EUROPESE REKENKAMER

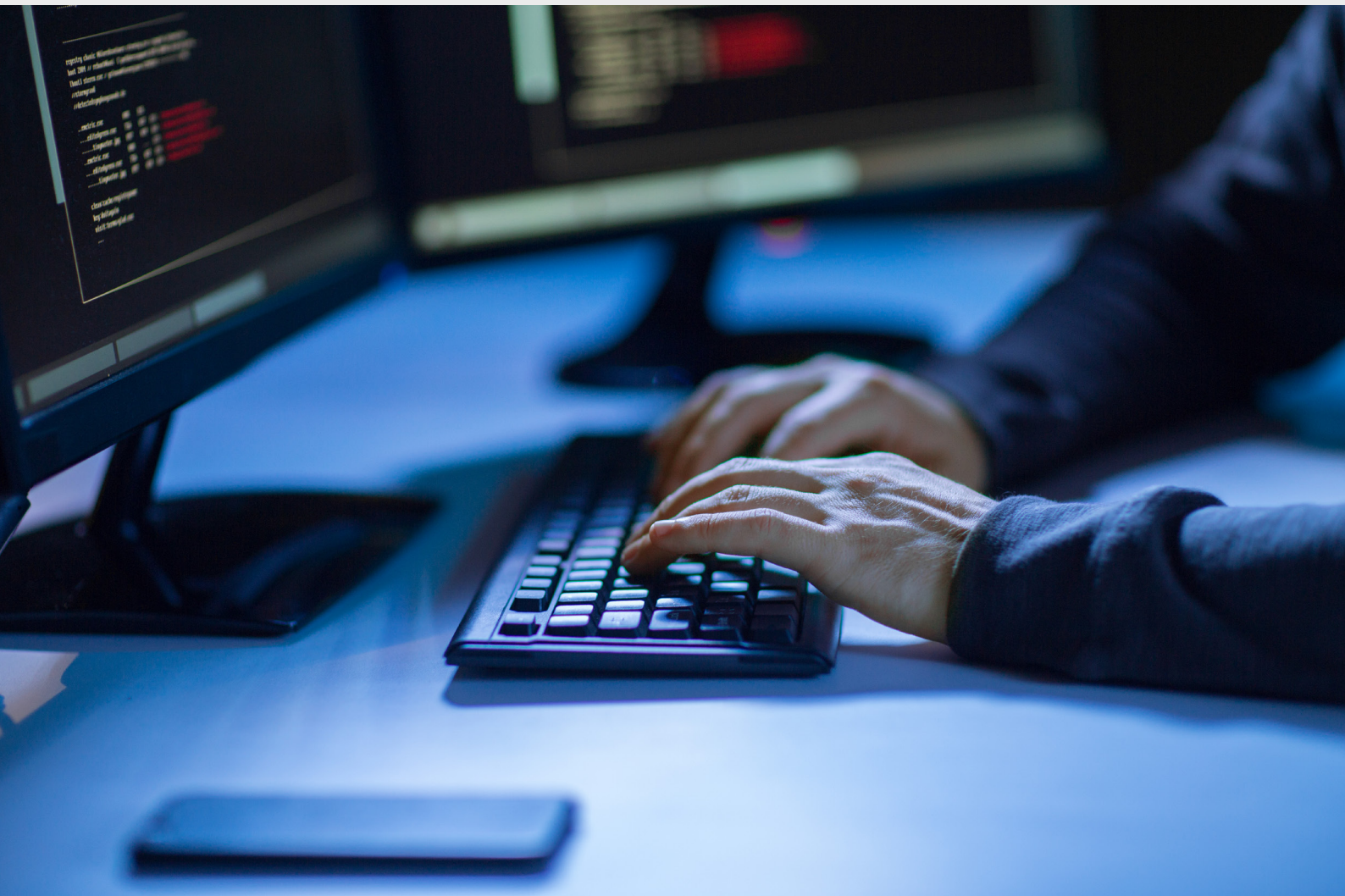
NL

2019

Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging

Briefingdocument

Maart 2019



Over het document:

Dit briefingdocument, dat geen controleverslag is, heeft tot doel een overzicht te geven van het complexe beleidslandschap met betrekking tot cyberbeveiliging in de EU en de grootste uitdagingen voor een doeltreffende beleidsuitvoering bloot te leggen. Het heeft betrekking op netwerk- en informatiebeveiliging, cybercriminaliteit, cyberdefensie en desinformatie. De informatie in dit document zal ook als input dienen voor toekomstige controlewerkzaamheden op dit gebied.

We hebben onze analyse gebaseerd op een onderzoek van stukken waarvoor openbaar beschikbare informatie uit officiële documenten, standpuntnota's en studies van derden werd gebruikt. Het veldwerk is uitgevoerd tussen april en september 2018 en er zijn ontwikkelingen tot en met december 2018 in meegenomen. We hebben dit werk aangevuld met een enquête onder de nationale rekenkamers van de lidstaten, evenals vraaggesprekken met relevante belanghebbenden binnen de EU-instellingen en met vertegenwoordigers van de particuliere sector.

De uitdagingen die werden vastgesteld, zijn ingedeeld in vier brede clusters: i) het beleidskader; ii) financiering en uitgaven; iii) vergroten van de cyberweerbaarheid, en iv) doeltreffend reageren op cyberincidenten. Het blijft noodzakelijk om binnen de EU een hoger niveau van cyberbeveiliging te verwezenlijken. Daarom sluiten we elk hoofdstuk af met een reeks ideeën voor verdere overweging door beleidsmakers, wetgevers en beroepsbeoefenaars.

We willen de diensten van de Commissie, de Europese Dienst voor extern optreden, de Raad van de Europese Unie, Enisa, Europol, de European Cybersecurity Organisation (Europese organisatie voor cyberbeveiliging) en de nationale rekenkamers van de lidstaten graag bedanken voor hun constructieve feedback.

Inhoud

Samenvatting

I Technologie opent de deur naar een heel nieuwe wereld vol kansen, waarin nieuwe producten en diensten een integraal deel zijn gaan uitmaken van ons dagelijks leven. De keerzijde van de medaille is echter dat het risico om het slachtoffer te worden van cybercriminaliteit of cyberaanvallen ook toeneemt en dat de maatschappelijke en economische gevolgen daarvan steeds groter worden. De recente inspanningen die de EU sinds 2017 levert om de cyberbeveiliging en haar digitale economie te versterken, komen daarom op een cruciaal moment.

II Met dit briefingdocument, dat geen controleverslag is en is gebaseerd op openbaar beschikbare informatie, wordt beoogd een overzicht te geven van een complex en onregelmatig beleidslandschap en de belangrijkste uitdagingen vast te stellen voor een doeltreffende tenuitvoerlegging van het beleid. In dit document wordt ingegaan op het EU-beleid inzake cyberbeveiliging, cybercriminaliteit en cyberdefensie, evenals inspanningen om desinformatie te bestrijden. De uitdagingen die werden vastgesteld zijn ingedeeld in vier brede clusters: i) het beleids- en wetgevingskader; ii) financiering en uitgaven; iii) opbouwen van de cyberweerbaarheid, en iv) doeltreffend reageren op cyberincidenten. Elk hoofdstuk bevat enkele aandachtspunten met betrekking tot de voorgestelde uitdagingen.

Het beleids- en wetgevingskader

III Het is een uitdaging om initiatieven te ontwikkelen die zijn afgestemd op het brede doel van de EU-strategie inzake cyberbeveiliging (namelijk “de veiligste digitale omgeving ter wereld worden”), aangezien meetbare doelstellingen ontbreken en betrouwbare gegevens schaars zijn. De resultaten worden zelden gemeten en op weinig beleidsterreinen zijn evaluaties uitgevoerd. Een van de grootste uitdagingen is daarom **zinvolle verantwoording en evaluatie te waarborgen** door over te stappen op een prestatiecultuur met geïntegreerde evaluatiepraktijken.

IV Het wetgevingskader blijft onvolledig. **Tekortkomingen in en de inconsequente omzetting van EU-wetgeving** kunnen een maximale verwezenlijking van het potentieel van de wetgeving belemmeren.

Financiering en uitgaven

V **Het afstemmen van de investeringen op de doelen** is een uitdaging: hiervoor moeten niet alleen de totale investeringen in cyberbeveiliging — die in de EU laag en

gefragmenteerd zijn — maar ook de effecten ervan worden opgeschaald, met name door de resultaten van bekostigd onderzoek beter te benutten en de doeltreffende benadering en financiering van start-ups te waarborgen.

VI **Een duidelijk overzicht van de uitgaven van de EU** is essentieel voor de EU en haar lidstaten om te kunnen weten welke kloven er moeten worden gedicht om de genoemde doelstellingen te realiseren. Aangezien er geen specifieke EU-begroting is om de strategie inzake cyberbeveiliging te financieren, is er geen duidelijk inzicht in de verdeling van de middelen.

VII In tijden waarin de politieke prioriteiten steeds meer worden ingegeven door veiligheid, kunnen **beperkingen voor de adequate financiering van EU-agentschappen voor cyberkwesties** belemmeren dat de ambities van de EU worden gerealiseerd. Om deze uitdagingen aan te pakken, moeten onder meer manieren worden gevonden om talent aan te trekken en vast te houden.

Opbouwen van de cyberweerbaarheid

VIII Er zijn ontzettend veel zwakke punten te vinden in de cyberbeveiligingsgovernance in de publieke en particuliere sector, zowel in de EU als daarbuiten. Dit belemmert het vermogen van de internationale gemeenschap om te reageren op cyberaanvallen en deze te beperken, en staat een samenhangende, EU-brede benadering in de weg. De uitdaging is derhalve om **de cyberbeveiligingsgovernance te verbeteren**.

IX **Het verbeteren van de vaardigheden en het vergroten van het bewustzijn** in alle sectoren en op alle niveaus binnen de samenleving is essentieel, aangezien het tekort aan vaardigheden op het gebied van cyberbeveiliging wereldwijd toeneemt. Er zijn momenteel beperkte EU-brede normen voor opleiding, certificering en cyberrisicobeoordelingen.

X Een klimaat van vertrouwen is essentieel voor het versterken van de algehele cyberweerbaarheid. De Commissie heeft zelf geoordeeld dat de coördinatie over het algemeen nog steeds ontoereikend is. **Het verbeteren van de informatie-uitwisseling en coördinatie** tussen de publieke en particuliere sector blijft een uitdaging.

Doeltreffend reageren op cyberincidenten

XI Digitale systemen zijn zo complex geworden dat het voorkomen van alle aanvallen inmiddels onmogelijk is. Op deze uitdagingen kan alleen worden gereageerd door

middel van **snelle detectie en reactie**. Cyberbeveiliging is echter nog niet volledig geïntegreerd in de bestaande coördinatiemechanismen voor crisisbestrijding op EU-niveau, hetgeen het vermogen van de EU om te reageren op grootschalige, grensoverschrijdende cyberincidenten mogelijk zal beperken.

XII De **bescherming van kritieke infrastructuur en maatschappelijke functies** is van cruciaal belang. Potentiële interferentie in verkiezingsprocessen en desinformatiecampagnes vormen een kritieke uitdaging.

XIII De huidige uitdagingen met betrekking tot cyberdreigingen waarmee de EU en de rest van de wereld worden geconfronteerd, vereisen constante inspanningen en een voortdurende, consequente eerbiediging van de kernwaarden van de EU.

Inleiding

01 Technologie opent de deur naar een wereld vol nieuwe kansen. Er komen nieuwe producten en diensten bij, die integraal deel gaan uitmaken van ons dagelijks leven. Met elke nieuwe ontwikkeling neemt onze technologische afhankelijkheid echter toe, en daarmee ook het belang van cyberbeveiliging. Hoe meer persoonsgegevens we online zetten en hoe meer we verbonden raken, hoe groter de kans dat we het slachtoffer worden van een vorm van cybercriminaliteit of cyberaanvallen.

Wat is cyberbeveiliging?

02 Er is geen vaste universeel aanvaarde definitie van cyberbeveiliging[1]. In brede zin betreft het alle waarborgen en maatregelen die worden ingevoerd om informatiesystemen en hun gebruikers te beschermen tegen onbevoegde toegang, aanvallen en schade, teneinde de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te garanderen.

03 Cyberbeveiliging heeft betrekking op de preventie en detectie van, het reageren op en het herstel na cyberincidenten. Incidenten kunnen al dan niet opzettelijk worden uitgelokt en bijvoorbeeld uiteenlopen van de abusievelijke verspreiding van informatie tot aanvallen op bedrijven en kritieke infrastructuur, diefstal van persoonsgegevens, en zelfs inmenging in democratische processen. Deze incidenten kunnen allemaal verreikende schadelijke gevolgen hebben voor personen, organisaties en gemeenschappen.

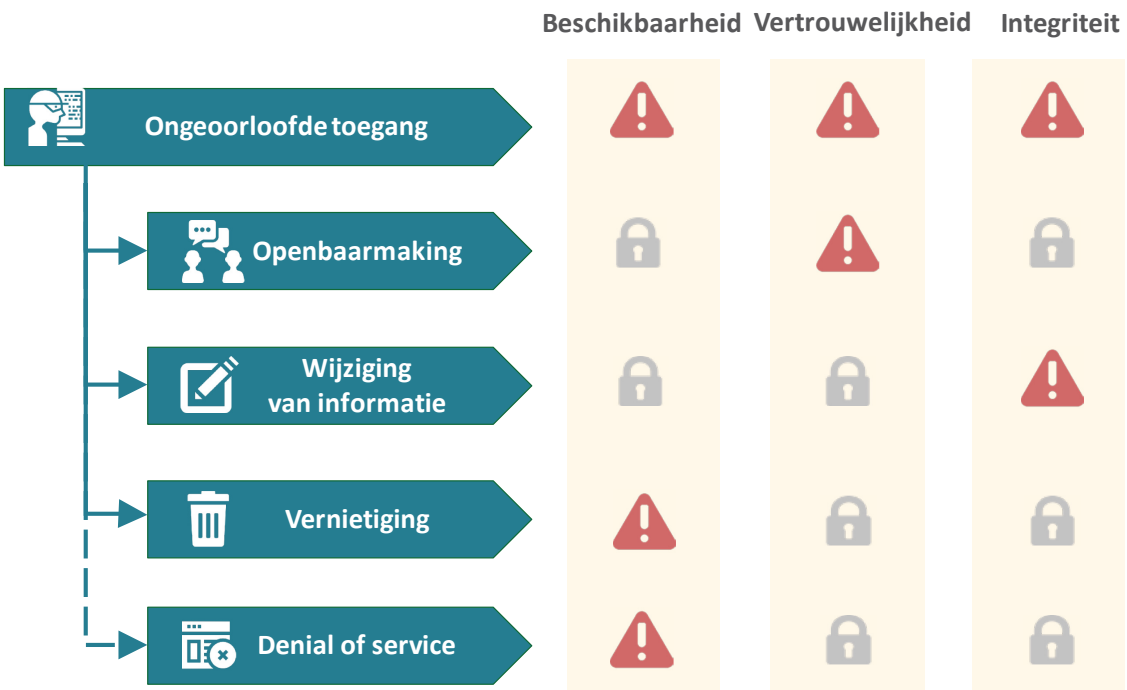
04 Cyberbeveiliging is een term die wordt gebruikt in EU-beleidskringen en is niet beperkt tot netwerk- en informatiebeveiliging. Het heeft betrekking op alle illegale activiteiten waarbij digitale technologieën worden gebruikt in cyberspace. Cyberbeveiliging kan derhalve ook cybermisdaden als aanvallen op computers met virussen en fraude met niet-contante betaalmiddelen omvatten en kan de kloof tussen systemen en inhoud overbruggen, zoals bij de onlineverspreiding van materiaal inzake seksueel misbruik van kinderen. Ook kan het betrekking hebben op desinformatiecampagnes om onlinedebatten en de verwachte uitkomsten van verkiezingen te beïnvloeden. Europol heeft bovendien opgemerkt dat cybercriminaliteit en terrorisme hand in hand gaan[2].

05 Verschillende actoren, waaronder staten, criminele organisaties en hacktivisten, sturen aan op cyberincidenten, hierbij gemotiveerd door verschillende factoren. De

gevolgen van deze incidenten zijn voelbaar op nationaal, Europees en zelfs internationaal niveau. De immateriële en grotendeels grensoverschrijdende aard van het internet en de instrumenten en tactieken die worden gebruikt, maken het vaak moeilijk om de identiteit van de dader van een aanval vast te stellen (het zogenaamde "probleem van attributie").

06 De verschillende soorten cyberbeveiligingsdreigingen kunnen worden geclassificeerd op basis van hun gevolgen voor de betrokken gegevens – vrijgave, wijziging, vernietiging en weigering van toegang – of de kernbeginselen van informatiebeveiliging die zij schenden, zoals te zien is in ***figuur 1*** hieronder. Een aantal voorbeelden van aanvallen wordt beschreven in ***tekstvak 1***. Aangezien de aanvallen op informatiesystemen steeds geavanceerder worden, worden onze verdedigingsmechanismen steeds minder doeltreffend[3].

Figuur 1 — Soorten dreigingen en de beginselen van beveiliging waarvoor zij een risico vormen



Bron: Studie van het Europees Parlement, aangepast door de Europese Rekenkamer[4]. Hangslot = geen gevolgen voor de beveiliging; Uitroepteken = beveiliging loopt gevaar

Tekstvak 1

Soorten cyberaanvallen

Telkens wanneer een nieuw apparaat online komt of verbinding maakt met andere apparaten, neemt het zogeheten "aanvalsoppervlak" voor cyberaanvallen toe. De

exponentiële groei van het “internet der dingen”, de cloud, big data en de digitalisering van het bedrijfsleven gaat vergezeld van een grotere blootstelling aan kwetsbaarheden, waardoor malafide actoren nog meer slachtoffers kunnen maken. De diverse soorten aanvallen en hun toenemende verfijning maken het echt lastig de ontwikkelingen bij te benen[5].

Malware (malafide software) is ontworpen om schade toe te brengen aan apparaten en netwerken. Het kan de vorm aannemen van virussen, Trojaanse paarden, ransomware, wormen, adware en spyware. **Ransomware** versleutelt gegevens zodat gebruikers geen toegang meer hebben tot hun bestanden zolang zij geen losgeld betalen (dit losgeld dient meestal in cryptovaluta te worden betaald) of een bepaalde actie uitvoeren. Volgens Europol komen ransomwareaanvallen het meest voor en is het aantal in de afgelopen jaren exponentieel toegenomen. De **verstoring van diensten** (zogeheten DDoS-aanvallen — Distributed Denial of Service), waarbij diensten of bronnen niet meer beschikbaar zijn omdat ze worden overladen met meer verzoeken dan zij aankunnen, komt ook steeds vaker voor. In 2017 werd een derde van de organisaties geconfronteerd met een dergelijke aanval[6].

