarnaast moeten de

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Een vraag- en antwoordprotocol dat op grote schaal wordt gebruikt voor opzoekingen in databanken met gegevens over de geregistreerde gebruikers of cessionarissen van een internetbron.

64 De Internet Corporation for Assigned Names and Numbers (ICANN) is een non-profitorganisatie die verantwoordelijk is voor de coördinatie van het onderhoud en de procedures van verscheidene databanken met betrekking tot de naamruimten van het internet.

65 De (virtuele) centrale command-and-controlserver van het Avalanche-botnet wisselde iedere vijf minuten van fysieke servers en domeinen, om maar een voorbeeld te noemen.

forensische vermogens worden versterkt om de traceerbaarheid en de toewijzing te verbeteren. Een van de stappen zou de verdere ontwikkeling van de forensische vermogens van Europol zijn, waarbij de bestaande budgettaire en personele middelen van het Europees Centrum voor de bestrijding van cybercriminaliteit, dat onderdeel is van Europol, zouden worden aangepast aan de groeiende behoefte aan operationele ondersteuning van grensoverschrijdende onderzoeken naar cybercriminaliteit. Een andere stap zou zijn om de hierboven beschreven technologische focus ook toe te passen op encryptie, door na te gaan hoe het misbruik van encryptie door criminelen grote uitdagingen met zich meebrengt in de strijd tegen zware criminaliteit, zoals terrorisme en cybercriminaliteit. De Commissie zal de resultaten van de huidige discussie over de **rol van encryptie in strafrechtelijke onderzoeken**[66] tegen oktober 2017 bekendmaken[67].

Gezien het grenzeloze karakter van het internet, biedt het kader voor internationale samenwerking van het door de Raad van Europa aangenomen **Verdrag van Boedapest inzake cybercriminaliteit**[68] een heterogene groep van landen de mogelijkheid om gebruik te maken van een optimale wettelijke norm voor de verschillende nationale wetten inzake cybercriminaliteit. Momenteel wordt een mogelijke toevoeging van een protocol bij het Verdrag onderzocht[69], wat een goede gelegenheid zou zijn om de kwestie van grensoverschrijdende toegang tot elektronisch bewijsmateriaal in een internationale context aan te kaarten. De EU dringt erop aan dat alle landen passende nationale wetgeving vaststellen en samenwerken binnen het bestaande internationale kader, in plaats van nieuwe internationale rechtsinstrumenten inzake cybercriminaliteit te creëren.

Door de algemene beschikbaarheid van anonimiseringsinstrumenten kunnen criminelen zich gemakkelijker verbergen. Het "**darknet**"[70] biedt criminelen nieuwe mogelijkheden om toegang te krijgen tot materiaal dat seksueel misbruik van kinderen bevat, tot drugs en tot vuurwapens, waarbij ze weinig risico lopen om te worden gepakt[71]. Het is nu ook een belangrijk middel om aan instrumenten te komen die worden gebruikt voor cybercriminaliteit, zoals malware en instrumenten om te hacken. De Commissie zal samen met de belanghebbenden de nationale benaderingswijzen analyseren om nieuwe oplossingen te zoeken. Europol moet onderzoek op het darknet vergemakkelijken en ondersteunen, dreigingen beoordelen, helpen met het bepalen van de jurisdictie en prioriteit geven aan

---

66 Voorzitterschap van de Raad, Conclusies van de Raad Justitie en Binnenlandse Zaken van 8 en 9 december 2016, nr. 15391/16.

67 Achtste voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie van 29 juni 2017 (COM(2017) 354 final).

68 Dit is het eerste internationale verdrag over via het internet en andere computernetwerken gepleegde misdrijven, en betreft met name inbreuken op auteursrechten, computergerelateerde fraude, kinderpornografie, en schendingen van netwerkbeveiliging. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 In 2017 hadden 55 regeringen het door de Raad van Europa aangenomen Verdrag inzake cybercriminaliteit bekrachtigd of waren ze ertoe toegetreden.

69 Mandaat voor de voorbereiding van een ontwerp voor een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit, T-CY (2017)3.