Gebruikers kunnen worden gemanipuleerd om onbewust een actie uit te voeren of vertrouwelijke informatie vrij te geven. Deze list kan vervolgens worden benut voor gegevensdiefstal of cyberspionage en wordt **social engineering** genoemd. Dit wordt op verschillende manieren gedaan, maar een veelgebruikte methode is **phishing**, waarbij e-mails afkomstig lijken te zijn van betrouwbare bronnen en gebruikers worden overgehaald om informatie vrij te geven of op links te klikken waardoor hun apparaat wordt besmet met gedownloade malware. Meer dan de helft van de lidstaten gaf aan onderzoeken te hebben lopen naar cyberaanvallen[7].

Geavanceerde aanhoudende dreigingen (advanced persistent threats, APT's) vormen misschien wel de meest schadelijke categorie dreigingen. Het gaat hierbij om geraffineerde aanvallers die gedurende lange tijd gegevens monitoren en stelen en soms ook destructieve doelen nastreven. Het doel hierbij is om onder de radar te blijven en zo lang mogelijk niet te worden ontdekt. APT's zijn vaak gekoppeld aan staten en gericht op bijzonder gevoelige sectoren als technologie, defensie en kritieke infrastructuur. Cyberspionage is naar verluidt verantwoordelijk voor ten minste een kwart van alle cyberincidenten en de meeste kosten[8].

Hoe ernstig is het probleem?

07 Het meten van het effect van een slechte voorbereiding op eventuele cyberaanvallen is lastig, omdat er geen betrouwbare gegevens zijn. De economische impact van cybercriminaliteit is tussen 2013 en 2017 vervijfvoudigd[9], met gevolgen voor zowel overheden als bedrijven, van klein tot groot. Deze trend blijkt wel uit de voorspelde groei in premies voor cyberverzekeringen van 3 miljard EUR in 2018 naar 8,9 miljard EUR in 2020.

08 De financiële gevolgen van cyberaanvallen worden steeds groter en er is sprake van een alarmerend verschil tussen de kosten van het uitvoeren van een aanval en die van preventie, onderzoek en herstel. Zo kan een DDoS-aanval al voor 15 EUR per maand worden uitgevoerd, terwijl de verliezen die worden geleden door de bedrijven die het slachtoffer worden, waaronder imagoschade, aanzienlijk hoger zijn[10].

09 Ook al heeft in 2016 80 % van de bedrijven te maken gekregen met ten minste één cyberbeveiligingsincident[11], het risico wordt nog steeds alarmerend weinig onderkend. Van de bedrijven in de EU heeft 69 % helemaal geen of slechts elementair inzicht in hun blootstelling aan cyberdreigingen[12] en heeft 60 % nooit een schatting gemaakt van de potentiële financiële verliezen[13]. Bovendien zou een derde van de organisaties volgens een wereldwijd onderzoek de hacker liever het losgeld betalen dan investeren in informatiebeveiliging[14].

10 De wereldwijde *Wannacry*-aanvallen met ransomware en de *NotPetya*-aanvallen met malware in 2017 hebben in totaal gevolgen gehad voor meer dan 320 000 mensen in ongeveer 150 landen[15]. Deze incidenten hebben ertoe geleid dat de wereld zich min of meer bewust werd van de dreiging van cyberaanvallen, waardoor een ideaal moment ontstond om cyberbeveiliging te introduceren in de mainstream-beleidsvorming. Daarnaast denkt 86 % van de EU-burgers inmiddels dat het risico dat zij het slachtoffer worden van cybercriminaliteit, toeneemt[16].

Het optreden van de EU op het gebied van cyberbeveiliging

11 De EU is in 2001 benoemd tot waarnemingsorganisatie van de commissie Cybercrimeverdrag van de Raad van Europa[17] (het Verdrag van Boedapest). Vanaf toen heeft de EU beleid, wetgeving en uitgaven toegepast om haar cyberweerbaarheid te vergroten. Tegen een achtergrond van een groeiend aantal grote cyberaanvallen en -incidenten is de activiteit sinds 2013 geïntensiveerd, zoals te zien is in ***figuur 2***. Tegelijkertijd hebben de lidstaten hun eerste nationale strategieën voor cyberbeveiliging goedgekeurd (en in sommige gevallen al geactualiseerd).

12 De belangrijkste EU-spelers met verantwoordelijkheden op het gebied van cyberbeveiliging worden beschreven in ***tekstvak 2*** en ***bijlage I***.

Tekstvak 2

Wie is hierbij betrokken?

De **Europese Commissie** heeft als doel de capaciteiten en samenwerking op het gebied van cyberbeveiliging te vergroten, de rol van de EU als speler op het gebied van cyberbeveiliging te versterken en cyberbeveiliging te mainstreamen in ander EU-beleid. De belangrijkste directoraten-generaal (DG's) die verantwoordelijk zijn voor het beleid inzake cyberbeveiliging zijn de DG's **CNECT** (cyberbeveiliging) en **HOME** (cybercriminaliteit), respectievelijk verantwoordelijk voor de digitale eengemaakte markt en de Veiligheidsunie. DG **DIGIT** is verantwoordelijk voor de IT-beveiliging van de eigen systemen van de Commissie.

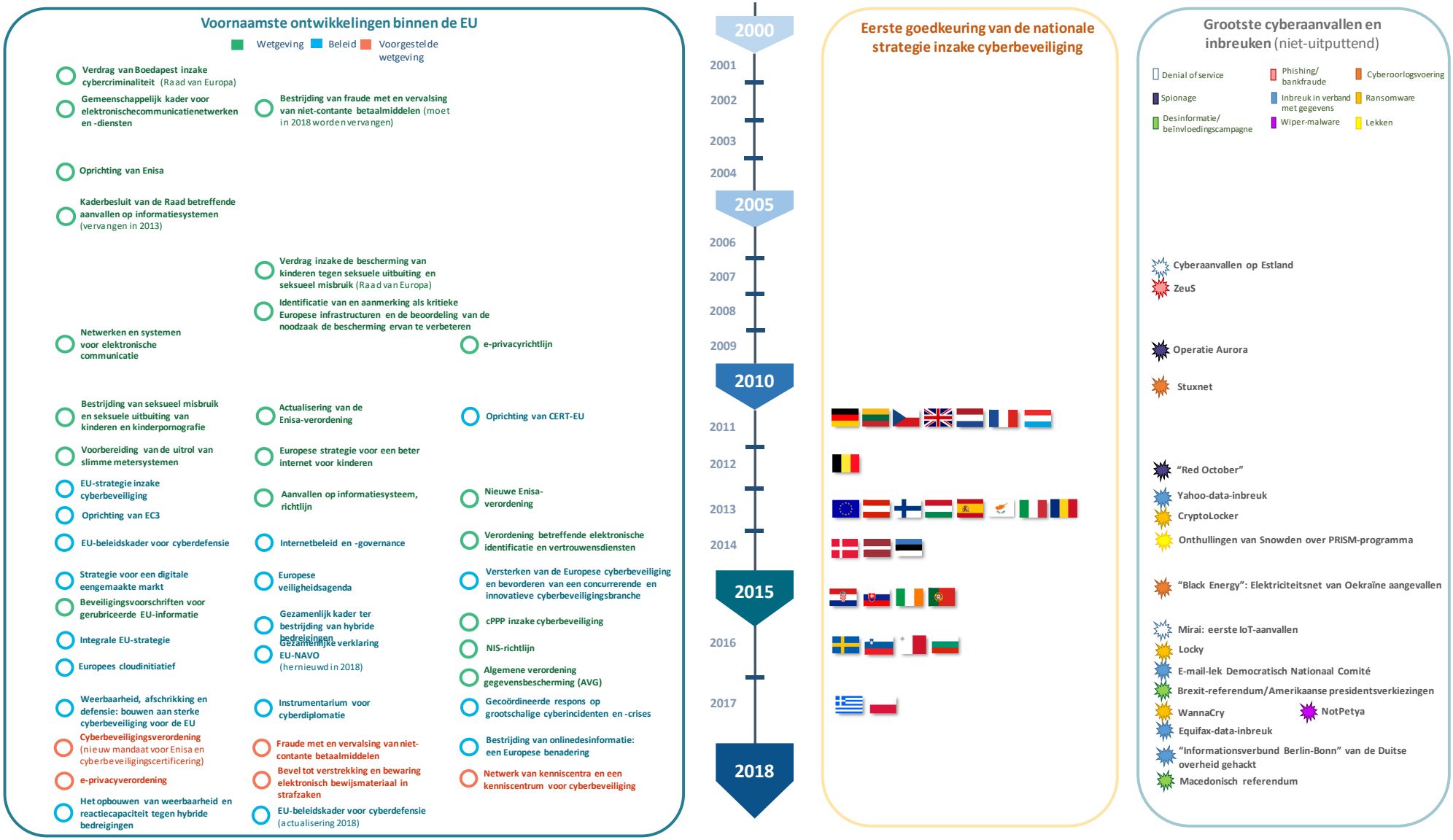
De Commissie wordt ondersteund door verschillende EU-agentschappen, met name **Enisa** (Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging), het agentschap van de Europese Unie voor cyberbeveiliging — een orgaan dat met name advies geeft ter ondersteuning van beleidsontwikkeling, capaciteitsopbouw en voorlichting. Het Centrum voor de bestrijding van cybercriminaliteit van Europol (**EC3**) is opgericht om ervoor te zorgen dat de wetshandhavingsinstanties van de EU bij cybercriminaliteit sterker kunnen optreden. De Commissie heeft een computercrisisteam (**CERT-EU**), dat alle instellingen, organen en agentschappen van de Unie ondersteunt.

De **Europese Dienst voor extern optreden** (EDEO) neemt de leiding als het gaat om cyberdefensie, cyberdiplomatie en strategische communicatie, en beschikt over inlichtingen- en analysecentra. Het **Europees Defensieagentschap** (EDA) heeft als doel capaciteiten op het gebied van cyberdefensie te ontwikkelen.

De **lidstaten** zijn primair verantwoordelijk voor hun eigen cyberbeveiliging en treden op EU-niveau op via de **Raad**, die over verschillende organen voor coördinatie en informatie-uitwisseling beschikt (waaronder de Horizontale groep cybervraagstukken). Het **Europees Parlement** fungeert als medewetgever.

Organisaties uit de particuliere sector, waaronder het bedrijfsleven, organen voor internetregulering en academici, zijn partners en leveren daarnaast een bijdrage aan de ontwikkeling en uitvoering van beleid, onder meer door middel van een contractueel publiek-privaat partnerschap (**cPPP**).

Figuur 2 — Een versnelling in de ontwikkeling van beleid en wetgeving (situatie op 31 december 2018)



Bron: ERK.

Beleid

13 Het ecosysteem voor cyberbeveiliging van de EU is complex, bestaat uit verschillende lagen en heeft raakvlakken met diverse interne beleidsterreinen, zoals justitie en binnenlandse zaken, de digitale eengemaakte markt en onderzoeksbeleid. Wat het externe beleid betreft, speelt cyberbeveiliging een rol in de diplomatie en maakt het in toenemende mate deel uit van het defensiebeleid van de EU dat momenteel wordt ontwikkeld.

14 De hoeksteen van het beleid van de EU wordt gevormd door de **Strategie inzake cyberbeveiliging uit 2013**[18]. Met deze strategie wordt beoogd van de EU de veiligste digitale omgeving ter wereld te maken en de fundamentele waarden en vrijheden te verdedigen. De strategie heeft vijf kerndoelstellingen: i) vergroten van de cyberweerbaarheid; ii) verminderen van cybercriminaliteit; iii) ontwikkelen van beleid en capaciteiten op het gebied van cyberdefensie; iv) ontwikkelen van industriële en technologische hulpmiddelen voor cyberbeveiliging, en v) formuleren van een internationaal beleid inzake cyberbeveiliging dat is afgestemd op de kernwaarden van de EU.

15 De strategie inzake cyberbeveiliging heeft raakvlakken met drie later aangenomen strategieën:

— Met de **Europese veiligheidsagenda** (2015) wordt beoogd de bestrijding van cybercriminaliteit door wetshandhavingsinstanties en het rechtssysteem te verbeteren, met name door bestaande wetgeving en beleid te vernieuwen[19]. Ook wordt ermee beoogd belemmeringen voor strafrechtelijk onderzoek naar cybercriminaliteit vast te stellen en de cybercapaciteitsopbouw te verbeteren.

— Met de **Strategie voor een digitale eengemaakte markt**[20] (2015) wordt beoogd betere toegang te creëren tot digitale goederen en diensten door de juiste voorwaarden te scheppen voor een maximaal groeipotentieel voor de digitale economie. In dit kader is het verbeteren van de beveiliging, het vertrouwen en de inclusie online essentieel.

— Met de **Integrale EU-strategie**[21] uit 2016 wordt beoogd de rol van de EU op het wereldtoneel te vergroten. Cyberbeveiliging vormt in de strategie een centrale pijler en dit komt tot uiting in de hernieuwde aandacht voor cybervraagstukken, samenwerking met belangrijke partners en het voornemen om alle cybervraagstukken op alle beleidsterreinen aan te pakken, onder meer door repliek op desinformatie door middel van strategische communicatie.

16 In de afgelopen jaren is de cyberspace steeds verder gemilitariseerd[22] en bewapend[23], waardoor het inmiddels wordt beschouwd als het vijfde domein van oorlogvoering[24]. Cyberdefensie schermt systemen, netwerken en kritieke infrastructuur in cyberspace af van militaire en andersoortige aanvallen. In 2014 werd een **beleidskader voor cyberdefensie** goedgekeurd, dat in 2018 werd geactualiseerd[25]. In de herziening van 2018 werden zes prioriteiten aangemerkt, waaronder de ontwikkeling van capaciteiten op het gebied van cyberdefensie en de bescherming van de communicatie- en informatienetwerken van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de EU. Cyberdefensie maakt ook deel uit van de permanente gestructureerde samenwerking (PESCO) en de samenwerking tussen de EU en de NAVO.

17 In het **Gezamenlijk kader ter bestrijding van hybride bedreigingen** van de EU (2016) wordt ingegaan op cyberdreigingen voor zowel kritieke infrastructuur als particuliere gebruikers, waarbij wordt benadrukt dat cyberaanvallen kunnen worden uitgevoerd via desinformatiecampagnes op sociale media[26]. Ook wordt erin opgemerkt dat het noodzakelijk is het bewustzijn te vergroten en de samenwerking tussen de EU en de NAVO te intensiveren, hetgeen concreet tot uiting kwam in de gemeenschappelijke EU-NAVO-verklaringen uit 2016 en 2018[27].

18 In 2017 heeft de Commissie een nieuw pakket inzake cyberbeveiliging gepresenteerd, waaruit duidelijk blijkt dat digitale bescherming steeds urgenter wordt. Het pakket omvat een nieuwe mededeling van de Commissie betreffende de actualisering van de strategie voor cyberbeveiliging uit 2013[28], evenals een blauwdruk voor een snelle en gecoördineerde respons bij een grote aanval en voor de spoedige tenuitvoerlegging van de richtlijn netwerk- en informatiebeveiliging (NIS-richtlijn)[29]. Voorts bevatte het pakket een aantal wetgevingsvoorstellen (zie paragraaf ***22***).

Wetgeving

19 Sinds 2002 is er wetgeving aangenomen die in meer of mindere mate relevant is voor cyberbeveiliging.

20 Als belangrijkste pijler van de strategie inzake cyberbeveiliging uit 2013 vormt de **richtlijn netwerk- en informatiebeveiliging (NIS-richtlijn)**[30] uit 2016, de eerste EU-brede wetgeving inzake cyberbeveiliging, de juridische hoeksteen. Met de richtlijn, die in mei 2018 omgezet had moeten zijn, wordt beoogd een minimumniveau van geharmoniseerde capaciteiten te waarborgen door lidstaten te verplichten nationale

NIS-strategieën aan te nemen en enkele contactpunten en computer security incident response teams (CSIRT's) op te richten[31]. Ook worden er beveiligings- en kennisgevingsvereisten in vastgesteld voor aanbieders van essentiële diensten in kritieke sectoren en voor digitaledienstverleners.

21 Tegelijkertijd trad ook de **algemene verordening gegevensbescherming**[32] (AVG) in 2016 in werking. Er wordt mee beoogd de persoonsgegevens van Europese burgers te beschermen door regels vast te stellen met betrekking tot de verwerking en verspreiding ervan. Uit hoofde van de verordening hebben betrokkenen bepaalde rechten en verwerkingsverantwoordelijken (aanbieders van digitale diensten) bepaalde plichten met betrekking tot het gebruik en de overdracht van informatie. Ook moet er van eventuele inbreuken verplicht melding worden gemaakt en kunnen er in sommige gevallen boetes worden opgelegd. In ***figuur 3*** is te zien hoe de nieuwe NIS-richtlijn en de AVG elkaar aanvullen wat betreft hun doelstelling om de cyberbeveiliging aan te scherpen en gegevensbescherming te waarborgen.

22 Er zijn momenteel verschillende ontwerpen van wetgeving in behandeling, waaronder de voorgestelde cyberbeveiligingsverordening waarmee wordt beoogd Enisa te versterken en een EU-breed certificeringsmechanisme op te zetten[33], de voorgestelde verordening betreffende bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal[34] en de voorgestelde richtlijn betreffende elektronisch bewijsmateriaal[35]. Het voorstel uit 2018 voor een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (hierna “netwerk van kenniscentra op het gebied van cyberbeveiliging en een kenniscentrum voor onderzoek” genoemd) maakt deel uit van het pakket cyberbeveiliging uit 2017[36].

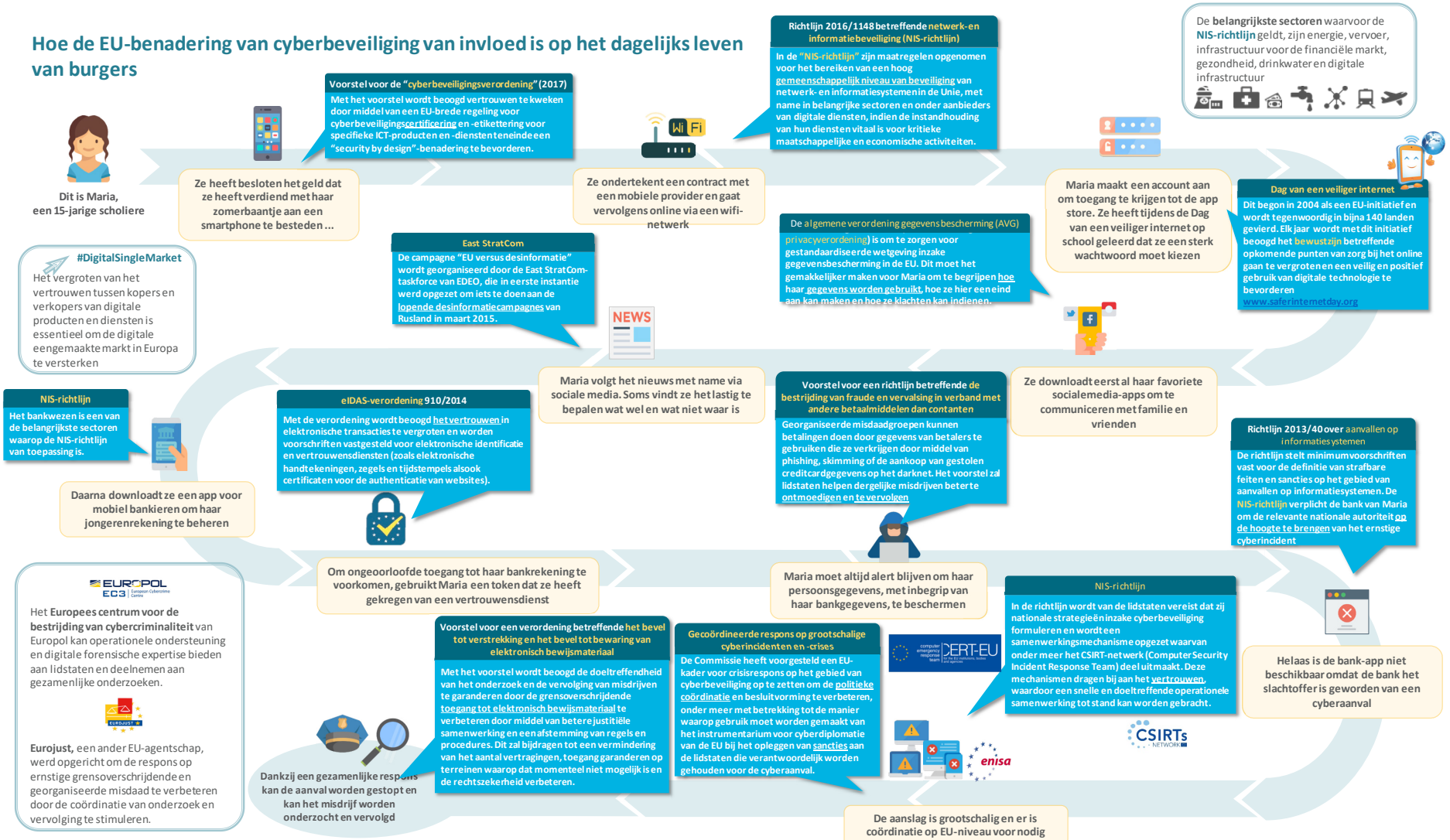
23 Het kan lastig zijn om een goed inzicht te krijgen in de reikwijdte van het beleids- en wetgevingskader dat verband houdt met cyberbeveiliging en in de effecten die dit kader heeft op ons dagelijks leven.

24 In ***figuur 4*** wordt getracht weer te geven hoe verschillende wetgevende handelingen en andere activiteiten een impact hebben op het leven van een fictieve Europese burger.

Figuur 3 — Hoe de AVG en de NIS-richtlijn elkaar aanvullen

Bron: ERK.

Figuur 4 — Hoe de EU-benadering van cyberbeveiliging van invloed is op het dagelijks leven van burgers



Bron: ERK.

Een beleids- en wetgevingskader ontwikkelen

25 Het cyberecosysteem van de EU is complex, bestaat uit meerdere lagen en er zijn allerlei partijen bij betrokken (zie ***bijlage I***). Het is een aanzienlijke uitdaging om al deze uiteenlopende onderdelen samen te brengen. Sinds 2013 is er sprake van een gecoördineerde impuls om samenhang te brengen in het beleid inzake cyberbeveiliging van de EU[37].

Uitdaging 1: zinvolle evaluatie en verantwoording

26 Zoals de Commissie heeft opgemerkt, is het lastig een causaal verband te leggen tussen de strategie uit 2013 en waargenomen veranderingen. De doelstellingen van de strategie uit 2013 waren erg breed geformuleerd en drukten eerder een visie dan een meetbare streefwaarde uit[38]. Het is een uitdaging om initiatieven te ontwikkelen die zijn afgestemd op deze brede doelstellingen, omdat meetbare streefwaarden ontbreken. Met het geactualiseerde beleidskader voor cyberdefensie (2018) zal worden beoogd doelstellingen te ontwikkelen die aangeven wat het minimale niveau van cyberbeveiliging en vertrouwen is dat moet worden bereikt. Deze zullen echter alleen betrekking hebben op cyberdefensie; er zijn geen doelstellingen bepaald voor het gewenste niveau van weerbaarheid voor de hele EU.

27 De resultaten worden zelden gemeten en op weinig beleidsterreinen zijn evaluaties uitgevoerd[39]. Dit komt met name doordat veel maatregelen — wetgeving en andere maatregelen — slechts recentelijk ten uitvoer zijn gelegd, waardoor hun impact nog niet volledig kan worden geëvalueerd. De uitdaging is om zinvolle beoordelingscriteria vast te stellen die kunnen helpen met het meten van deze impact. Bovendien is rigoureuze evaluatie over het algemeen nog niet de norm voor cyberbeveiliging. Er moet daarom worden overgestapt op een prestatiecultuur met geïntegreerde evaluatiepraktijken en gestandaardiseerde verslaglegging. De evaluatie en monitoring van de stand van zaken met betrekking tot de cyberbeveiliging en -paraatheid van de EU maken geen deel uit van het huidige mandaat van Enisa.

28 Op feiten gebaseerde beleidsvorming is afhankelijk van de beschikbaarheid van voldoende betrouwbare gegevens en statistieken om trends en behoeften te kunnen monitoren en analyseren. Het ontbreken van een verplicht, gemeenschappelijk monitoringsysteem heeft tot gevolg dat betrouwbare gegevens schaars zijn. Indicatoren zijn vaak niet voorhanden en zijn lastig te definiëren[40]. Op bepaalde

terreinen zijn echter wel specifieke maatstaven ontwikkeld die worden gebruikt voor de bestrijding van ernstige en georganiseerde misdaad. Dit geldt bijvoorbeeld voor de EU-beleidscyclus.

29 Weinig lidstaten verzamelen met regelmaat officiële gegevens over cyberkwesties, waardoor de vergelijkbaarheid van gegevens beperkt is. De EU heeft tot nu toe weinig aanwijzingen gegeven met betrekking tot de noodzaak om statistieken op Europees niveau te consolideren[41]. Er zijn ook een paar onafhankelijke, EU-brede analyses beschikbaar waarin wordt ingegaan op belangrijke onderwerpen als[42] de economie van cyberbeveiliging, met inbegrip van gedragsaspecten (slecht afgestemde prikkels, informatieasymmetrie); het begrijpen van de impact van cyberstoringen en cybercriminaliteit; macrostatistieken over cybertrends en verwachte uitdagingen, en de beste oplossingen om dreigingen het hoofd te bieden.

30 Wegens het ontbreken van specifieke doelstellingen en de schaarsheid van betrouwbare gegevens en duidelijk gedefinieerde indicatoren, is de beoordeling van wat er is bereikt met de strategie tot nu toe grotendeels kwalitatief geweest. In voortgangsverslagen worden vaak de activiteiten die worden uitgevoerd of de bereikte mijlpalen beschreven, zonder dat de resultaten grondig worden gemeten. Bovendien is er nog geen referentiepunt voor de beoordeling van de weerbaarheid van het systeem bepaald. Voorts is het wegens het ontbreken van een gecodificeerde definitie van cybercriminaliteit bijna onmogelijk relevante EU-indicatoren te vinden die zouden kunnen helpen met de monitoring en evaluatie.

31 Het onafhankelijke toezicht op de tenuitvoerlegging van het beleid inzake cyberbeveiliging verschilt van lidstaat tot lidstaat. We hebben een enquête gehouden onder nationale rekenkamers over hun ervaringen met controles op dit terrein. De helft van de respondenten[43] had op dit terrein nooit controles uitgevoerd. Degenen die wel controles op dit gebied hebben uitgevoerd, richtten zich hierbij met name op informatiegovernance, de bescherming van kritieke infrastructuur, informatie-uitwisseling en coördinatie tussen belangrijke belanghebbenden, alsook op paraatheid, het melden van en het reageren op incidenten. De onderwerpen waar het minst aandacht aan werd besteed waren maatregelen om bewustzijn te kweken en de kloof op het gebied van digitale vaardigheden. De resultaten van deze controles of evaluaties werden niet altijd openbaar gemaakt op grond van nationale veiligheid. Er is een lijst met gepubliceerde controleverslagen van nationale rekenkamers opgenomen in ***bijlage III***.

32 Beperkte cybervaardigheden (zie ook de paragrafen ***82-90***) en moeilijkheden in het evaluatieproces werden gezien als de grootste uitdagingen voor het controleren van overheidsmaatregelen op dit terrein.

Uitdaging 2: iets doen aan de hiaten in de EU-wetgeving en de ongelijke omzetting ervan

33 Nieuwe technologieën en dreigingen ontstaan veel sneller dan dat de EU wetgeving opstelt en ten uitvoer legt. Bij het ontwerpen van de procedures van de Unie is geen rekening gehouden met het digitale tijdperk. Het ontwikkelen van innovatieve en flexibele procedures om een beleids- en juridisch kader te garanderen dat geschikt is voor het beoogde doel[44] en het mogelijk maakt om de toekomst beter te anticiperen en vorm te geven, is een kritieke prioriteit[45].

34 Ondanks een streven naar meer samenhang blijft het wetgevingskader voor cyberbeveiliging onvolledig (zie ***tabel 1*** voor enkele voorbeelden). Fragmentatie en hiaten staan de verwezenlijking van de algehele beleidsdoelstellingen in de weg en leiden tot ondoelmatigheden. In de beoordeling van de strategie stelde de Commissie onder meer hiaten vast op de volgende terreinen: het Internet der dingen, het evenwicht in de verantwoordelijkheden van gebruikers en leveranciers van digitale producten en bepaalde aspecten waarop niet wordt ingegaan in de NIS-richtlijn. Met de voorgestelde cyberbeveiligingsverordening wordt getracht hier iets aan te doen door “security-by-design” te bevorderen middels een EU-brede certificeringsregeling. Sommige belanghebbenden zijn van mening dat er nog steeds een zichtbaar gebrek is aan een welomschreven beleid voor de cybersector en een gemeenschappelijke benadering van cyberspionage[46].

Tabel 1 — Hiaten in en ongelijke omzetting van het wetgevingskader (niet uitputtend)

Beleidsterrein	Voorbeelden
Digitale eengemaakte markt	o In de huidige richtlijn inzake de verkoop van consumptiegoederen wordt niet ingegaan op cyberbeveiliging. Met de voorgestelde richtlijn betreffende digitale inhoud[47] en onlineverkoop[48] wordt getracht deze kloof te dichten. o Er bestaan in de EU-lidstaten beperkte en diverse juridische kaders met betrekking tot de zorgplicht, hetgeen leidt tot juridische onzekerheid en problemen bij het afdwingen van rechtsmiddelen[49]. o In de lidstaten wordt op uiteenlopend tempo beleid inzake de openbaarmaking van zwakke punten in software ontwikkeld, zonder dat er op EU-niveau een overkoepelend juridisch kader is om een gecoördineerde benadering mogelijk te maken[50].
Versterking van de netwerk- en informatiebeveiliging	o De lidstaten mogen als zij dat willen sectoren opnemen die in de NIS-richtlijn niet worden genoemd[51]. De accommodatiesectoren, die niet in de richtlijn worden genoemd, kunnen een toegangspoort vormen voor andere misdaden, waaronder mensen- en drugshandel en illegale migratie[52].
Bestrijding van cybercriminaliteit	o Veel lidstaten hebben elektronisch bewijsmateriaal nog niet gedefinieerd in hun nationale wetgeving[53] (zie ook paragraaf ***22***). o In het huidige kaderbesluit over fraude met niet-contante betaalmiddelen wordt niet uitdrukkelijk ingegaan op niet-fysieke betaalmiddelen als virtuele valuta, elektronisch geld en mobiel geld, en ook wordt er geen aandacht besteed aan phishing, skimming en het bezitten en delen van informatie over betalers[54]. o In de richtlijn over aanvallen op informatiesystemen wordt niet rechtstreeks ingegaan op de illegale verkrijging van gegevens van binnenuit (bijv. cyberspionage), hetgeen het lastig maakt om de wet te handhaven[55]. o In het verlengde van het vonnis van het Hof van Justitie van de Europese Unie inzake het bewaren van gegevens[56]vermogen hebben verschillen in de toepassing van het juridisch kader door de lidstaten de handhaving van de wetgeving in de weg gestaan, hetgeen mogelijk heeft geleid tot het verlies van onderzoekslijnen en een belemmering van de doeltreffende vervolging van online criminele activiteiten[57].

Bron: ERK.

35 De toepassing van bepaalde aspecten van de wetgeving blijft voor zowel nationale autoriteiten als particuliere exploitanten optioneel. Zo is in het kader van de Samenwerkingsgroep de evaluatie van de nationale strategieën voor de beveiliging van netwerk- en informatiesystemen en de doeltreffendheid van CSIRT's bijvoorbeeld vrijwillig. Ook zal de toepassing van certificering voor ICT-producten en -diensten in het kader van de voorgestelde certificeringsregeling vrijwillig zijn.

36 In de EU is cyberbeveiliging een bevoegdheid van de lidstaten. Desondanks heeft de EU een cruciale rol te spelen bij het scheppen van de voorwaarden waaronder de lidstaten hun capaciteiten kunnen uitbreiden, samen kunnen werken en vertrouwen kunnen wekken. Maar met het oog op de grote verschillen tussen de lidstaten wat betreft hun vermogen en betrokkenheid[58] blijft het verstrekken van (voor de nationale veiligheid) gevoelige informatie vrijwillig.

37 De inconsequente omzetting van de EU-wetgeving in de verschillende lidstaten kan leiden tot juridische en operationele incoherentie en belemmert dat het volledige potentieel van de wetgeving wordt benut. Zo kijken de lidstaten bijvoorbeeld verschillend naar de manier waarop controles op de uitvoer van producten voor tweeërlei gebruik moeten worden uitgevoerd[59], met als resultaat dat sommige in de EU gevestigde bedrijven mogelijk technologieën en diensten uitvoeren die kunnen worden gebruikt voor cyberbewaking en mensenrechtenschendingen door middel van censuur of inbreuk. Het Europees Parlement heeft hierover zijn bezorgdheid geuit[60].

38 Voorts is om de privacy en vrijheid van meningsuiting te beschermen een op maat gemaakt wetgevingsinitiatief nodig om het noodzakelijke evenwicht te garanderen tussen de bescherming van de fundamentele waarden en het tegemoetkomen aan de behoeften van de EU op het gebied van veiligheid. Hoe kunnen we bijvoorbeeld end-to-end-versleuteling garanderen en tegelijkertijd de beste manier vinden om de wetshandhaving te ondersteunen? Of hoe kunnen we de doelstellingen van de AVG verwezenlijken en tegelijkertijd begrijpen wat de implicaties ervan zijn voor openbaar beschikbare informatie over de eigenaren van domeinnamen of van blokken IP-adressen? En welke negatieve gevolgen kan dit hebben voor onderzoeken van wetshandhavingsinstanties[61]?

39 Wetgeving alleen garandeert geen weerbaarheid. Het doel van de NIS-richtlijn is om in de EU een hoog niveau van beveiliging te garanderen, maar de richtlijn concentreert zich expliciet op het realiseren van een minimale in plaats van een maximale harmonisering[62]. Er zullen hiaten blijven ontstaan naarmate het cyberlandschap zich verder ontwikkelt.

Aandachtspunten — beleidskader

- Welke kritieke stappen zijn nodig om onder zowel beleidsmakers als wetgevers een verschuiving teweeg te brengen in de richting van een sterker op prestaties gerichte cultuur met betrekking tot cyberbeveiliging, met inbegrip van een definitie van algehele weerbaarheid?

- Hoe kan onderzoek beter bijdragen aan het genereren van de gegevens en statistieken die nodig zijn om zinvolle evaluaties mogelijk te maken?

- Hoe kunnen de wetgevingsprocedures van de EU worden aangepast zodat ze flexibeler zijn en beter rekening houden met de snelheid waarmee nieuwe technologieën en dreigingen ontstaan?

- Hoe kan de ontwikkeling van maatstaven (indicatoren, streefwaarden) in de EU-beleidscyclus worden aangepast, opgeschaald en gerepliceerd in het hele domein van cyberbeveiliging?

- Wat kunnen nationale rekenkamers leren van elkaars benaderingen van controles van beleid en maatregelen op het gebied van cyberbeveiliging?

- Welke inconsistenties in de omzetting en tenuitvoerlegging van het juridisch kader van de EU ondermijnen een doeltreffender aanpak van tekortkomingen op het gebied van cyberbeveiliging en -criminaliteit en hoe kunnen de lidstaten en EU-instellingen deze het best verhelpen?

- Hoe doeltreffend zijn de controles van de EU op de uitvoer van cybergoederen en -diensten teneinde mensenrechtenschendingen buiten de EU te voorkomen?

Financiering en uitgaven

40 De EU wil de veiligste onlineomgeving ter wereld worden. Om deze ambitie waar te maken, moeten alle belanghebbenden aanzienlijke inspanningen leveren, onder meer door te zorgen voor voldoende en goed beheerde financiële basis.

Uitdaging 3: de investeringsniveaus afstemmen op de doelstellingen

De investeringen opschalen

41 Naar schatting bedragen de wereldwijde uitgaven voor cyberbeveiliging als percentage van het bbp 0,1 %. In de Verenigde Staten[63] is dit percentage ongeveer 0,35 % (de particuliere sector meegerekend). De uitgaven van de Amerikaanse federale overheid als percentage van het bbp liggen rond de 0,1 %, hetgeen voor 2019 overeenkomt met een begroting van 21 miljard dollar[64].

42 In vergelijking hiermee zijn de uitgaven in de EU lager, gefragmenteerd en worden ze vaak niet gedaan in het kader van een gecoördineerd, door de overheid geleid programma. Het is lastig om cijfers te vinden, maar naar schatting bedragen de overheidsuitgaven voor cyberbeveiliging in de EU tussen de 1 en 2 miljard euro per jaar[65]. Sommige lidstaten geven als percentage van hun bbp slechts een tiende, of zelfs nog minder, van dat van de VS uit[66]. De EU en haar lidstaten moeten weten hoeveel ze collectief investeren om te kunnen bepalen welke kloven moeten worden gedicht.

43 Het is lastig om een compleet beeld te schetsen, aangezien er wegens de transversale aard van cyberbeveiliging geen duidelijke gegevens beschikbaar zijn en omdat het vaak lastig is om een onderscheid te maken tussen uitgaven voor cyberbeveiliging en algemene IT-uitgaven[67]. Uit onze enquête is gebleken dat het, zowel in de publieke als in de particuliere sector, moeilijk is betrouwbare statistieken te vinden over de uitgaven. Driekwart van de nationale rekenkamers gaf aan geen gecentraliseerd overzicht te hebben van cybergerelateerde overheidsuitgaven en geen enkele lidstaat verplicht overheidsinstanties om in hun financiële plannen afzonderlijk verslag uit te brengen van uitgaven voor cyberbeveiliging.