70 Het darknet bestaat uit content in overlaynetwerken die gebruikmaken van het internet, maar waarvoor specifieke software, configuraties of toegangsbevoegdheid nodig is. Het darknet is een klein deel van het deep web, het deel van het web dat niet door zoekmachines wordt geïndexeerd.

71 Opvallende uitzondering zijn twee van de grootste criminele marktplaatsen op het dark web, Alphabay en Hansa, die onlangs offline werden gehaald: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

gevallen met een hoog risico, terwijl de EU een leidende rol kan spelen bij de coördinatie van internationale acties[72].

Een florerende vorm van cybercriminaliteit is het frauduleus gebruik van creditcardgegevens of andere elektronische betaalmiddelen. Betalingsgegevens die door middel van cyberaanvallen worden ontfutseld van online detailhandelaren of andere bonafide bedrijven, worden vervolgens online verhandeld en kunnen door criminelen worden gebruikt om fraude te plegen[73]. De Commissie dient een voorstel in om het afschrikkingseffect te versterken door middel van een **richtlijn betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten**[74]. Deze richtlijn is bedoeld om de bestaande regels op dit gebied te actualiseren en de rechtshandhavingsinstanties beter te wapenen in de strijd tegen deze vorm van criminaliteit.

De rechtshandhavingsinstanties van de lidstaten moeten ook over betere onderzoeksvermogens op het vlak van cybercriminaliteit beschikken en de openbare aanklagers en de rechterlijke macht moeten een beter inzicht krijgen in cybercriminaliteit en onderzoeksmogelijkheden. Eurojust en Europol dragen bij aan de verwezenlijking van deze doelstelling, alsook aan een betere coördinatie, in nauwe samenwerking met gespecialiseerde adviesgroepen binnen het Centrum voor de bestrijding van cybercriminaliteit van Europol en met het netwerk van hoofden van cybercriminaliteitseenheden en openbare aanklagers die gespecialiseerd zijn in de bestrijding van cybercriminaliteit. De Commissie stelt 10,5 miljoen EUR ter beschikking voor de strijd tegen cybercriminaliteit, hoofdzakelijk uit het **Fonds voor interne veiligheid – Politie**. Aangezien opleiding ook een belangrijk element is, heeft de Europese groep voor opleiding in verband met cybercriminaliteit nuttig opleidingsmateriaal ontwikkeld. Dit materiaal moet nu, met de steun van het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving (Cepol), op grote schaal worden bezorgd aan rechtshandhavingsambtenaren.

### 3.3 Publiek-private samenwerking tegen cybercriminaliteit

De doeltreffendheid van de traditionele mechanismen voor rechtshandhaving komt onder druk te staan in de digitale wereld, die grotendeels bestaat uit particuliere infrastructuren en uiteenlopende actoren in verschillende jurisdicties. Om misdaad doeltreffend te kunnen bestrijden, is het daarom van fundamenteel belang dat overheden de samenwerking aangaan met de particuliere sector, zoals het bedrijfsleven en het maatschappelijk middenveld. In dit verband is ook de financiële sector van cruciaal belang en moet de samenwerking met deze sector worden geïntensiveerd. Zo moeten de financiële-inlichtingeneenheden[75] een grotere rol spelen in de strijd tegen cybercriminaliteit.

*Sommige lidstaten hebben al belangrijke stappen gezet. In Nederland werken financiële instellingen en rechtshandhavingsautoriteiten samen in de "Electronic Crimes Taskforce" om online fraude en cybercriminaliteit aan te pakken. Het "German Competence Centre against Cyber Crime" fungeert als operationeel centrum waar zijn leden in nauwe samenwerking met*

[72] Europol speelt al een belangrijke rol op dit gebied. Voor een recent voorbeeld zie: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[73] Fraude is een belangrijke inkomstenbron van de georganiseerde misdaad en is dan ook een faciliterende factor voor andere criminele activiteiten, zoals terrorisme, drugs- en mensenhandel.

[74] COM(2017) 489 final.

[75] Financiële-inlichtingeneenheden fungeren als nationale centra voor de ontvangst en analyse van meldingen van verdachte transacties en andere informatie met betrekking tot witwaspraktijken, daarmee verband houdende gronddelicten en terrorismefinanciering, en voor de verspreiding van de resultaten van die analyse.

*de Duitse federale politie informatie uitwisselen en maatregelen uitwerken om het hoofd te bieden aan cybercriminaliteit. Zestien lidstaten[76] hebben kenniscentra op het gebied van cybercriminaliteit opgericht om de samenwerking tussen rechtshandhavingsautoriteiten, de academische wereld en privépartners te vergemakkelijken bij de ontwikkeling en uitwisseling van beste praktijken, opleidingen en capaciteitsopbouw.*
*De Commissie ondersteunt de oprichting van publiek-private partnerschappen en samenwerkingsmechanismen via specifieke projecten, zoals het "Online Fraud Cyber Centre and Experts Network"[77] ("netwerk van cybercentra en -experts op het gebied van online fraude"), dat een model en standaard voor informatie-uitwisseling in praktijk brengt om het risico op cybercriminaliteit en online fraude te analyseren en in te perken.*

In de context van cybercriminaliteit moeten particuliere ondernemingen informatie over concrete incidenten kunnen delen met rechtshandhavingsinstanties – ook persoonsgegevens – met volledige inachtneming van de regels inzake gegevensbescherming. De hervorming van de gegevensbeschermingsregels van de EU, die in mei 2018 in werking zal treden, voorziet in gemeenschappelijke regels met voorwaarden waaronder rechtshandhavingsinstanties en particuliere instanties kunnen samenwerken. De Europese Commissie zal samenwerken met het Europees Comité voor gegevensbescherming en met belanghebbenden om de beste praktijken op dit gebied vast te stellen en waar passend richtsnoeren te verstrekken.

### 3.4 Versterking van de politieke reactie

In het onlangs goedgekeurde **kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten**[78] ("instrumentarium voor cyberdiplomatie") zijn de maatregelen in het kader van het gemeenschappelijk buitenland- en veiligheidsbeleid vastgesteld, waaronder ook beperkende maatregelen die kunnen worden gebruikt voor een sterkere EU-respons op activiteiten die schadelijk zijn voor de politieke, veiligheids- en economische belangen. Met het kader wordt een belangrijke stap gezet in de ontwikkeling op EU- en lidstaatniveau van de vermogens om dergelijke activiteiten te signaleren en erop te reageren. We zullen hierdoor beter in staat zijn kwaadwillige cyberactiviteiten toe te wijzen, zodat we het gedrag van potentiële agressors kunnen beïnvloeden, tegelijk rekening houdend met het belang van een evenredige respons. De toewijzing aan een staat of een niet-statelijke actor blijft een soeverein politiek besluit, dat gebaseerd is op inlichtingen uit alle bronnen. Met de lidstaten wordt momenteel aan de uitvoering van het kader gewerkt en deze werkzaamheden zouden ook gebeuren in nauwe samenhang met de blauwdruk voor respons op grootschalige cyberaanvallen[79]. Het situationeel bewustzijn dat nodig is om de maatregelen binnen dit kader te kunnen gebruiken, moet, in nauwe samenwerking met de lidstaten en de instellingen van de EU, door IntCen[80] worden samengevoegd, geanalyseerd en gedeeld.

### 3.5 Bouwen aan cyberafschrikking met de defensievermogens van de lidstaten

De lidstaten ontwikkelen al cyberdefensievermogens. Gezien de vervagende grenzen tussen cyberdefensie en cyberbeveiliging, het tweeërlei gebruik van digitale instrumenten en

[76] België, Bulgarije, Tsjechië, Duitsland, Estland, Ierland, Griekenland, Spanje, Frankrijk, Cyprus, Litouwen, Oostenrijk, Polen, Roemenië, Slovenië en het Verenigd Koninkrijk.
[77] Dit initiatief is bedoeld om op EU-niveau tussen banken en rechtshandhavingsinstanties informatie over internetfraude uit te wisselen zodat betalingen aan fraudeurs en geldezels worden vermeden en de daders worden onderzocht en vervolgd. Het wordt medegefinancierd door de EU (Fonds voor interne veiligheid – Politie).
[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/
[79] C(2017) 6100 final.
[80] JOIN(2016) 18 final.

technologieën, en de grote verschillen in benadering tussen de lidstaten, is de EU goed geplaatst om synergieën tussen militaire en civiele inspanningen mee te bevorderen[81].