44 Het opschalen van de publieke en particuliere investeringen in Europese bedrijven die zich specialiseren in cyberbeveiliging is een bijzonder grote uitdaging. Publiek kapitaal is vaak wel beschikbaar voor de opstartfase, maar wordt slechts in

mindere mate vrijgemaakt voor groei en expansie[68]. Er bestaan meerdere financieringsinitiatieven in de EU, maar deze worden onvoldoende benut, grotendeels wegens de bureaucratie die ermee is gemoeid[69]. In het algemeen presteren cyberbeveiligingsbedrijven in de EU slechter dan hun internationale evenknieën: het zijn er minder en gemiddeld werven ze aanzienlijk minder fondsen[70]. Garanderen dat start-ups doeltreffend worden bereikt en gefinancierd, is daarom cruciaal om de digitale-beleidsdoelstellingen van de EU te verwezenlijken.

Vergroten van de impact

45 Het dichten van de investeringskloof met betrekking tot cyberbeveiliging moet wel leiden tot nuttige resultaten. Zo worden resultaten, ondanks de kracht van de onderzoeks- en innovatiesector van de EU, onvoldoende gepatenteerd, gecommercialiseerd en opgeschaald om bij te dragen aan een verbetering van de weerbaarheid, het concurrentievermogen en de digitale autonomie[71]. Dit doen de wereldwijde concurrenten van de EU een stuk beter. Dat resultaten onvoldoende worden benut, komt door een hele reeks van factoren[72], waaronder:

- het ontbreken van een consistente transnationale strategie om de benadering op te schalen en deze zo af te stemmen op de bredere behoefte van de EU aan digitaal concurrentievermogen en meer digitale autonomie;
- de aanzienlijke duur van de cyclus van de waardeketen, waardoor instrumenten soms verouderd raken;
- het gebrek aan duurzaamheid, aangezien projecten meestal eindigen omdat het projectteam uiteenvalt, waarna de ondersteuning, onder meer in de vorm van updates en patches, ook wordt stopgezet.

46 Het voorstel van de Commissie om een netwerk van kenniscentra voor cyberbeveiliging en een kenniscentrum voor onderzoek op te richten, vormt een poging om fragmentatie in het onderzoek naar cyberbeveiliging tegen te gaan en grootschalige investeringen te bevorderen[73]. In totaal zijn er zo'n 665 kenniscentra in de hele EU.

Uitdaging 4: een duidelijk overzicht van de uitgaven uit de EU-begroting

47 Het is belangrijk om een gecentraliseerd overzicht te hebben van de uitgaven met het oog op de transparantie en een betere coördinatie. Zonder een dergelijk overzicht

is het moeilijk voor beleidsmakers om te zien hoe de uitgaven aansluiten op de behoeften om prioritaire doelstellingen te verwezenlijken.

48 Er is geen speciale begroting waaruit de strategie inzake cyberbeveiliging wordt gefinancierd. Op EU-niveau worden de uitgaven voor cyberbeveiliging in plaats daarvan gefinancierd uit de algemene begroting van de EU en medegefinancierd door de lidstaten. Uit onze analyse komt een complexe combinatie naar voren van ten minste tien verschillende instrumenten binnen de algemene begroting van de EU, maar het is niet duidelijk hoe de fondsen worden verdeeld (zie ***bijlage II***).

49 Het opstellen van een duidelijk overzicht van de uitgaven voor een onderwerp dat raakvlakken heeft met vele beleidsterreinen, blijft een forse uitdaging. De uitgavenprogramma's worden beheerd door verschillende onderdelen van de Commissie, die elk hun eigen doelen, regels en tijdschema's hebben. Het plaatje wordt nog ingewikkelder als we rekening houden met de medefinanciering door de lidstaten, waarvan sprake is bij het Fonds voor interne veiligheid (Politie)[74].

Herleidbare uitgaven voor cyberbeveiliging

50 In de periode 2014-2018 heeft de Commissie ten minste 1,4 miljard EUR uitgegeven aan de tenuitvoerlegging van de strategie[75], waarvan het grootste deel werd toegewezen aan Horizon 2020[76] (“H2020”). De financiering voor H2020 wordt grotendeels gekanaliseerd via het programma betreffende de uitdagingen voor veilige samenlevingen en via projecten inzake leiderschap in ontsluitende en industriële technologieën[77]. We hebben vastgesteld dat er tot september 2018 contractuele verplichtingen zijn aangegaan voor 279 projecten op het gebied van cyberbeveiliging, met een totale EU-financiering van 786 miljoen EUR[78]. In ***figuur 5*** wordt, op basis van de analyse, de typologie van deze projecten weergegeven.

Figuur 5 — H2020-onderzoeksprojecten op het gebied van cyberbeveiliging waarvoor een overeenkomst is ondertekend (miljoen EUR)

Bron: ERK.

51 In 2016 werd een contractueel publiek-privaat partnerschap (cPPP's) opgezet om de Europese cyberbeveiligingssector een impuls te geven. Het doel was om 450 miljoen EUR uit het H2020-programma naar het cPPP te kanaliseren en uiterlijk in 2020 nog eens 1,8 miljard EUR uit de particuliere sector aan te trekken. In de periode van 18 maanden tot en met 31 december 2017, was 67,5 miljoen EUR uit H2020 naar cPPP gekanaliseerd en had de particuliere sector 1 miljard EUR geïnvesteerd[79].

52 De strijd tegen cybercriminaliteit wordt ook ondersteund door het Fonds voor interne veiligheid — Politie (ISF-P). Het ISF-P ondersteunt studies, bijeenkomsten van deskundigen en communicatieactiviteiten. Tussen 2014 en 2017 werd hier bijna 62 miljoen EUR aan besteed. De lidstaten kunnen bovendien subsidies aanvragen voor apparatuur, opleiding, onderzoek en gegevensverzameling onder gedeeld beheer. Negentien lidstaten hebben van deze subsidies, met een waarde van 42 miljoen EUR, geprofiteerd.

53 In het kader van het programma “Justitie” van DG JUST bedroegen de financiële middelen voor de ondersteuning van justitiële samenwerking en de uitvoering van de

verdragen betreffende wederzijdse rechtshulp, met bijzondere aandacht voor de uitwisseling van elektronische gegevens en financiële informatie, 9 miljoen EUR.

54 In de NIS-richtlijn wordt expliciet aangegeven dat CSIRT's over voldoende middelen moeten beschikken om hun taken doeltreffend uit te kunnen voeren[80]. Tussen 2016 en 2018 was jaarlijks een bedrag van 13 miljoen EUR beschikbaar uit de Financieringsfaciliteit voor Europese verbindingen dat lidstaten konden aanvragen ter ondersteuning van de tenuitvoerlegging van de vereisten van de richtlijn. Er is geen onderzoek gedaan naar de financiële middelen die het CSIRT-netwerk en de Samenwerkingsgroep daadwerkelijk nodig hebben om een impact te hebben.

55 Meerdere van de operationele uitgaven van de agentschappen zijn specifiek bestemd voor activiteiten op het gebied van cyberbeveiliging of cybercriminaliteit. Het is echter lastig om exacte cijfers uit de openbaar beschikbare informatie te halen.

56 Het Verdrag van Boedapest (zie paragraaf ***11***) vormde de ruggengraat van de externe cybergerelateerde uitgaven van de EU. De EU heeft in de periode 2014-2018 ongeveer 50 miljoen EUR uitgegeven aan de versterking van de cyberbeveiliging buiten haar grenzen. Ongeveer de helft van dit bedrag is uitgegeven via het Instrument voor bijdrage aan stabiliteit en vrede, met één hoofdproject — GLACY+, goed voor 13,5 miljoen EUR — waarmee wordt beoogd wereldwijd de capaciteit voor de ontwikkeling en tenuitvoerlegging van wetgeving inzake cybercriminaliteit te vergroten en de internationale samenwerking te versterken[81]. Bij de uitgaven via andere financiële instrumenten van de EU lag de nadruk met name op de Westelijke Balkan[82] en het Europees nabuurschap. Met het Cybercrime@EaP-project met de landen van het Oostelijk Partnerschap wordt bijvoorbeeld beoogd de internationale samenwerking inzake cybercriminaliteit en elektronisch bewijsmateriaal te verbeteren.

Andere uitgaven voor cyberbeveiliging

57 Het is niet altijd mogelijk om specifiek aan te geven hoeveel er binnen EU-programma's wordt uitgegeven aan cyberbeveiliging.

- Zo zijn er ook H2020-fondsen gekanaliseerd via de Gemeenschappelijke Onderneming elektronische componenten en systemen voor Europees leiderschap (ECSEL) voor cyber-fysieke systemen. We konden echter niet vaststellen welke van de 27 projecten waarvoor tussen 2015 en 2016 in totaal 437 miljoen EUR werd uitgetrokken, verband hielden met cyberbeveiliging.

- Er is tot 400 miljoen EUR beschikbaar voor uitgaven aan cyberbeveiliging en vertrouwensdiensten in het kader van de Europese structuur- en investeringsfondsen. Dit kan onder meer worden gebruikt voor investeringen in beveiliging en gegevensbescherming om de interoperabiliteit en interconnectie van digitale infrastructuur, elektronische identificatie en privacy- en vertrouwensdiensten te verbeteren.

58 In haar activiteitenplan voor 2018 heeft de Europese Investeringsbank aangegeven voornemens te zijn de financiering voor technologie voor tweeërlei gebruik, cyberbeveiliging en civiele veiligheid te verhogen naar 6 miljard EUR voor een periode van drie jaar[83].

Vooruitblik

59 Het cyberbeveiligingscomponent van het voorgestelde nieuwe programma Digitaal Europa (DEP), met een begroting van 2 miljard EUR[84] voor de periode 2021-2027, is ontwikkeld om de cyberbeveiligingssector van de EU en de algehele bescherming van de maatschappij te versterken door de tenuitvoerlegging van de NIS-richtlijn te ondersteunen. Het voorgestelde netwerk van kenniscentra voor cyberbeveiliging en het kenniscentrum voor onderzoek, waarmee wordt beoogd een meer gestroomlijnde benadering toe te passen, zal naar verwachting het belangrijkste uitvoeringsmechanisme vormen voor EU-uitgaven in het kader van het DEP.

60 De defensie-uitgaven uit de EU-begroting zijn onlangs gestegen dankzij de Industriële ontwikkelingsprogramma's voor de Europese defensie, waarvoor in 2019 en 2020 500 miljoen EUR moet worden toegewezen[85]. Hierbij zal de nadruk liggen op de verbetering van de coördinatie en efficiëntie van de defensie-uitgaven van de lidstaten door middel van stimuleringsmaatregelen voor gezamenlijke ontwikkeling. Er wordt mee beoogd na 2020 in totaal 13 miljard EUR aan investeringen in defensiecapaciteiten te genereren via het Europees Defensiefonds, waarvan een deel bestemd zal zijn voor cyberbeveiliging[86].

Uitdaging 5: de EU-agentschappen voorzien van voldoende middelen

61 De drie organen die centraal staan binnen het beleid van de EU inzake cyberbeveiliging — Enisa, EC3 van Europol en CERT-EU (zie ***tekstvak 2***) — worden, in een tijd waarin politieke prioriteiten steeds meer worden ingegeven door veiligheid, geconfronteerd met een tekort aan middelen. Met de huidige toewijzing van personele

en financiële middelen aan de EU-agentschappen blijft het voor hen een uitdaging om aan de verwachtingen te voldoen[87].

62 Aan de verzoeken van de agentschappen om aanvullende middelen teneinde te kunnen voldoen aan de steeds hogere verwachtingen, is nog niet volledig tegemoetgekomen, hetgeen de (tijdige) verwezenlijking van beleidsdoelstellingen in gevaar kan brengen. Bijvoorbeeld:

- Enisa kon in 2017 zijn doelstellingen niet volledig realiseren wegens de beperkte middelen[88]. In het pakket van 2017 werden aanvullende middelen voorgesteld om het nieuwe mandaat van Enisa ten uitvoer te kunnen leggen.

- Gezien het tempo waarop analisten worden geworven en wordt geïnvesteerd in ICT-capaciteiten kan EC3 van Europol de vraag niet bijbenen[89]. De Taskforce voor gezamenlijke actie op het gebied van cybercriminaliteit (J-CAT) van Europol en de EC wordt ondersteund door deskundigen uit de lidstaten en derde landen om op inlichtingen gebaseerde onderzoeken te kunnen uitvoeren. De kosten hiervan worden echter grotendeels gedragen door de uitzendende lidstaten, waardoor de inzet van een groter aantal deskundigen wordt ontmoedigd. Deskundigen worden tijdelijk, per case aangenomen met gedeeltelijke financiering door Europol of uit de EU-beleidscyclus, zodat er meer landen kunnen deelnemen.

63 Sommige beperkingen zijn door de agentschappen zelf veroorzaakt. Veel personeelsleden van CERT-EU en Enisa zijn contractanten en de procedures voor hun werving zijn over het algemeen langzaam. Andere beperkingen, bijvoorbeeld met betrekking tot het aantrekken en vasthouden van talent, vloeien voort uit het onvermogen van de agentschappen om te concurreren met de salarissen uit de particuliere sector of om aantrekkelijke doorgroeimogelijkheden te bieden. Daarom heeft Enisa tussen 2014 en 2016 veel werk uitbesteed[90].

64 Een tekort aan personeel en noodzakelijke tools kan tot aanzienlijke risico's leiden, met name wat betreft de verzameling van inlichtingen over dreigingen. De hoeveelheid data uit open en gesloten bronnen blijft groeien en het risico bestaat dat dit het vermogen van analisten om gedegen analyses van de dreigingen uit te voeren, te boven gaat. Zonder de juiste capaciteiten en instrumenten om dergelijke gegevens met succes te integreren en onderling te verbinden, zullen deze data niet op doeltreffende wijze leiden tot bruikbare informatie over dreigingen die in de hele EU kan worden gedeeld en geanalyseerd[91].

Aandachtspunten — financiering en uitgaven

- Hoe kunnen de Commissie en wetgevers de uitgaven van de EU voor cyberbeveiliging stroomlijnen en beter afstemmen op duidelijk geformuleerde doelstellingen?

- Hoe kan het tekort aan middelen voor de EU-agentschappen op een integrale manier worden aangepakt, rekening houdend met de behoeften en doelstellingen van de Unie?

- Welke maatregelen zijn vastgesteld op het niveau van de EU en van de lidstaten om de obstakels weg te nemen die belemmeren dat kmo's investeringskapitaal aantrekken om hun activiteiten op te schalen?

- Welke concrete, constante resultaten worden behaald met de H2020-fondsen wat betreft de ontwikkeling van oplossingen voor cyberbeveiliging?

- Hoe leiden de initiatieven voor capaciteitsopbouw van de EU tot een versterking van de capaciteiten buiten haar grenzen, in overeenstemming met de EU-waarden?

De cyberweerbaarheid van de maatschappij vergroten

65 Cyberbeveiligingsgovernance heeft betrekking op de beheersing van dreigingen en risico's, de versterking van de capaciteiten en het bewustzijn, en coördinatie en informatie-uitwisseling op basis van vertrouwen.

Uitdaging 6: versterken van de governance en normen

Informatiebeveiligingsgovernance

66 Informatiebeveiligingsgovernance heeft betrekking op het invoeren van structuren en beleid om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen. Het is meer dan slechts een technische kwestie en vereist doeltreffend leiderschap, robuuste processen en strategieën die zijn afgestemd op de doelstellingen van de organisatie[92]. Cyberbeveiligingsgovernance maakt hier deel van uit en heeft betrekking op alle soorten cyberdreigingen, waaronder gerichte, geavanceerde aanvallen, inbreuken en incidenten die lastig te detecteren of te beheersen zijn.

67 Lidstaten hebben verschillende modellen voor cyberbeveiligingsgovernance en de verantwoordelijkheden voor cyberbeveiliging zijn vaak verspreid over diverse entiteiten. Deze verschillen kunnen de samenwerking in de weg staan die nodig is om te reageren op grootschalige, grensoverschrijdende incidenten en om inlichtingen over dreigingen uit te wisselen op nationaal niveau en — in nog sterkere mate — EU-niveau. Uit onze enquête onder nationale rekenkamers kwam naar voren dat de zwakke plekken in de governanceregelingen en de risicobeheersing van overheidsinstanties werden gezien als de grootste risico's.

68 De consequenties voor organisaties uit de particuliere sector kunnen ook ernstig zijn, maar toch wemelt het ook hier van de zwakke plekken in de cybergovernance. Bijna negen op de tien organisaties geven aan dat met hun cyberbeveiligingsfunctie niet volledig tegemoet wordt gekomen aan hun behoeften[93] en de personen die verantwoordelijk zijn voor cyberbeveiliging zijn vaak ten minste twee niveaus verwijderd van het bestuur[94].

69 In de EU-richtlijnen inzake vennootschapsrecht worden geen specifieke vereisten vastgesteld met betrekking tot de vrijgave van informatie over cyberrisico's. In de Verenigde Staten heeft de Securities and Exchange Commission onlangs niet-bindende richtsnoeren gepubliceerd om overheidsbedrijven te helpen informatie te publiceren over risico's en incidenten met betrekking tot cyberbeveiliging[95]. Het Gemengd Comité van de Europese toezichthoudende autoriteiten (ETA's)[96] heeft gewaarschuwd voor de toenemende cyberrisico's en heeft financiële instellingen aangemoedigd hun fragiele IT-systemen te verbeteren en de inherente risico's van informatiebeveiliging, connectiviteit en uitbesteding te analyseren[97].

70 Het versterken van de informatiebeveiligingsgovernance van kmo's is bijzonder lastig, aangezien zij over het algemeen niet in staat zijn de juiste systemen in te voeren. Kmo's beschikken niet over geschikte richtsnoeren voor de toepassing van vereisten met betrekking tot informatiebeveiliging en -privacy en het beperken van technologische risico's[98]. Het is daarom een belangrijke uitdaging om hun behoeften beter te begrijpen en de nodige prikkels en ondersteuning aan te bieden.

71 Het gebrek aan een samenhangend, internationaal governancekader voor cyberbeveiliging beperkt het vermogen van de internationale gemeenschap om te reageren op cyberaanvallen en deze te beperken. Het is daarom belangrijk om een consensus te bereiken over een dergelijk governancekader, waarin de belangen en waarden van de EU optimaal tot uitdrukking komen[99]. Pogingen om bindende internationale cyberspace-normen vast te stellen worden steeds meer beladen, hetgeen blijkt uit het gebrek aan overeenstemming binnen de VN-groep van regeringsdeskundigen in 2017 over de manier waarop het internationaal recht moeten worden toegepast wanneer staten reageren op incidenten.

72 Om haar agenda voor cyberspace-governance te versterken, heeft de EU ook zes cyberpartnerschappen geformaliseerd teneinde regelmatige beleidsdialogen te voeren waarmee wordt beoogd vertrouwen te kweken en gemeenschappelijke gebieden voor samenwerking vast te stellen[100]. De resultaten zijn gemengd, maar over het algemeen kan de EU in het internationale domein nog niet worden beschouwd als een “belangrijke speler op het gebied van cyberbeveiliging”, al heeft zij haar rol wel vergroot[101].