Lidstaten die over meer geavanceerde cyberbeveiligingsvermogens beschikken en deze vermogens willen bundelen, kunnen overwegen om met de steun van de hoge vertegenwoordiger, de Commissie en het Europees Defensieagentschap een "permanente gestructureerde samenwerking" (PESCO) voor cyberdefensie op te zetten. Hiervoor zou kunnen worden voortgebouwd op de hierboven vermelde werkzaamheden ter bevordering van de industriële capaciteiten en strategische autonomie van de EU. De EU kan ook de interoperabiliteit bevorderen, onder meer door de vermogensontwikkeling, de coördinatie van training en opleiding en de normalisatie-inspanningen voor tweeërlei gebruik te bevorderen.

Ook moet het gemeenschappelijke kader ten volle worden benut om te reageren op hybride dreigingen (waar cyberaanvallen vaak een onderdeel van zijn), met name via de EU-Fusiecel en het onlangs opgerichte Europees Centrum voor de bestrijding van hybride bedreigingen in Helsinki, dat tot taak heeft de strategische dialoog aan te zwengelen en onderzoek en analyse uit te voeren.

De EU zal sterker de nadruk leggen op het EU-beleidskader voor cyberdefensie[82] van 2014, als een instrument voor de verdere integratie van cyberbeveiliging en -defensie in het gemeenschappelijk veiligheids- en defensiebeleid (GVDB). Voor de GVDB-missies en -operaties zelf is cyberweerbaarheid van essentieel belang: er zullen gestandaardiseerde procedures en technische vermogens worden ontwikkeld ter ondersteuning van zowel civiele als militaire missies en operaties, en van de respectieve plannings- en uitvoeringsvermogensstructuren en verleners van informatietechnologiediensten van de EDEO. Om de samenwerking tussen de lidstaten verder te ontwikkelen en de inspanningen van de EU op dit gebied beter te richten, zullen het Europees Defensieagentschap en de EDEO, samen met de diensten van de Commissie, de samenwerking op strategisch niveau bevorderen tussen de beleidsmakers van de lidstaten die zich met cyberdefensie bezighouden. De EU zal ook steun verlenen aan de ontwikkeling van Europese cyberbeveiligingsoplossingen in het kader van haar inspanningen ten gunste van een Europese industriële en technologische defensiebasis. Dit omvat ook de bevordering van regionale excellentieclusters op het gebied van cyberbeveiliging en defensie.

De diensten van de Commissie zullen, in nauwe samenwerking met de EDEO, de lidstaten en andere betrokken EU-organen, uiterlijk in 2018 **een opleidings- en onderwijsplatform voor cyberbeveiliging** oprichten om de bestaande vaardigheidskloof op het vlak van cyberdefensie te dichten. Dit platform zal een aanvulling vormen op de werkzaamheden van het Europees Defensieagentschap op dit gebied en helpen om de bestaande vaardigheidskloof op het vlak van cyberbeveiliging en cyberdefensie te dichten.

**Kernacties**

- Een initiatief van de Commissie betreffende grensoverschrijdende toegang tot elektronisch bewijsmateriaal (begin 2018);
- Snelle vaststelling door het Europees Parlement en de Raad van het voorstel voor een richtlijn betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten;

[81] De cyberruimte is voor de EU een operationeel gebied zoals land, lucht en zee. Onder de cyberdefensie-inspanningen vallen ook de bescherming en weerbaarheid van ruimtesystemen en de daarmee samenhangende grondinfrastructuur.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

- De invoering van vereisten inzake IPv6 in overheidsopdrachten, onderzoeks- en projectfinanciering van de EU; Vrijwillige overeenkomsten tussen lidstaten en aanbieders van internetdiensten om vaart te zetten achter de invoering van IPv6;
- Meer/bredere aandacht van Europol voor digitale forensische wetenschap en monitoring van het darknet;
- Uitvoering van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten;
- Meer financiële steun voor nationale en grensoverschrijdende projecten ter verbetering van de strafrechtspleging in de cyberruimte;
- Een platform voor cyberbeveiligingsonderwijs om de bestaande vaardigheidskloof op het gebied van cyberbeveiliging en cyberdefensie aan te pakken in 2018.