Informatiebeveiliging en de EU-instellingen

73 Elke EU-instelling heeft eigen regels met betrekking tot informatiebeveiligingsgovernance. Op grond van een interinstitutionele overeenkomst krijgen andere instellingen en agentschappen van de Commissie bijstand op het gebied

van informatiebeveiliging. De instellingen en organen van de EU hebben erkend dat zij hun cybercapaciteiten en benaderingen van risicobeheersing op samenhangende wijze moeten ontwikkelen. De Commissie, de Raad en de EDEO zullen in 2020 een verslag presenteren aan de Horizontale groep cybervraagstukken over governance en de vorderingen die zijn gemaakt met het verduidelijken en harmoniseren van cyberbeveiligingsgovernance in de EU-instellingen en -agentschappen[102].

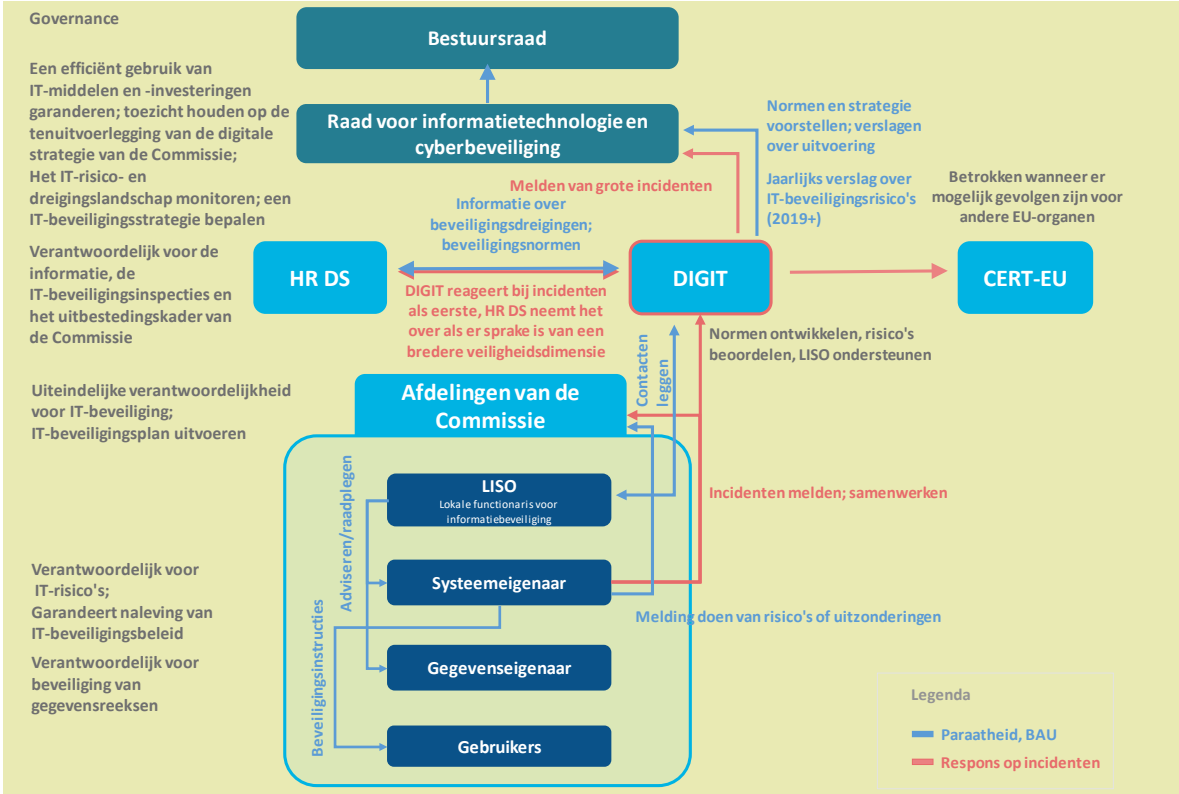
74 Binnen de Commissie is directoraat-generaal Informatica (DIGIT) verantwoordelijk voor de beveiliging van de IT-infrastructuur en -diensten (zie ***tekstvak 3***). De belangrijkste doelstellingen met betrekking tot IT in de digitale strategie van de Commissie zijn het opnemen van IT-beveiliging in het beheerproces, het verstrekken van (kosten)effectieve infrastructuur en weerbaarheid, het verbreden van de reikwijdte van de detectie van en de respons bij incidenten, en het integreren van IT en beveiligingsgovernance[103]. De Commissie garandeert in haar overeenkomsten met aanbieders dat bijna alle software actief wordt onderhouden en dat alleen door de leverancier ondersteunde software wordt gebruikt[104].

75 Het belang van het beschermen van de instellingen geldt ook voor de wereldwijde GVDB-missies en -structuren van de EU. Een van de prioriteiten van het beleidskader voor cyberdefensie van de EU (update 2018) is om de bescherming aan te scherpen van de communicatie- en informatiesystemen die door de EU-entiteiten worden gebruikt voor het GVDB. Er is bij EDEO inmiddels een interne Raad voor Cybergovernance opgericht, die voor het eerst is bijeengekomen in juni 2017[105].

Tekstvak 3

Beschermen van de informatiesystemen van de Commissie

De circa 1 300 systemen en 50 000 apparaten van de Commissie zijn een constant doelwit van cyberaanvallen. De verantwoordelijkheid voor IT is gedecentraliseerd, zoals te zien is in het diagram hieronder. Informatie- en IT-beveiliging zijn gebaseerd op een gemeenschappelijk IT-beveiligingsplan dat door DIGIT wordt opgesteld. De Raad voor informatietechnologie en cyberbeveiliging fungeert in feite als het hoofd Informatiebeveiliging van de Commissie en verbindt de operationele zijde van informatiebeveiliging met de hoogste bestuurslaag van de Commissie, die wordt vertegenwoordigd door de bestuursraad.



Bron: ERK, op basis van besluiten van de Commissie[106].

De voornaamste taak van het DG Personele middelen en Beveiliging (DG HR DS) is om het personeel, de informatie en de activa van de Commissie te beschermen. Ook voert het DG veiligheidsonderzoeken uit bij incidenten die een bredere veiligheidsdimensie hebben dan alleen IT en draagt het derhalve bij aan activiteiten op het gebied van contra-intelligentie en terrorismebestrijding.

DIGIT is verantwoordelijk voor IT-beveiliging en treedt als gastheer op voor CERT (Computercrisisteam). CERT-EU werd in 2011 opgericht en werkt met een begroting van circa 2,5 miljoen EUR per jaar en ongeveer 30 personeelsleden. Het is het team dat als eerst in actie komt bij een incident op het gebied van informatiebeveiliging waarbij meerdere instellingen zijn betrokken, maar is niet 24/7 actief. Het team beheert een platform voor het delen van informatie. In 2018 heeft CERT-EU een niet-bindend memorandum van overeenstemming met Enisa, EC3 en het Europees Defensieagentschap ondertekend om de samenwerking en coördinatie te verbeteren. Ook heeft het een technische overeenkomst met het computercrisisteam van de NAVO (NCIRC).

Dreigings- en risicobeoordelingen

76 Gefundeerde, constante risicobeoordelingen zijn belangrijke instrumenten voor zowel publieke als particuliere organisaties. Er is echter geen standaardbenadering voor het classificeren en in kaart brengen van cyberdreigingen en voor risicobeoordelingen, hetgeen tot gevolg heeft dat de inhoud van beoordelingen

aanzienlijk varieert, wat een uitdaging vormt voor een coherente EU-brede aanpak van cyberbeveiliging[107]. Bovendien wordt bij deze beoordelingen vaak gebruikgemaakt van dezelfde bronnen of zelfs van andere dreigingsanalyses, waardoor een echokamer ontstaat waarin dezelfde bevindingen telkens weerklinken[108] en het gevaar bestaat dat er onvoldoende aandacht wordt besteed aan andere risico's. Deze tendens wordt versterkt door de constante terughoudendheid om informatie te delen en het feit dat te weinig incidenten worden gemeld.

77 De in de EDEO geïntegreerde Fusiecel voor analyse van hybride bedreigingen[109] is opgericht om het situationele bewustzijn te vergroten en de besluitvorming te ondersteunen door middel van het delen van analyses. De cel moet zijn expertise, onder meer op het gebied van cyberbeveiliging, echter uitbreiden. Tegelijkertijd verschaft CERT-EU de EU-instellingen, -organen en -agentschappen verslagen en briefings met betrekking tot de cyberdreigingen die voor hen relevant zijn.

78 Enisa heeft in het verleden opgemerkt dat veel lidstaten een kwalitatief inzicht hebben in de dreigingen en dat cyberdreigingen beter moeten worden gemodelleerd[110]. Het monitoren van de capaciteit voor strategische analyse zal de algehele kennis vergroten. In dreigingsanalyses wordt echter niet alleen ingegaan op technologische dreigingen, maar ook op sociaal-politieke en economische dreigingen, de drijvende krachten achter dreigingen en de motivering van actoren, om zo een completer beeld te verschaffen.

Stimuleringsmaatregelen

79 Er zijn nog steeds te weinig wettelijke en economische prikkels voor organisaties om incidenten te melden en er informatie over te delen. Veel organisaties zijn bang voor imagoschade en behandelen cyberaanvallen liever discreet of kopen de daders af. Het valt te bezien in welke mate het aantal meldingen met de NIS-richtlijn zal stijgen. De Commissie verwacht dat de verbeteringen met name op nationaal niveau zichtbaar zullen worden, maar de cyberbeveiligingsverordening zal een EU-brede visie toevoegen[111].

80 Door bepaalde normen op te nemen in de aanbestedingsprocedures, kunnen overheidsinstanties als kopers van digitale producten en diensten via openbare aanbestedingen en de financiering van onderzoek en programma's een aanzienlijke invloed uitoefenen op leveranciers (bijvoorbeeld wanneer ze bepaalde technische normen, zoals het internetprotocol IPv6, vaststellen om cybercriminaliteit te bestrijden). Momenteel is er echter geen gemeenschappelijk kader voor

cyberbeveiligingsinfrastructuur[112]. In dit opzicht kan de Commissie veel betekenen. Met het voorgestelde DEP voor het volgende meerjarig financieel kader wordt beoogd iets te doen aan de tot nu toe beperkte investeringen van de publieke sector in de aanschaf van de nieuwste cyberbeveiligingstechnologie.

81 Door middel van haar regelgevende bevoegdheden kan de Commissie garanderen dat de juiste normen worden ontwikkeld en breed worden toegepast om een betere beveiliging te garanderen. De Commissie en Europol werken samen met organen voor internetgovernance als ICANN (zie paragraaf ***38***) en RIPE-NCC[113], hetgeen essentieel is om te zorgen voor de juiste architectuur voor cyberbeveiliging om de wetshandhavings- en gerechtelijke autoriteiten te ondersteunen.

Uitdaging 7: de vaardigheden en het bewustzijn vergroten

82 Enisa heeft erop gewezen dat gebruikers een cruciale rol spelen bij het voorkomen en bestrijden van cyberaanvallen en dat het vergroten van de vaardigheden, de intensivering van de voorlichting en sterkere bewustmaking van groot belang zijn om de cyberweerbaarheid van de maatschappij te vergroten[114]. Mensen die goed weten hoe ze waarschuwingssignalen kunnen opvangen en over de juiste technieken beschikken, kunnen thuis en op hun werk aanvallen vertragen of voorkomen.

83 Met name de toenemende asymmetrie tussen de knowhow die nodig is om een cybermisdaad te begaan of een cyberaanval uit te voeren en de vaardigheden die nodig zijn om systemen ertegen te beschermen, is zorgwekkend. Het “crime-as-a-service”-model heeft de barrières voor toegang tot de markt van de cybercriminaliteit verlaagd: personen zonder technische kennis om deze objecten te bouwen, kunnen nu botnets huren of gebruikmaken van kits of ransomware-pakketten.

Opleiding, vaardigheden en capaciteitsontwikkeling

84 Het wereldwijde tekort aan cyberbeveiligingsvaardigheden wordt steeds groter. Sinds 2015 is dit tekort bij personeel met 20 % toegenomen[115]. Via de traditionele kanalen voor werving kan niet aan de vraag worden voldaan. Dit geldt onder meer voor management- en interdisciplinaire functies[116]. Bijna 90 % van het personeel dat zich wereldwijd bezighoudt met cyberbeveiliging is van het mannelijk geslacht. Dit hardnekkige gebrek aan genderdiversiteit beperkt het aanwezige talent verder[117]. Bovendien worden er aan universiteiten binnen niet-technische programma's bijna geen cybergerelateerde vakken onderwezen.

85 Er is over de gehele linie onderwijs en voorlichting nodig, voor ambtenaren, rechtshandhavingsambtenaren, gerechtelijke autoriteiten, de strijdkrachten en onderwijzers. De rechtbanken moeten kunnen omgaan met de snel veranderende specifieke technische kenmerken van cybercriminaliteit en de slachtoffers ervan[118]. Er zijn momenteel geen EU-brede normen voor opleiding en certificering[119]. Bij de EU-instellingen is het verkrijgen van de juiste mix van vaardigheden belangrijk. Zonder deze juiste mix van vaardigheden zijn de instellingen mogelijk niet in staat de reikwijdte, juiste partners en beveiligingsbehoeften te bepalen of hebben zij onvoldoende capaciteit om programma's te beheren. Dit kan op zijn beurt de doeltreffendheid van de EU-programma's of de beleidsvorming ondermijnen.

86 De lidstaten zijn verantwoordelijk voor onderwijsbeleid op EU-niveau; er vinden al verschillende opleidingsactiviteiten (zie ***tabel 2***) en -oefeningen (zie ***tekstvak 4***) plaats. De EU kan helpen met EU-brede normen voor studieprogramma's voor alle relevante disciplines[120]. Op het gebied van de digitale forensische wetenschap is bijvoorbeeld behoefte aan gemeenschappelijke opleidingsnormen om de weg naar de toelaatbaarheid als bewijsmiddel in de lidstaten te effenen. Als gevolg van de grensoverschrijdende aard van cybercriminaliteit kunnen er verschillende jurisdicties bij betrokken zijn, wat opleiding op EU-niveau vergt. Toch heeft Cepol, de politieacademie van de EU, opgemerkt dat meer dan twee derde van de lidstaten hun rechtshandhavingsambtenaren geen regelmatige cursussen inzake cyberkwesties aanbiedt[121]. De EU kan mogelijk ook manieren vaststellen om synergieën van onderwijs en opleiding in zowel de civiele als de militaire sfeer te benutten[122]. Enisa concludeerde echter dat er veel opleidingsmogelijkheden zijn in de kritieke sectoren, maar dat daarbij niet voldoende aandacht wordt besteed aan de weerbaarheid van kritieke infrastructuur[123].

Tabel 2 — Een aantal van de cybergerelateerde opleidingsinitiatieven van de EU

Projecten van het Europees Defensieagentschap, bijv. ondersteuning van oefeningen door de particuliere sector en het Cyber Ranges-project	Netwerk van de Europese Veiligheids- en defensieacademie (verschaft civiel-militaire opleidingen), met inbegrip van het Platform voor onderwijs, opleiding, evaluatie en oefeningen op cybergebied	Opleidingen van Enisa, dat programma's aanbiedt die mogelijk niet op de commerciële markt verkrijgbaar zijn
Opleidingsprogramma's van Europol, CEPOL, ECTEG[124] — met inbegrip van het Governancemodel voor opleidingen en het Kader voor opleidingscompetenties (incl. certificering)	Netwerk van kenniscentra en een onderzoeks- en kenniscentrum (voorstel)	Maatregelen inzake versleuteling, voorgesteld in het elfde voortgangsverslag over de Veiligheidsunie
Samenwerking tussen de EU en de NAVO inzake opleiding en onderwijs op het gebied van cyberdefensie	Militair Erasmusprogramma	Europees netwerk voor justitiële opleiding

Bron: ERK.

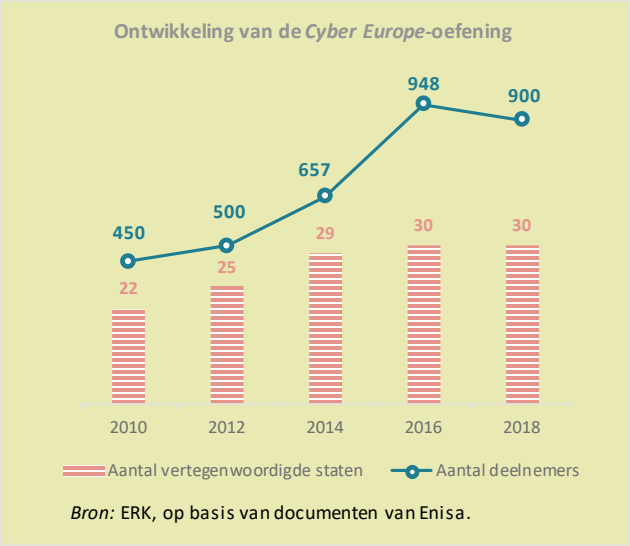
87 De EU heeft deskundigen op het gebied van terrorismebestrijding en veiligheid gedetacheerd bij 17 delegaties om de koppeling tussen de interne en externe veiligheid van de EU te versterken[125]. Ondanks de beperkte middelen kan cyber-knowhow helpen om de juiste projecten op te starten en synergieën vast te stellen met andere programma's of financieringsbronnen[126]. Deze knowhow kan er ook voor zorgen dat in politieke dialoog de schijnwerper meer wordt gericht op cyberbeveiliging, al concurreert het als thema wel met verschillende andere prioriteiten als migratie, georganiseerde misdaad en de terugkeer van buitenlandse strijders.

Tekstvak 4

Oefeningen

Oefeningen vormen een belangrijk element van onderwijs en opleiding op cybergebied en bieden unieke kansen om de paraatheid te vergroten door capaciteiten te testen, reacties op realistische scenario's te ontwikkelen en netwerken en werkrelaties op te bouwen. Sinds 2010 zijn er opmerkelijk meer oefeningen uitgevoerd.

Aan deze oefeningen wordt ter plekke of op afstand deelgenomen. Na de oefeningen worden beoordelingen uitgevoerd om vast te stellen welke lessen zijn geleerd, al wordt deze kennis op strategisch/politiek, operationeel en technisch niveau mogelijk nog niet volledig benut[127].



Bron: ERK, op basis van documenten van Enisa.

De vlaggenschipoefeningen van de EU en de NAVO — het tweejaarlijkse Cyber Europe (operationeel) en het jaarlijkse Locked Shields (technisch) — trekken meer dan 1 000 deelnemers uit ongeveer 30 deelnemende landen aan. Beide oefeningen zijn gericht op het beschermen en handhaven van kritieke infrastructuur tijdens gesimuleerde aanvalsscenario's. De diepgang van de oefeningen is aanzienlijk verbeterd: in beide oefeningen worden inmiddels elementen van media-, juridisch en financieel beleid geïntegreerd om het situationele bewustzijn van de deelnemers te vergroten. Met de parallelle en gecoördineerde PACE-oefeningen wordt de EU-NAVO-interactie in een hybride crisisscenario (strategisch) getest.