## 4. VERSTERKING VAN DE INTERNATIONALE SAMENWERKING OP HET VLAK VAN CYBERBEVEILIGING

Het internationale cyberbeveiligingsbeleid gaat uit van de fundamentele waarden en grondrechten van de EU, zoals de vrijheid van meningsuiting en het recht op privacy en bescherming van persoonsgegevens, is gericht op de bevordering van een open, vrije en beveiligde cyberruimte, en is ontworpen om de mondiale cyberstabiliteit te bevorderen in een voortdurend veranderende realiteit en bij te dragen aan de Europese strategische autonomie in de cyberruimte.

### 4.1 Cyberbeveiliging in externe betrekkingen

Uit gegevens blijkt dat mensen in de hele wereld cyberaanvallen uit andere landen tot de grootste bedreigingen voor de nationale veiligheid rekenen[83]. Gezien de mondiale aard van de dreiging is de opbouw en de handhaving van robuuste allianties en partnerschappen met derde landen van fundamenteel belang voor de preventie en afschrikking van cyberaanvallen, die een steeds grotere rol spelen in de internationale stabiliteit en veiligheid. De EU zal in haar bilaterale, regionale en multilaterale overeenkomsten en in haar overeenkomsten met verschillende belanghebbenden voorrang geven aan de oprichting van een strategisch kader voor conflictpreventie en stabiliteit in de cyberruimte.

De EU pleit sterk voor het standpunt dat het internationale recht, en met name het Handvest van de Verenigde Naties, van toepassing is op de cyberruimte. Als aanvulling op bindende internationale wetgeving spreekt de EU haar steun uit aan de vrijwillige, niet-bindende normen, voorschriften en beginselen voor verantwoordelijk gedrag van staten die door de VN-groep van regeringsdeskundigen zijn beschreven[84] en moedigt zij de ontwikkeling en tenuitvoerlegging van regionale vertrouwenwekkende maatregelen aan, zowel in de Organisatie voor Veiligheid en Samenwerking in Europa als in andere regio's.

Op bilateraal niveau zullen er meer cyberdialogen[85] worden aangegaan en deze zullen worden aangevuld met inspanningen ter bevordering van de samenwerking met derde landen met het oog op de versterking van de beginselen van zorgvuldigheid en verantwoordelijkheid van de staat in de cyberruimte. De EU zal in haar internationale verbintenissen prioriteit toekennen aan internationale veiligheidskwesties in de cyberruimte en er tegelijk voor zorgen dat cyberbeveiliging geen excuus wordt voor marktbescherming en de beperking van grondrechten en fundamentele vrijheden, zoals de vrijheid van meningsuiting en de toegang

[83] Global Attitudes Survey, voorjaar 2017, Pew Research Centre.
[84] A/68/98 en A/70/174.
[85] In september 2017 is de EU cyberdialogen aangegaan met de VS, China, Japan, de Republiek Korea en India.

tot informatie. Een totaalaanpak van cyberbeveiliging vereist de eerbiediging van de mensenrechten en de EU zal haar fundamentele waarden wereldwijd blijven uitdragen en daarbij voortbouwen op de EU-mensenrechtenrichtsnoeren inzake online vrijheid[86]. In dit verband benadrukt de EU dat het belangrijk is dat alle belanghebbenden betrokken zijn bij het beheer van het internet.

De Commissie heeft daarnaast een voorstel[87] ingediend voor de modernisering van de Europese uitvoercontroles, onder meer door de invoering van controles op de uitvoer van kritieke technologieën voor cybertoezicht die kunnen leiden tot schendingen van de mensenrechten of door oneigenlijk gebruik de eigen beveiliging van de EU in het gedrang kunnen brengen, en zal de dialoog met derde landen intensiveren ter bevordering van mondiale convergentie en verantwoordelijk gedrag op dit gebied.

### 4.2 Opbouw van cyberbeveiligingscapaciteit

De mondiale cyberstabiliteit hangt af van de lokale en nationale capaciteit van alle landen om cyberincidenten te voorkomen of erop te reageren en om cybercriminaliteit te onderzoeken en vervolgen. Steun voor de opbouw van nationale weerbaarheid in derde landen zal het mondiale niveau van cyberbeveiliging verhogen, met positieve gevolgen voor de EU. Om de snel veranderende cyberdreigingen het hoofd te kunnen bieden, moeten er inspanningen worden geleverd voor de ontwikkeling van opleidingen, beleid en wetgeving en is er behoefte aan efficiënt functionerende computercrisisteams en cybercriminaliteitseenheden in alle landen ter wereld.

Sinds 2013 speelt de EU een leidende rol in internationale opbouw van cyberbeveiligingscapaciteit en koppelt ze die inspanningen systematisch aan haar ontwikkelingssamenwerking. De EU zal zich blijven inzetten voor een op rechten gebaseerd model voor capaciteitsopbouw, in overeenstemming met de “Digital4Development”-aanpak[88]. Wat de capaciteitsopbouw betreft, zal prioriteit worden verleend aan de buurlanden van de EU en aan ontwikkelingslanden die geconfronteerd worden met snel toenemende connectiviteit en snelle ontwikkeling van het dreigingslandschap. De inspanningen van de EU zullen een aanvulling vormen op haar ontwikkelingsagenda in het licht van de agenda 2030 voor duurzame ontwikkeling en de globale inspanningen voor de opbouw van institutionele capaciteit.

Om de EU beter toe te laten haar gemeenschappelijke expertise aan te wenden ter ondersteuning van die capaciteitsopbouw, moet een specifiek EU-netwerk voor cybercapaciteitsopbouw worden opgezet, waarin de EDEO, de cyberautoriteiten van de lidstaten, de EU-agentschappen, de diensten van de Commissie, de academische wereld en het maatschappelijk middenveld worden samengebracht. Er zullen EU-richtsnoeren voor cybercapaciteitsopbouw worden opgesteld, zodat de inspanningen van de EU ter ondersteuning van derde landen politiek beter kunnen worden gestuurd en geprioriteerd.

De EU zal op dit gebied ook met andere donoren samenwerken om dubbel werk te vermijden en gerichtere capaciteitsopbouw in verschillende regio's te bevorderen.

### 4.3 Samenwerking tussen de EU en de NAVO

[86] EU-mensenrechtenrichtsnoeren inzake vrijheid van meningsuiting online en offline.
[87] COM(2016) 616 final.
[88] SWD(2017) 157 final.

De EU zal voortbouwen op de wezenlijke vooruitgang die al is geboekt, om haar samenwerking met de NAVO op het vlak van cyberbeveiliging, hybride dreigingen en defensie te verdiepen zoals voorzien in de gezamenlijke verklaring van 8 juli 2016[89]. Tot de prioriteiten behoren het stimuleren van interoperabiliteit via coherente vereisten en normen inzake cyberbeveiliging, het versterken van de samenwerking op het gebied van opleiding en oefeningen, en het harmoniseren van de opleidingsvereisten.

De EU en de NAVO zullen ook samenwerking op het vlak van onderzoek en innovatie inzake cyberdefensie bevorderen en voortbouwen op de huidige technische regeling voor de uitwisseling van informatie over cyberbeveiliging tussen hun respectieve instanties die bevoegd zijn voor cyberbeveiliging[90]. Recente gezamenlijke inspanningen in de strijd tegen hybride dreigingen, in het bijzonder de samenwerking tussen de EU-Fusiecel en de Hybrid Analysis Branch van de NAVO, moeten verder worden uitgebuit om de weerbaarheid en de respons op cybercrises te versterken. De EU en de NAVO zullen verder samenwerken in het kader van cyberdefensie-oefeningen, waarbij de EDEO en andere EU-entiteiten en relevante NAVO-tegenhangers betrokken zullen zijn, inclusief het Cooperative Cyber Defence Centre of Excellence van de NAVO in Tallinn. Voor het eerst zullen de NAVO en de EU parallelle en gecoördineerde oefeningen uitvoeren volgens een hybride scenario, waarbij de NAVO in 2017 het voortouw neemt en de EU in 2018. Het volgende verslag over de samenwerking tussen de EU en de NAVO, dat in december 2017 aan de respectieve raden zal worden voorgelegd, zal de gelegenheid bieden om na te denken over een verdere uitbreiding van de samenwerking, met name door te zorgen voor gemeenschappelijke, beveiligde en degelijke communicatiemiddelen tussen alle betrokken instellingen en organen, waaronder het Enisa.