Dit zijn niet de enige internationale oefeningen. Enisa organiseert een jaarlijkse cyberuitdaging waarin teams concurreren om uitdagingen met betrekking tot beveiliging aan te gaan, zoals web- en mobiele beveiliging, cryptopuzzels, reverse engineering, alsook ethische en forensische aspecten. De eerste oefening op ministerieel niveau, EU CYBRID, vond plaats in september 2017. Bij deze oefening lag de nadruk op strategische besluitvorming. In 2018 werd van start gegaan met de aan de NAVO gekoppelde oefening Crossed Swords, met als doel de offensieve elementen van de Locked Shields-oefening te verbeteren. De NAVO organiseert ook de Cyber Coalition-oefeningen.

Een belangrijke uitdaging is om te garanderen dat alle relevante spelers worden betrokken bij de oefeningen en dat alle oefeningen goed worden gecoördineerd, teneinde dubbel werk te voorkomen en geleerde lessen efficiënt te delen.

Bewustzijn

88 Burgers zijn vaak gemakkelijke doelwitten voor aanvallen en de verspreiding van desinformatie, aangezien de kans groot is dat zij zich ongewild blootstellen door het gebruik van goedkope en breed gedistribueerde apparaten en software, en zij het slachtoffer kunnen worden van social engineering. Het kweken van bewustzijn is daarom essentieel om een doeltreffende cyberweerbaarheid te waarborgen, maar dit is bepaald geen gemakkelijke opgave, aangezien het moeilijk is voor leken om de complexiteit van cyberbeveiliging en de gerelateerde risico's te begrijpen.

89 De jaarlijkse Europese maand van de cyberbeveiliging en de Dag voor een veiliger internet zijn voorbeelden van initiatieven om het bewustzijn te vergroten. Zeven niet-EU-lidstaten nemen nu ook deel aan de Europese maand van de cyberbeveiliging[128]. Met de *Zeg nee!*-campagne van Europol wordt beoogd het risico te verkleinen dat kinderen online het slachtoffer worden van seksuele dwang en afpersing. Het is belangrijk dit risico te verkleinen, want momenteel doen weinig slachtoffers aangifte van deze strafbare feiten bij de politie[129]. De Commissie geeft toe dat de strategie inzake cyberbeveiliging slechts deels doeltreffend is geweest in het vergroten van het bewustzijn van burgers en bedrijven[130]. Dit komt door de omvang van de taak, de beperkte middelen, de ongelijke inspanningen van lidstaten en een gebrek aan wetenschappelijk bewijs over de beste manier om bewustzijn te kweken en te meten.

90 De uitdaging voor de Commissie en de relevante agentschappen is om te garanderen dat de maatregelen om het bewustzijn te vergroten, gericht zijn en voldoende openbaar worden gemaakt, inclusief zijn en zijn afgestemd op het dreigingslandschap, dat onbedoelde effecten als “beveiligingsmoeheid”[131] worden voorkomen en dat evaluatiemethoden en -indicatoren worden ontwikkeld om de doeltreffendheid ervan te beoordelen. Dit moet in gelijke mate gelden voor de EU-instellingen zelf, waar de cultuur van bewustzijn voor verbetering vatbaar is[132].

Uitdaging 8: betere informatie-uitwisseling en coördinatie

91 Cyberbeveiliging vereist samenwerking tussen de publieke en particuliere sector, met name om informatie en beste praktijken uit te wisselen. Om het juiste klimaat te creëren voor het delen van vertrouwelijke gegevens over de grenzen heen, is

vertrouwen op alle niveaus essentieel. Slechte coördinatie leidt tot fragmentatie, dubbel werk en een versnippering van expertise. Doeltreffende coördinatie kan resulteren in tastbare successen, zoals het van het internet halen van darkweb-marktplaatsen[133]. Ondanks de vorderingen die de afgelopen jaren zijn gemaakt, is het niveau van vertrouwen nog steeds ontoereikend[134], zowel op EU-niveau als in bepaalde lidstaten[135].

Coördinatie tussen EU-instellingen onderling en met de lidstaten

92 Een van de doelstellingen van de strategie inzake cyberbeveiliging en de coöperatieve structuren die zijn ingevoerd bij de NIS-richtlijn was om het vertrouwen tussen de belanghebbenden te vergroten. Bij de beoordeling van de strategie werd onderkend dat er op EU-niveau een basis is gelegd voor strategische en operationele samenwerking[136]. Desondanks is de coördinatie in het algemeen ontoereikend[137]. De uitdaging is om te garanderen dat de informatie-uitwisseling niet alleen zinvol is, maar ook een volledig beeld verschaft. In dit opzicht is het belangrijk om tot een gemeenschappelijk inzicht te komen met betrekking tot de aanvaarde terminologie (zie ***tekstvak 5***).

93 In de Enisa-evaluatie werd echter opgemerkt dat de aanpak van cyberbeveiliging in de EU onvoldoende gecoördineerd wordt, waardoor er weinig synergieën ontstaan tussen de activiteiten van Enisa en die van andere belanghebbenden. De samenwerkingsmechanismen bevinden zich nog in een relatief pril stadium[138]; met de cyberbeveiligingsverordening wordt getracht hier iets aan te doen door de coördinerende rol van Enisa te versterken. De wens om de samenwerking te intensiveren was de beweegreden achter het memorandum van overeenstemming dat in 2018 werd ondertekend tussen Enisa, EDA, EC3 van Europol en CERT-EU[139]. De komende jaren zal het voor de Commissie een prioriteit zijn om passende afstemming te garanderen tussen beleidsinitiatieven, behoeften en investeringsprogramma's teneinde de fragmentatie weg te nemen en synergieën te smeden[140].

94 De coördinatiefuncties zijn geïntegreerd in verschillende institutionele organen. De taskforce Veiligheidsunie werd opgericht om een centrale rol te spelen in de coördinatie van de verschillende directoraten-generaal van de Commissie ter ondersteuning van de agenda van de Veiligheidsunie[141]. DG CNECT zit de subwerkgroep voor cyberbeveiliging van de taskforce voor.

95 Binnen de Raad wordt cyberbeveiliging behandeld door de Horizontale groep cybervraagstukken (HWP), die strategische en horizontale cybervraagstukken

coördineert en helpt met de voorbereiding van oefeningen en de evaluatie van de resultaten ervan. De groep werkt nauw samen met het Politiek en Veiligheidscomité dat een centrale rol speelt in de besluitvorming met betrekking tot cybergerelateerde diplomatieke maatregelen (zie ***tekstvak 6*** in het volgende hoofdstuk). Aangezien cyberbeveiliging een interdisciplinair onderwerp is, is het niet eenvoudig om alle relevante belangen te coördineren; recentelijk hebben maar liefst 24 werkgroepen en voorbereidende organen zich beziggehouden met cyberkwesties[142].

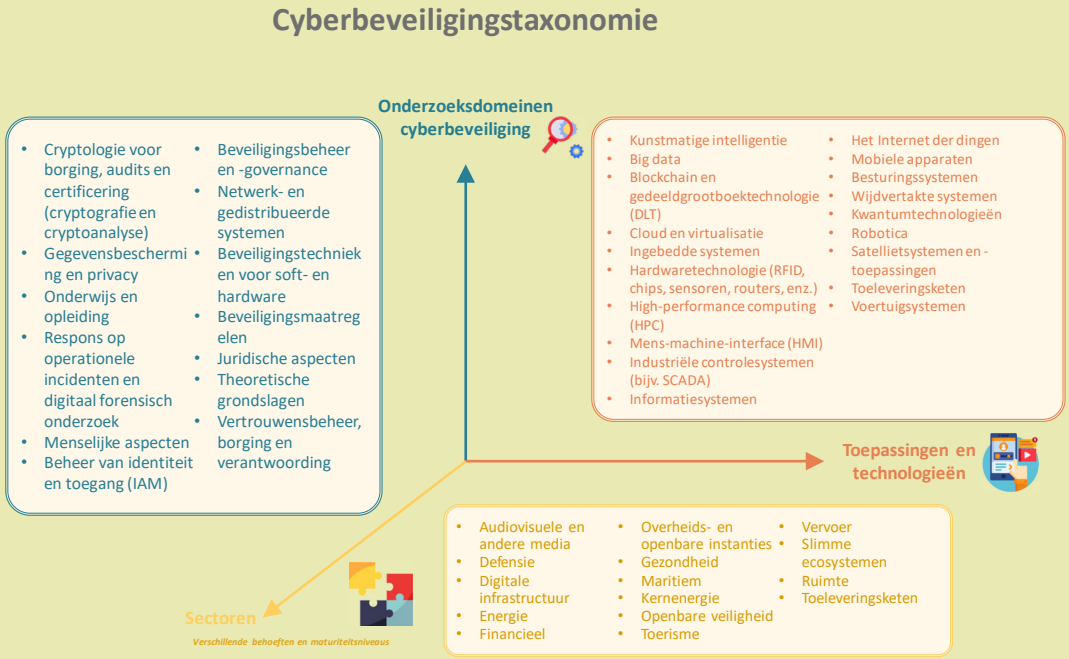
96 De twee meest recente wetgevingsvoorstellen inzake de versterking van Enisa (2017) en voor de oprichting van een netwerk van kenniscentra voor cyberbeveiliging en een kenniscentrum voor onderzoek (2018) zijn specifiek ontworpen om iets te doen aan de fragmentatie en duplicatie van inspanningen. Een drijvende kracht achter het netwerk van kenniscentra voor cyberbeveiliging en een kenniscentrum voor onderzoek was de behoefte om de kloof te dichten die met de coöperatieve structuren van de NIS-richtlijn niet kan worden gedicht omdat deze structuren niet zijn ontworpen om de ontwikkeling van geavanceerde oplossingen te ondersteunen.

Tekstvak 5

Trachten dezelfde cybertaal te spreken: *technologische samenhang*

Duidelijkheid omtrent terminologie verbetert het situationele bewustzijn en de coördinatie[143] en helpt te bepalen wat precies een dreiging of een risico vormt.

Het Gemeenschappelijk Centrum voor Onderzoek van de Commissie (JRC) heeft een herziene onderzoekstaxonomie ontwikkeld op basis van verschillende internationale normen[144]. De bedoeling is dat dit een referentiepunt wordt dat kan worden gebruikt als index door onderzoeksinstanties in heel Europa.



Bron: Door de ERK aangepaste gegevens van de Europese Commissie.

Tot voor kort hadden de instellingen en agentschappen van de EU geen gemeenschappelijke definities. Daar komt momenteel verandering in. In het kader van zijn blauwdruk heeft de Samenwerkingsgroep een taxonomie voor incidenten ontwikkeld om een efficiënte grensoverschrijdende samenwerking mogelijk te maken.

Samenwerking en informatie-uitwisseling met de particuliere sector

97 Samenwerking tussen overheidsinstanties en de particuliere sector is essentieel om de algehele niveaus van cyberbeveiliging te verhogen. Desondanks concludeerde de Commissie in haar beoordeling van de Strategie inzake cyberbeveiliging uit 2017 dat de informatie-uitwisseling tussen particuliere belanghebbenden en tussen de publieke en particuliere sector nog niet optimaal was als gevolg van het ontbreken van betrouwbare verslagleggingsmechanismen en prikkels om informatie te delen[145], hetgeen de verwezenlijking van strategische doelstellingen in de weg staat. De Commissie heeft ook opgemerkt dat er geen efficiënt samenwerkingsmechanisme bestaat dat lidstaten kunnen gebruiken om samen te werken teneinde duurzame industriële capaciteiten op grote schaal naar een hoger niveau te tillen[146].

98 Centra voor de uitwisseling en analyse van informatie (ISAC's) zijn organisaties die zijn opgezet om platforms en middelen te verschaffen om de informatie-uitwisseling

tussen de publieke en particuliere sector te faciliteren en informatie te verzamelen over cyberdreigingen. Ze beogen vertrouwen te creëren door het delen van ervaringen, kennis en analyses, met name over onderliggende oorzaken, incidenten en dreigingen. In veel lidstaten bestaan al ISAC's, maar op Europees niveau komen ze nog steeds relatief weinig voor[147]. Deze centra worden echter met meerdere uitdagingen geconfronteerd (beperkte middelen, problemen met het evalueren van hun succes, het garanderen van de juiste structuren om spelers uit zowel de publieke als de particuliere sector te betrekken, het betrekken van wetshandhavingsinstanties) die zij het hoofd moeten bieden om te kunnen bijdragen aan de tenuitvoerlegging van de NIS-richtlijn en de ontwikkeling van beveiligingscapaciteiten in heel Europa[148].

99 Nauwe samenwerking met de particuliere sector is met name cruciaal om complexe cybercriminaliteit te bestrijden, maar de doelmatigheid van deze samenwerking varieert in de verschillende lidstaten en hangt af van het niveau van vertrouwen[149]. Het EC3 van Europol heeft echter een reeks adviesgroepen opgericht met marktpartijen uit de particuliere sector, instellingen en organen van de EU en andere internationale organisaties om de samenwerking te verbeteren door middel van netwerkvorming, het delen van strategische inlichtingen en samenwerking. Deze groepen werken op basis van plannen die zijn afgestemd op de doelen van de EU-beleidscyclus[150]. Het misbruik door criminelen van versleuteling is een ander gebied vol uitdagingen waarop meer moet worden samengewerkt met de particuliere sector. EC3 van Europol analyseert momenteel opties om als gastheer te fungeren voor uitbreidingen op korte termijn van de J-CAT voor specifieke zaken (zie paragraaf ***62***) voor deskundigen uit de particuliere sector en academici.

100 Een gebrek aan efficiënte samenwerkingsmechanismen is een probleem voor civiele en defensiegemeenschappen, zowel publiek als privaat. Gebieden die steeds een uitdaging vormen, zijn onder meer cryptografie, beveiligde ingebedde systemen, malware-detectie, simulatietechnieken, technologieën voor de bescherming van de communicatie via netwerken en systemen en technologieën voor authenticatie. Het bevorderen van civiel-militaire samenwerking en het ondersteunen van onderzoek en technologie (in het bijzonder door kmo's te ondersteunen) zijn de twee prioriteiten in het geactualiseerde beleidskader voor cyberdefensie (update 2018).

Aandachtspunten — de weerbaarheid vergroten

- Hoe kan een passend evenwicht worden bereikt op EU-niveau tussen de behoefte om het beleid inzake cyberbeveiliging te mainstreamen en een efficiënte coördinatie tussen de verschillende spelers te garanderen en de verspreiding van verantwoordelijkheden?
- Hoe goed zijn de instellingen en agentschappen van de Unie voorbereid op de volgende grote, rechtstreeks op hen gerichte aanval?
- Hoe kunnen EU-agentschappen voor cyberkwesties meer talent aantrekken?
- Welke verdere stappen moeten worden genomen om adequate capaciteit te garanderen in de verschillende EU-instellingen en -agentschappen teneinde een samenhangend kader voor risico- en dreigingsanalyse mogelijk te maken?
- Hoe gaan de Europese toezichthoudende autoriteiten (de Europese Bankautoriteit, de Europese Autoriteit voor effecten en markten en de Europese Autoriteit voor verzekeringen en bedrijfspensioenen) om met zwakke plekken op het gebied van cyberbeveiliging in de financiële sector en wat kunnen andere sectoren hiervan in dit opzicht leren?
- Hoe kan de technische bijstand van de EU voor overheidsinstanties, met het oog op het algehele tekort aan expertise, het best worden gebruikt om de algehele cyberweerbaarheid te optimaliseren?
- Hoe kunnen de EU en de lidstaten een rol van betekenis spelen in internationale discussies, teneinde cyberspace-governance en -normen vorm te geven en de EU-waarden te bevorderen?
- Welke maatregelen om het bewustzijn te vergroten op EU- en lidstaatniveau (met inbegrip van preventieve inspanningen) maken echt een verschil en wat kan de EU doen om deze op te schalen?
- Welke rol kan de EU spelen om de genderdiversiteit in de wereld van cyberbeveiliging te vergroten?
- Hoe kunnen de EU en de lidstaten de synergieën vergroten tussen de civiele en defensiegemeenschappen, in overeenstemming met het beleidskader voor cyberdefensie (update 2018)?

Doeltreffend reageren op cyberincidenten

101 Het ontwikkelen van een doeltreffende reactie op cyberaanvallen is van fundamenteel belang om deze in een zo vroeg mogelijk stadium te kunnen stopzetten. Het is met name belangrijk dat kritieke sectoren, lidstaten en EU-instellingen snel en gecoördineerd kunnen reageren. Vroegtijdige detectie is hierbij essentieel.

Uitdaging 9: doeltreffende detectie en respons

Detectie en melding

102 Gewone detectie-instrumenten helpen dagelijks de overgrote meerderheid van de aanvallen voorkomen[151]. Digitale systemen zijn echter zo complex geworden dat het voorkomen van alle aanvallen inmiddels onmogelijk is geworden. Geavanceerde aanvallen zullen vaak gedurende lange tijd onopgemerkt blijven. Deskundigen zeggen daarom dat de nadruk moet liggen op snelle detectie en verdediging[152]. Sommige detectie-instrumenten, zoals automatisering, machinaal leren en gedragsstatistieken, met als doel het risico terug te dringen en systeemgedrag te analyseren en ervan te leren, worden weinig gebruikt door bedrijven[153]. Dit komt deels doordat deze systemen veel vertekend positieve resultaten geven, wat betekent dat activiteiten die in werkelijkheid geen dreiging vormen, ten onrechte worden aangemerkt als malafide.

103 Zodra een inbreuk is gedetecteerd en geanalyseerd, moet deze snel worden gemeld en gerapporteerd zodat andere publieke en particuliere entiteiten preventieve maatregelen kunnen nemen en de relevante autoriteiten de getroffenen ondersteuning kunnen bieden. Veel organisaties erkennen liever niet dat er cyberincidenten hebben plaatsgevonden en melden deze liever niet[154]. De vroegtijdige betrokkenheid van wetshandhavingsinstanties bij de eerste reactie op vermoedelijke cybermisdaden en een proactieve informatie-uitwisseling met CSIRT's zijn ook essentieel.

104 Door het eerdere gebrek aan gemeenschappelijke EU-vereisten met betrekking tot het melden van incidenten ontstond het risico op vertraging van de communicatie over inbreuken, hetgeen de respons bemoeilijkte. Met de invoering van de NIS-richtlijn werd beoogd hier iets aan te doen (zie paragraaf ***20***). Naar aanleiding van de Wannacry-aanvallen uit 2017 concludeerde de Commissie dat het CSIRT-

netwerksysteem nog niet volledig operationeel was[155]. Naarmate de richtlijn verder ten uitvoer wordt gelegd, zal moeten blijken of de door de Samenwerkingsgroep ontwikkelde richtsnoeren de terughoudendheid om incidenten te melden zal verminderen[156].

105 Aanbieders van essentiële diensten in bepaalde sectoren hebben uit hoofde van de bestaande EU-verordeningen meerdere meldingsplichten (onder meer naar consumenten toe), hetgeen afbreuk kan doen aan de efficiëntie van het proces. Zo gelden voor marktdeelnemers in de financiële sector en het bankwezen op grond van de AVG, de NIS-richtlijn, de richtlijn betalingsdiensten, ECB/GTM, Target 2 en de eIDAS-verordening verschillende criteria, normen, drempels en termijnen voor melding[157]. Het is daarom belangrijk om deze verplichtingen te stroomlijnen, aangezien een dergelijke heterogeniteit niet alleen onnodige administratieve lasten met zich meebrengt, maar ook kan leiden tot gefragmenteerde verslaglegging.