**Kernacties**

- Vooruitgang boeken met het strategisch kader voor conflictpreventie en stabiliteit in de cyberruimte;
- Een nieuw netwerk voor capaciteitsopbouw ontwikkelen ter ondersteuning van het vermogen van derde landen om zich tegen cyberdreigingen te verdedigen, en EU-richtsnoeren voor de opbouw van cyberbeveiligingscapaciteit uitwerken om de inspanningen van de EU beter te kunnen prioriteren;
- Verdere samenwerking tussen de EU en de NAVO, zoals deelname aan parallelle en gecoördineerde oefeningen en een verhoogde interoperabiliteit van de cyberbeveiligingsnormen.

## 5. CONCLUSIE

De paraatheid van de EU op het vlak van cyberbeveiliging is van essentieel belang voor zowel de digitale eengemaakte markt als onze veiligheids- en defensie-unie. Het is absoluut noodzakelijk dat de Europese cyberbeveiliging wordt versterkt en dat de dreigingen voor civiele en militaire doelen worden aangepakt.

De Digitale Top die op 29 september 2017 door het Estse voorzitterschap wordt georganiseerd, is een uitgelezen moment om uiting te geven aan onze gemeenschappelijke vastberadenheid om cyberbeveiliging centraal te stellen in de digitale samenleving die de EU is. Als onderdeel van dit gemeenschappelijke engagement worden de lidstaten door de Commissie verzocht toe te zeggen hoe zij van plan zijn te handelen op de gebieden waarvoor

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[90] CERT-EU en de Computer Incident Response Capability van de NAVO (NCIRC).

zij primair verantwoordelijk zijn. Dit moet de versterking van de cyberbeveiliging omvatten door middel van de volgende maatregelen:

- Ervoor zorgen dat de NIS-richtlijn uiterlijk op 9 mei 2018 volledig en effectief is uitgevoerd en dat de nodige middelen worden uitgetrokken zodat de voor cyberbeveiliging bevoegde overheidsinstanties hun taken doeltreffend kunnen vervullen;
- Dezelfde regels toepassen op overheidsdiensten, gezien de rol die ze spelen in de maatschappij en de economie als geheel;
- Opleidingen inzake cyberbeveiliging organiseren bij de overheidsdiensten;
- Prioriteit verlenen aan bewustmakingscampagnes rond cyberbewustzijn en cyberbeveiliging opnemen in de leerplannen van academische en beroepsopleidingen;
- De ontwikkeling van cyberdefensieprojecten ondersteunen met initiatieven in het kader van de permanente gestructureerde samenwerking (PESCO) en het Europese Defensiefonds.

In deze gezamenlijke mededeling is een overzicht gegeven van de omvang van de uitdaging en van de reeks maatregelen die de EU kan nemen. Wij hebben een weerbaar Europa nodig dat zijn bevolking doeltreffend kan beschermen door te anticiperen op mogelijke cyberincidenten, door sterke beveiliging in te bouwen in zijn structuren en gedragingen, door snel te herstellen van cyberaanvallen en door aanvallers af te schrikken. Deze mededeling bevat gerichte maatregelen die, met de volledige medewerking van de lidstaten en de verschillende structuren van de EU en met inachtneming van hun bevoegdheden en verantwoordelijkheden, moeten leiden tot een verdere, gecoördineerde versterking van de cyberbeveiligingsstructuren en -vermogens van de EU. De uitvoering ervan zal een duidelijk signaal geven dat de EU en de lidstaten zullen samenwerken om een norm voor cyberbeveiliging te hanteren die bestand is tegen de groeiende uitdagingen waar Europa vandaag mee wordt geconfronteerd.