Gecoördineerde respons

106 Aan de ontwikkeling van een Europees samenwerkingskader voor cyberbeveiligingscrises wordt nog steeds gewerkt. De verwante "blauwdruk"[158] (zie paragraaf ***18***) werd daarom ingevoerd om een cyberperspectief toe te voegen aan de geïntegreerde regeling politieke crisisrespons (IPCR) om het situationele bewustzijn te vergroten en om een betere integratie met andere EU-mechanismen voor crisisbeheer te waarborgen[159]. Bij deze blauwdruk zijn EU-instellingen, agentschappen en lidstaten betrokken. Het is een uitdaging om al deze mechanismen voor crisisrespons naadloos te integreren[160]. Het feit dat er momenteel geen gezamenlijk beveiligd netwerk voor communicatie tussen de instellingen van de EU bestaat, is ook een belangrijke tekortkoming[161].

107 Het vermogen van de EU om in het geval van een grootschalige, grensoverschrijdende cyberaanval op operationeel en politiek niveau te reageren, is aangemerkt als "beperkt", deels omdat cyberbeveiliging nog niet is geïntegreerd in de bestaande coördinatiemechanismen voor crisisbestrijding op EU-niveau[162]. In de NIS-richtlijn werd hieraan geen aandacht besteed.

108 De onlangs voorgestelde hervorming van Enisa, waarbij een grotere operationele rol voor het agentschap werd beoogd bij grootschalige cyberbeveiligingsincidenten, werd door de lidstaten niet gesteund. Zij gaven er de voorkeur aan dat het agentschap hun eigen operationele acties ondersteunt en aanvult[163]. Er zijn al veel CERT's/CSIRT's op lidstaatniveau, maar hun capaciteiten

variëren aanzienlijk. Dit vormt een obstakel voor de doeltreffende grensoverschrijdende samenwerking die nodig is in reactie op grootschalige incidenten[164].

109 We hebben geprobeerd de verschillende rollen in kaart te brengen die zijn toegewezen aan de verschillende spelers die in de blauwdruk worden genoemd, maar er zijn lacunes die moeten worden ingevuld naarmate de tenuitvoerlegging vordert. Een gebied waaraan in eerste instantie te weinig aandacht werd besteed, was wetshandhaving, ondanks het feit dat het EU-wetshandhavingsprotocol voor respons in noodsituaties in december 2018 in werking trad[165]. Garanderen dat de blauwdruk praktisch toepasbaar is en dat alle partijen weten wat ze moeten doen, is cruciaal voor het slagen ervan. Dit moet de komende jaren dan ook uitgebreid worden getest.

110 Een doeltreffende respons betekent meer dan alleen het beperken van de schade. Ook het toeschrijven van de verantwoordelijkheid voor de aanvallen is van groot belang. Het volgen en vaststellen van de identiteit van de daders kan, met name bij hybride aanvallen, moeilijk zijn omdat er steeds meer tools voor anonimisering, cryptovaluta en versleutelingstechnologieën kunnen worden misbruikt. Dit wordt het probleem van attributie genoemd. Het is niet alleen een technische, maar ook een strafrechtelijke uitdaging om dit probleem op te lossen. De juridische en procedurele verschillen tussen landen kunnen strafrechtelijke onderzoeken en de vervolging van verdachten in de weg staan. Om het probleem van attributie op te lossen, is een formelere operationele uitwisseling van informatie nodig op basis van duidelijker procedures, bijvoorbeeld met Europol of het Europees justitieel netwerk cybercriminaliteit van Eurojust.

111 Op politiek niveau is het instrumentarium voor cyberdiplomatie (zie ***tekstvak 6***) ontwikkeld ter bevordering van de vreedzame beslechting van internationale disputen in cyberspace. Het opzetten van snellereactieteams bij cyberincidenten en een initiatief voor wederzijdse bijstand op het gebied van cyberbeveiliging zijn twee projecten die een betere informatie-uitwisseling bevorderen en momenteel worden ontwikkeld binnen het Pesco-kader[166].

Tekstvak 6

Het instrumentarium voor cyberdiplomatie

De gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten[167], of het “instrumentarium voor cyberdiplomatie”, kwam voort uit de conclusies van de Raad over cyberdiplomatie uit 2015[168]. Met cyberdiplomatie wordt beoogd een gemeenschappelijke en alomvattende benadering voor de cyberspace te

ontwikkelen en ten uitvoer te leggen die is gebaseerd op de EU-waarden, de rechtsstaat, capaciteitsopbouw en partnerschappen, de bevordering van het multistakeholdermodel voor internetgovernance en de terugdringing van cyberbeveiligingsdreigingen en meer stabiliteit in de internationale betrekkingen.

Het instrumentarium stelt de EU en haar lidstaten in staat een gezamenlijke diplomatieke respons te ontwikkelen op kwaadwillige cyberactiviteiten door volledig gebruik te maken van de maatregelen in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid. Het kan hierbij gaan om preventieve maatregelen (zoals het kweken van bewustzijn, capaciteitsopbouw), coöperatieve, stabiliteits- en beperkende maatregelen (bijv. reisverboden, wapenembargo's, het bevriezen van tegoeden) of ondersteuning van de respons van lidstaten[169]. Het idee hierachter is dat verdere samenwerking om de dreiging te verminderen en om een duidelijk signaal af te geven over de mogelijke consequenties van een gezamenlijke respons, (potentieel) agressief gedrag zal ontmoedigen.

Een gezamenlijke EU-respons op kwaadwillige cyberactiviteiten zou in verhouding staan tot de reikwijdte, de omvang, de duur, de intensiteit, de complexiteit, de verfijning en de impact van de cyberactiviteit.

Het succes van het instrumentarium zal afhangen van de mate waarin het is verweven met de blauwdruk en de IPCR (zie paragraaf ***106***), de mate van situationele bewustmaking door middel van een snelle en constante informatie-uitwisseling (onder meer over elementen van attributie)[170] en, ten slotte, van een doeltreffende samenwerking. Bovendien is doeltreffende en gecoördineerde communicatie cruciaal voor een succesvolle toepassing van het instrumentarium. Tot nu toe is het instrumentarium twee keer gebruikt: om een dialoog aan te gaan met de Verenigde Staten na de *Wannacry*-aanval[171] en om conclusies van de Raad op te stellen om het kwaadwillige gebruik van ICT te veroordelen[172]. Het instrumentarium wordt nog geoperationaliseerd; het zal moeten blijken hoe doeltreffend het zal zijn in het realiseren van de nagestreefde doelstellingen.

Uitdaging 10: bescherming van kritieke infrastructuur en maatschappelijke functies

Bescherming van infrastructuur

112 Veel van de kritieke infrastructuur van de EU wordt beheerd via industriële controlesystemen (ICS)[173]. Veel van deze systemen zijn ontworpen als losstaande systemen, met een beperkte connectiviteit met de buitenwereld. Aangezien componenten van de ICS zijn verbonden met het internet, zijn deze kwetsbaarder

geworden voor verstoring van buitenaf. Het onderhouden en patchen van bestaande systemen zal mogelijk niet langer haalbaar zijn, maar het kost tijd en geld om ze te upgraden. Daarom moet het upgraden van ICS deel uitmaken van de inspanningen om de beveiliging van kritieke infrastructuur te verbeteren.

113 Nu het bedrijfsleven steeds verder digitaliseert (deze tendens wordt vaak "Industry 4.0" genoemd), kan een grootschalig incident in één sector elders ingrijpende consequenties hebben. Enisa heeft erop gewezen hoe belangrijk het is om de impact van kritieke sectoren en hun onderlinge afhankelijkheid in kaart te brengen[174]. Dit is van essentieel belang om de potentiële verspreiding van een incident te begrijpen en moet aan de basis liggen van een goed gecoördineerde respons.

114 Met de NIS-richtlijn wordt beoogd de paraatheid in de sectoren met veel kritieke infrastructuur te vergroten. Niet alle sectoren vallen hier echter onder (zie ***tabel 1***)[175], hetgeen de doeltreffendheid van de strategie vermindert[176]. In dit opzicht is het bijvoorbeeld bijzonder belangrijk om de democratische integriteit van verkiezingen te beschermen en interferentie in de infrastructuur voor verkiezingen en desinformatie te voorkomen (zie ***tekstvak 7***). De bestaande wetgeving moet niet alleen worden herzien, maar het is ook van groot belang om deze sectoren te betrekken bij een doeltreffende respons op grootschalige incidenten.

115 Zwakke plekken in de kritieke infrastructuur houden niet op bij de Europese grenzen. Het is voor de Commissie een grote uitdaging om kandidaat-lidstaten aan te moedigen dezelfde normen aan te nemen als de lidstaten, bijvoorbeeld op gebieden als cyberwetgeving en de bescherming van kritieke infrastructuur.

Tekstvak 7

Bescherming van kritieke maatschappelijke functies: *het bestrijden van inmenging in verkiezingen*

In mei 2019 zullen ongeveer 400 miljoen kiezers naar de stembus gaan voor de verkiezingen van het Europees Parlement. Het zijn de eerste verkiezingen die plaatsvinden sinds de inwerkingtreding van de AVG. De verkiezingen vinden plaats in de nasleep van de schandalen rondom het misbruik van persoonsgegevens voor politieke micro-targeting en de ongekende, goed gecoördineerde desinformatiecampagnes ("fake news"). De Commissie heeft gewaarschuwd voor de grote kans op cyberinterferentie in deze verkiezingen[177]; om dit te bestrijden is een aanpak nodig waarbij de hele overheid en de hele maatschappij worden betrokken.

Verkiezingsinfrastructuur

De organisatie van verkiezingen is complex en het is de verantwoordelijkheid van de lidstaten om de bescherming en integriteit ervan te waarborgen. Met inmenging in verkiezingen en electorale infrastructuur kan worden getracht de voorkeuren van stemmers, de opkomst of het verkiezingsproces zelf — waaronder de eigenlijke stemming, de stemtabellering en de communicatie — te beïnvloeden. Bij de verkiezingen voor het Europees Parlement vormt de zogenoemde "laatste mijl" (de communicatie van de resultaten van de nationale hoofdsteden aan Brussel) een bijzonder kritieke uitdaging, aangezien hiervoor geen gemeenschappelijke beveiligingsbenadering bestaat of is getest[178].

In het recente verkiezingspakket van de Commissie zijn maatregelen opgenomen om de cyberbeveiliging van de verkiezingen te versterken, onder meer door de aanwijzing van nationale contactpunten die in de aanloop naar de verkiezingen informatie zullen coördineren en uitwisselen. Met name het delen van beste praktijken en geleerde lessen is belangrijk[179].

Verkiezingssystemen worden niet beschouwd als onderdeel van de kritieke infrastructuur[180] en vallen ook niet onder de NIS-richtlijn. Desondanks heeft de Samenwerkingsgroep praktische richtsnoeren ontwikkeld over technologieën die kunnen worden gebruikt om de verkiezingen te beveiligen, teneinde overheidsinstanties hierbij te helpen. Naar verwachting zullen de nationale contactpunten begin 2019 bijeenkomen[181]. De lidstaten worden aangemoedigd risicobeoordelingen uit te voeren om de cyberdreigingen voor hun verkiezingsprocessen te evalueren.

Desinformatie

Desinformatie is een onderdeel van hybride aanvallen dat steeds belangrijker wordt en betrekking heeft op cyberaanvallen en het hacken van netwerken. Het kan worden gebruikt om samenlevingen te polariseren, een klimaat van wantrouwen te scheppen en het vertrouwen in het democratische proces of andere kwesties (bijvoorbeeld antivaccinatie of klimaatverandering) te ondermijnen. Desinformatie is grootschaliger geworden en verspreidt zich sneller en verder dan ooit, en vormt derhalve een echte beveiligingsdreiging voor de EU.

De EU heeft een aantal maatregelen genomen om desinformatie te bestrijden. Zo werd in 2015 de East StratCom Task Force opgericht binnen de EDEO om de Russische desinformatiecampagnes onderuit te halen[182]. Deskundigen zijn zeer lovend over de werkzaamheden van deze taskforce op het gebied van het bevorderen van het EU-beleid, het ondersteunen van onafhankelijke media in het nabuurschap en het voorspellen, volgen en aanpakken van desinformatie[183]. De taskforce beschikt echter over beperkte middelen gezien de schaal en complexiteit van de desinformatiecampagnes[184]. Er is een meer systematische interactie met bestaande EU-structuren en verbeterde samenwerking op het gebied van

strategische communicatie nodig[185]. In december 2018 heeft de Europese Raad zich achter een nieuw actieplan[186] geschaard.

Meer recentelijk heeft de Commissie, naar aanleiding van haar mededeling over de bestrijding van desinformatie uit april 2018[187], een vrijwillige praktijkcode voor zelfregulering ontwikkeld[188] die is gebaseerd op bestaande beleidsinstrumenten en waar onlineplatforms en de reclamesector zich bij hebben aangesloten[189]. De code omvat onder meer acties om de betrouwbaarheid van inhoud te vergroten en inspanningen om de media- en nieuwsgeletterdheid te ondersteunen. Ook is er een onafhankelijk Europees netwerk van factcheckers opgericht.

De Commissie heeft aangegeven dat er mogelijk aanvullende regelgevende maatregelen zullen volgen indien de praktijkcode niet wordt nageleefd. Het blijft cruciaal om de doeltreffendheid van maatregelen te bepalen en, met name, om te beslissen hoe verbeteringen in het vertrouwen, de transparantie en de verantwoording kunnen worden gemeten.

Het zal ook een uitdaging zijn om manieren te vinden om desinformatie beter op te sporen, te analyseren en aan de kaak te stellen[190]. Daarnaast moeten open gegevensbronnen op actieve en strategische wijze worden gemonitord en geanalyseerd[191]. Bij pogingen om een beter inzicht te verwerven in het dreigingsklimaat moet ook aandacht worden besteed aan nieuwe trends, zoals “deepfakes” (nepvideo’s die worden gemaakt met behulp van kunstmatige intelligentie en “diep” machinaal leren), evenals aan de tools die nodig zijn om ze te detecteren.

De autonomie vergroten

116 De EU is een netto-importeur van producten en diensten voor cyberbeveiliging, hetgeen het risico van technologische afhankelijkheid van niet-EU-spelers en haar kwetsbaarheid vergroot[192]. Dit is in het bijzonder ongunstig voor de beveiliging van de kritieke infrastructuur van de EU en wordt tevens mogelijk gemaakt door complexe wereldwijde toeleveringsketens. Het risico neemt nog verder toe wanneer niet-EU-spelers Europese cyberbeveiligingsondernemingen overnemen. Lidstaten zijn verantwoordelijk voor het screenen van buitenlandse directe investeringen (BDI) en er is momenteel geen EU-breed screeningmechanisme[193].

117 Grotere strategische autonomie is een doelstelling van de integrale EU-strategie en de mededeling uit 2017 getiteld *Weerbaarheid, afschrikking en defensie*[194] De aanpak van de verschillende uitdagingen die in dit verslag worden aangekaart, zal de gewenste autonomie vergroten. Dit zal met geen enkele afzonderlijke maatregel kunnen worden bereikt.

Aandachtspunten — doeltreffende respons

- In hoeverre heeft de NIS-richtlijn ervoor gezorgd dat cyberincidenten binnen en buiten de kritieke sectoren vaker worden gemeld?
- Hoe goed internaliseren de EU-instellingen crisisresponscoördinatie voor een groot cyberincident?
- Hoe kan cyberdiplomatie een prominentere rol spelen in het externe optreden van de EU?
- Staan de bestaande EU-structuren en -acties om desinformatie te bestrijden in verhouding tot de schaal en complexiteit van het probleem?

Slotopmerkingen

118 De afgelopen jaren hebben de EU en haar lidstaten cyberbeveiliging hoger op de agenda gezet teneinde de algehele cyberweerbaarheid te vergroten. Het blijft echter een gigantische onderneming om een hoger niveau van cyberbeveiliging tot stand te brengen in de Unie. In dit briefingdocument hebben we geprobeerd een aantal van de grootste uitdagingen te bespreken met betrekking tot de ambitie van de EU om de veiligste digitale omgeving ter wereld te worden.

119 Uit onze evaluatie blijkt dat een verschuiving naar een prestatiecultuur met geïntegreerde evaluatiepraktijken nodig is om zinvolle **verantwoording en evaluatie** te garanderen. **Er blijven** bepaalde **tekortkomingen in de wetgeving bestaan en de bestaande wetgeving is bovendien niet consistent omgezet door de lidstaten.** Dit kan een optimale benutting van het potentieel van de wetgeving belemmeren. Een andere uitdaging die is vastgesteld, heeft betrekking op het **afstemmen van de investeringsniveaus op de strategische doelstellingen**, waarvoor de investeringen en de impact ervan moeten worden opgeschaald. Dit vereist meer inspanningen wanneer de EU en haar lidstaten geen **duidelijk overzicht hebben van wat de EU uitgeeft** aan cyberbeveiliging. Het is ook bekend dat **de middelen voor de EU-agentschappen voor cyberkwesties niet toereikend zijn,** en dat deze agentschappen onder meer moeite hebben om talent aan te trekken en vast te houden.

120 In de beschikbare studies wordt geconcludeerd dat **de cyberbeveiligingsgovernance moet worden verbeterd** teneinde het vermogen van de internationale gemeenschap om te reageren op cyberaanvallen en -incidenten te vergroten. Toch is het onmogelijk alle aanvallen te voorkomen. Daarom moet aandacht worden besteed aan de volgende belangrijke uitdagingen: **snelle detectie enreactie** en de **bescherming van kritieke infrastructuur en maatschappelijke functies**, evenals **een betere uitwisseling van informatie en coördinatie** tussen de publieke en particuliere sector. Ten slotte betekent het toenemende wereldwijde tekort aan cyberbeveiligingsvaardigheden dat **het vergroten van de vaardigheden en het bewustzijn** in alle sectoren en op alle niveaus binnen de samenleving ook een vitale uitdaging vormt.

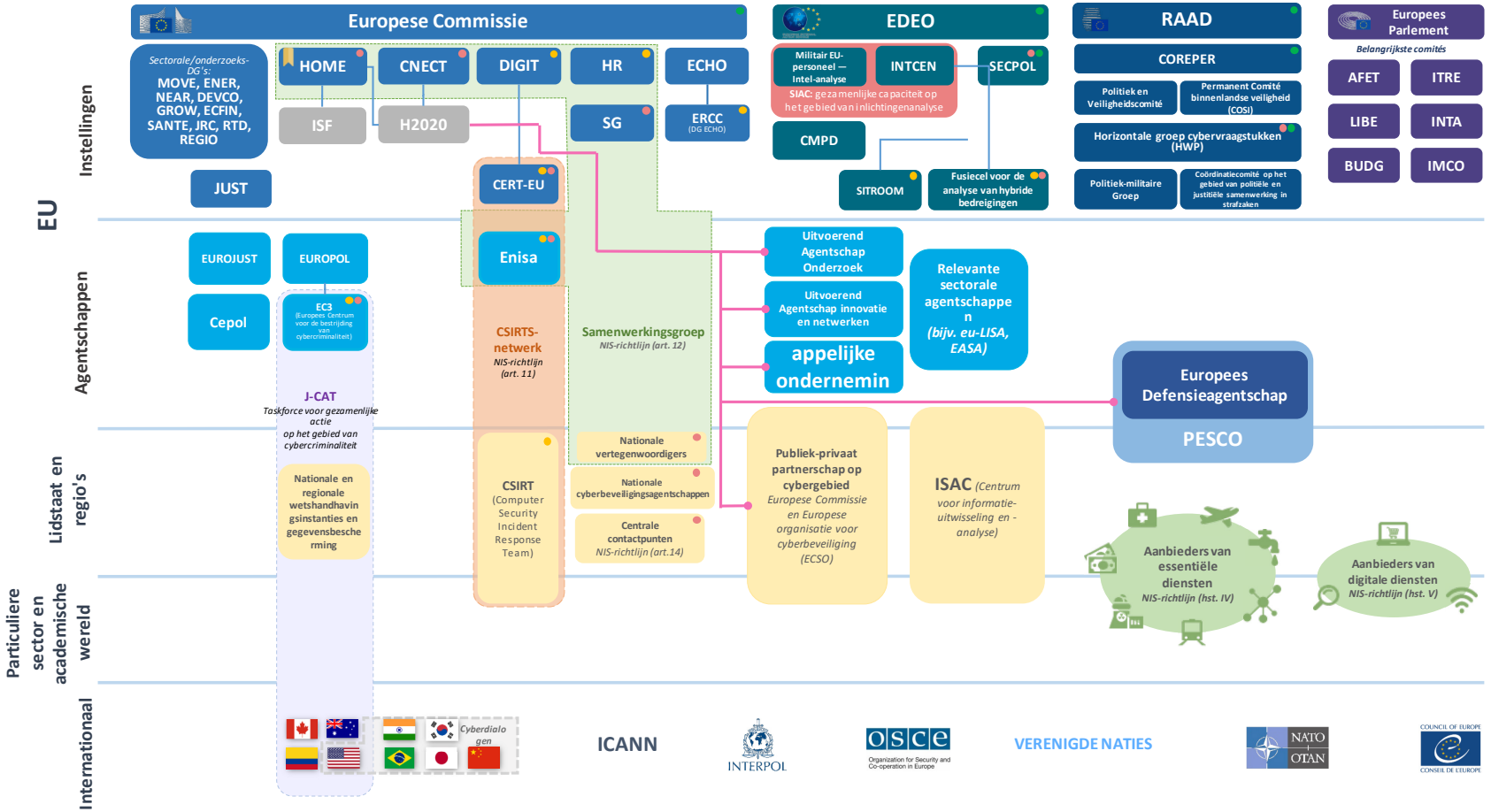
121 Deze uitdagingen met betrekking tot cyberdreigingen waarmee de EU en de rest van de wereld worden geconfronteerd, vereisen constante inspanningen en een voortdurende, consequente naleving van de waarden van de EU.

Dit briefingdocument werd door kamer III vastgesteld op haar vergadering van 14 februari 2019.

Voor de Rekenkamer

Klaus-Heiner Lehne
President

Bijlage I — Een complex meerlagig landschap en vele spelers



Niveaus van samenwerking voor de EU-***blauwdruk*** voor grootschalige cyberbeveiligingsincidenten uit 2017, om tot een gecoördineerde respons te komen; gedeeld situationeel bewustzijn en openbare mededelingen

- Technisch
- Operationeel
- Politiek

Respons op incidenten tijdens een crisis; incidenten monitoren en bewaken, met inbegrip van constante dreigings- en risicoanalyse

Besluitvorming op politiek niveau voorbereiden; beheer van cyberbeveiligingscrisis coördineren; consequenties en impact op EU-niveau beoordelen

Strategisch en politiek beheer van zowel cyber- als niet-cybergerelateerde aspecten van de crisis, met inbegrip van maatregelen uit hoofde van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("EU-instrumentarium voor cyberdiplomatie")

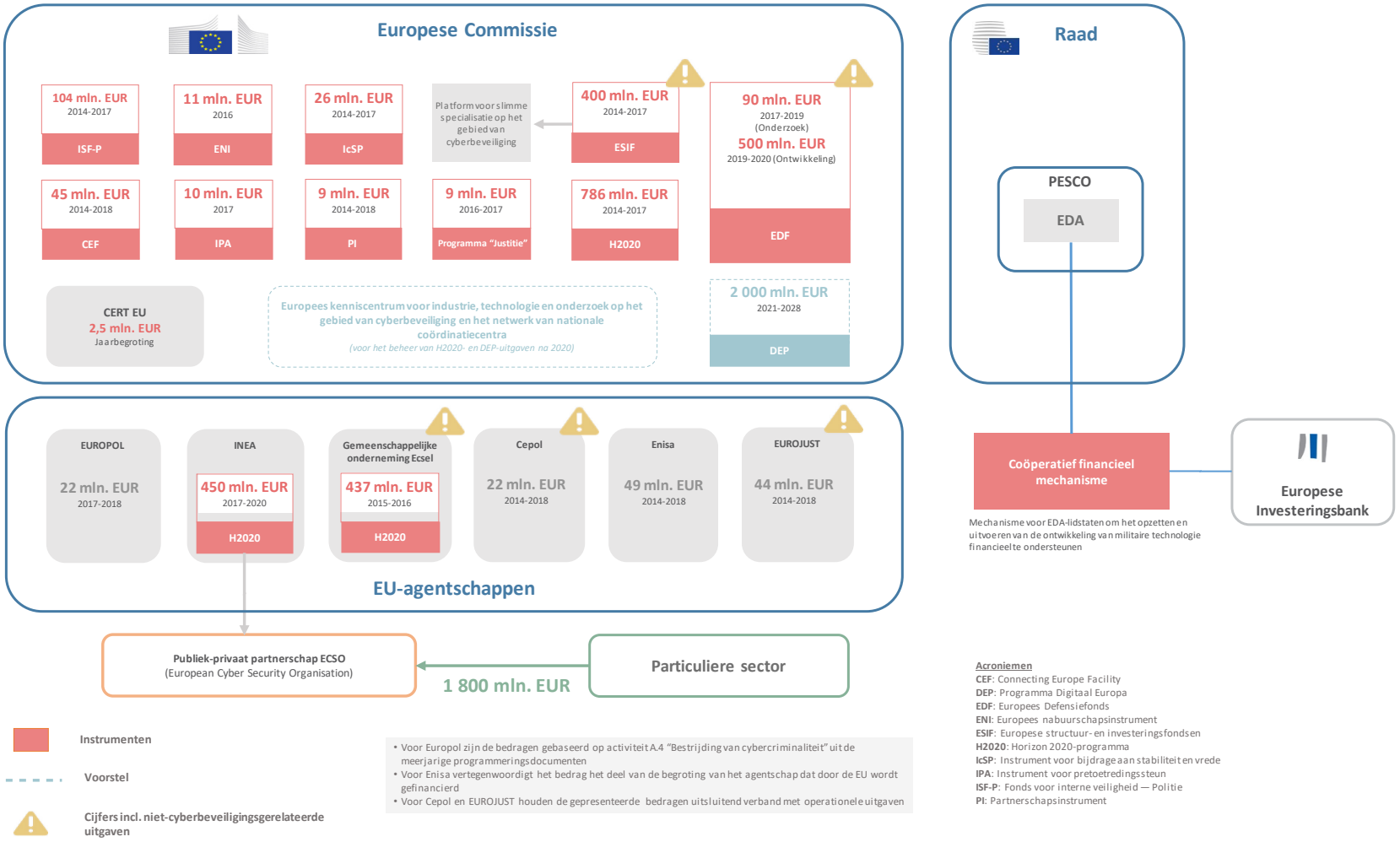
Primaire uitgavenstromen voor het H2020-programma

Het secretariaat van de taskforce Veiligheidsunie is bij DG HOME gevestigd

NB: De interinstitutionele overeenkomst CERT-EU heeft betrekking op 11 EU-instellingen en -organen en 37 EU-agentschappen

Bron: ERK.

Bijlage II — EU-uitgaven voor cyberbeveiliging sinds 2014



Bron: ERK, op basis van gegevens van de Europese Commissie en documenten van EU-agentschappen.

Bijlage III — Verslagen van de rekenkamers van de EU-lidstaten

Type	Titel (met hyperlink)	Jaar	LS
Nalevingsgerichte controles	Beoordelingsnota interne controle	2014	FR
	Certificeringsverslag voor de rekeningen van het algemene socialezekerheidsstelsel (defensie, buitenlandse zaken)	2016	FR
	Certificering van de staatsrekeningen	2016	FR
	Waarborgen van de beveiliging en instandhouding van de Estse nationale databanken die van kritiek belang zijn	Fin. 2018/nog niet gepubliceerd	EE
	Effectiveness of internal controls in the protection of personal data in national databases	2008	EE
Doelmatigheidscontroles/controles van de kosteneffectiviteit	Verslag over de beperking van cyberaanvallen	2013	DK
	RiR 2014:23 Information security in the civil public administration	2014	SE
	Verslag over de verwerking van vertrouwelijke gegevens over personen en bedrijven door de overheid	2014	DK
	Het nationale programma voor cyberbeveiliging	2014	VK
	Verslag voor de begrotingscommissie van de Duitse Bondsdag uit hoofde van § 88, lid 2, van de Federale begrotingswet (BHO) — IT-consolidatie, federale overheid	2015	DE
	Verslag over de toegang tot IT-systemen die de verlening van essentiële diensten aan de Deense samenleving ondersteunen	2015	DK
	Autoriteit voor overheidsplanning Plaine de France	2015	FR
	Het cyberbeveiligingsklimaat in Litouwen een versie in het Litouws een naar het Engels vertaalde samenvatting	2015	LT
	Prestaties van de Poolse overheidsinstanties met betrekking tot cyberbeveiligingstaken (in PL)	2015	PL
	RiR 2015:21 Cybercrime — police and prosecutors can be more efficient.	2015	SE
	Digital Skills Gap in Government (Survey)	2015	VK
	Verslag aan het federale Parlement: FOD financiën: inning van successierechten	2016	BE
	Verslag over het beheer van IT-beveiliging in systemen die worden uitbesteed aan externe leveranciers	2016	DK
	Controleverslag over de leenactiviteiten van de officiële kredietinstelling 2016	2016	ES
	Steering of the Government Security Network	2016	FI
	De beveiliging garanderen van IT-systemen die worden gebruikt voor politieke taken	2016	PL

Type	Titel (met hyperlink)	Jaar	LS
	Preventie en bestrijding van cyberpesten onder kinderen en jongeren	2016	PL
	Information security work at nine agencies — Nog een controle van informatiebeveiliging bij de overheid. RiR 2016:8	2016	SE
	Protecting Information across government	2016	VK
	Verslag over de bescherming van IT-systemen en gezondheidsgerelateerde gegevens in drie Deense regio's	2017	DK
	Nota over de resultaten van de internationale parallelle controle met betrekking tot de doeltreffendheid van interne controles voor de bescherming van persoonsgegevens in nationale databanken	2017	EE
	Cyber protection arrangements	2017	FI
	Steering of the operational reliability of electronic services	2017	FI
	Netwerk van landbouwkamers (synthese)	2017	FR
	Kamer van Koophandel en Nijverheid van Vaucluse (door de regionale controle-instantie PACA)	2017	FR
	Waarborgen van de beveiliging en instandhouding van de Estse nationale databanken die van kritiek belang zijn	Fin. 2018/nog niet gepubliceerd	EE
	Stand van zaken met betrekking tot de ontwikkeling van infrastructuur voor elektronische communicatie een versie in het Litouws een naar het Engels vertaalde samenvatting	2017	LT
	Information Technology Audit: Cyber Security across Government Entities	2017	MT
	Het nationale registersysteem: beveiliging, prestaties en bruikbaarheid	2017	PL
	The WannaCry incident	2017	VK
	Online Fraud	2017	VK
	Verslag over de bescherming tegen ransomware-aanvallen	2018	DK
	Ziekenhuis van Arpajon (door de regionale Kamer van Koophandel van Île-de-France)	2018	FR
	Beheer van kritieke informatiehulpbronnen van de staat	2018	LT
	Elektronische misdaden	2019	LT
	Informatiebeveiliging in Polen	2019	PL
Anders	Databank met overheidsinstanties	N.v.t.	BE
	Vragenlijst over beleid inzake beveiliging en risicoanalyse (lopend)	N.v.t.	BE

Acroniemen en afkortingen

AVG: Algemene verordening gegevensbescherming

BDI: Buitenlandse directe investeringen

CERT-EU: Computercrisisteam van de EU

cPPP: Contractueel publiek-privaat partnerschap

CSIRT: Computer Security Incident Response Team

DDoS: Distributed Denial of Services

DEP: Programma Digitaal Europa

DG CONNECT: Directoraat-generaal Communicatienetwerken, Inhoud en Technologie

DG HOME: Directoraat-generaal Migratie en Binnenlandse Zaken

DG JUST: Directoraat-generaal Justitie en Consumentenzaken

DIGIT: Directoraat-generaal Informatica

EC3: Europees cybercriminaliteitscentrum van Europol

ECSEL: Elektronische componenten en systemen voor Europees leiderschap

ECSM: Europese maand van de cyberbeveiliging

ECSO: European cyberbeveiligingsorganisatie

EDA: Europees Defensieagentschap

EDEO: Europese Dienst voor extern optreden

Enisa: Europees Agentschap voor netwerk- en informatiebeveiliging

ERK: Europese Rekenkamer

ESIF: Europees structuur- en investeringsfonds

ETA: Europese toezichthoudende autoriteit

EU: Europese Unie

GVDB: Gemeenschappelijk veiligheids- en defensiebeleid

HWPCI: Horizontale Groep cybervraagstukken

ICS: Industriële controlesystemen

ISF-P: Fonds voor interne veiligheid – Politie

ISSB: Stuurgroep voor informatiebeveiliging

JRC: Gemeenschappelijk Centrum voor onderzoek

Kmo's: Kleine en middelgrote ondernemingen

LISO: Lokale functionaris voor informatiebeveiliging

NAO: Nationale Rekenkamer

NCIRC: Responscapaciteit van de NAVO voor computerincidenten

NIS-richtlijn: Richtlijn netwerk- en informatiebeveiliging

PESCO: Permanente gestructureerde samenwerking

Woordenlijst

Adware: Malafide software die banners met advertenties of pop-ups toont waarin code is opgenomen om het onlinegedrag van slachtoffers te traceren.

Beheer van zwakke plekken: Een integraal onderdeel van computer- en netwerkbeveiliging waarmee wordt beoogd op proactieve wijze misbruik van zwakke plekken van een systeem of software te beperken of te voorkomen door middel van identificatie, classificatie en herstel ervan.

Beschikbaarheid: Het waarborgen van tijdige en betrouwbare toegang tot en gebruik van informatie.

Botnet: Een netwerk van computers die zijn geïnfecteerd met malafide software en, zonder dat de gebruiker zich hiervan bewust is, op afstand worden aangestuurd om spam te versturen, informatie te stelen of gecoördineerde cyberaanvallen uit te voeren.

Cloudcomputing: De levering van IT-middelen — zoals opslag, rekenkracht of capaciteit om gegevens te delen — op verzoek, via het internet en via hostingservers op afstand.

Crime-as-a-service-model (Caas): Een crimineel zakelijk model dat de digitale ondergrondse economie aandrijft en een breed scala van commerciële diensten en tools aanbiedt om ongeschoolde, beginnende cybercriminelen in staat te stellen cybermisdaden te begaan.

Cryptovaluta: Digitale activa die worden uitgegeven en uitgewisseld met behulp van versleutelingstechnieken, zonder tussenkomst van een centrale bank. Deze valuta worden aanvaard als betaalmiddel onder leden van een virtuele gemeenschap.

Cyberaanval: Een poging om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens of een computersysteem via de cyberspace te ondermijnen of ze te vernietigen.

Cyberafhankelijke criminaliteit: Een misdaad die alleen kan worden begaan met IT-apparatuur.

Cyberbeveiliging: Alle waarborgen en maatregelen die worden ingevoerd om IT-systemen en hun gegevens te beschermen tegen onbevoegde toegang, aanvallen en schade, teneinde hun beschikbaarheid, vertrouwelijkheid en integriteit te garanderen.

Cybercriminaliteit: Verschillende criminele activiteiten met computers en IT-systemen als primaire tool of als primair doelwit. Het gaat hierbij onder meer om activiteiten als traditionele strafbare feiten (bijv. fraude, vervalsing en identiteitsdiefstal), met inhoud verband houdende strafbare feiten (bijv. de onlinedistributie van kinderporno of het aanzetten tot rassenhaat), en strafbare feiten die alleen voorkomen in verband met computers en informatiesystemen (bijv. aanvallen op informatiesystemen, denial of service-aanvallen en malware).

Cyberdefensie: Een categorie van cyberbeveiliging waarmee wordt beoogd de cyberspace te beschermen met militaire en andere passende middelen om militair-strategische doelstellingen te realiseren.

Cyberecosysteem: Een complexe gemeenschap van interagerende apparaten, gegevens, netwerken, mensen, processen en organisaties en de omgeving van processen en technologieën die deze interacties beïnvloeden en ondersteunen.

Cybergefaciliteerde criminaliteit: Een traditioneel strafbaar feit dat op grotere schaal wordt gepleegd dankzij het gebruik van IT-systemen.

Cyberincident: Een voorval dat direct of indirect schade berokkent aan of een dreiging vormt voor de weerbaarheid en beveiliging van een IT-systeem en de gegevens die ermee worden verwerkt, opgeslagen of verzonden.

Cyberspace: De immateriële wereldwijde omgeving waarin onlinecommunicatie plaatsvindt tussen mensen, software en diensten via computernetwerken en technologische apparaten.

Cyberweerbaarheid: Het vermogen om cyberaanvallen en -incidenten te voorkomen, erop voorbereid te zijn, ze te weerstaan en ervan te herstellen.

Desinformatie: Aantoonbaar foute of misleidende informatie die wordt gecreëerd, gepresenteerd en verspreid voor economisch gewin of om het publiek opzettelijk te bedriegen, en die schade in het publieke domein kan veroorzaken.

Digitale inhoud: Gegevens — zoals tekst, geluid, afbeeldingen of video's — die zijn opgeslagen in digitale vorm.

Distributed Denial of Service (DDoS): Een cyberaanval die het legitieme gebruikers onmogelijk maakt toegang te krijgen tot een onlinedienst of -bron door deze dienst of bron te overspoelen met meer verzoeken dan deze aankan.

Exploitkit: Een soort toolkit die cybercriminelen gebruiken om zwakke punten in netwerk- en informatiesystemen te benutten om malware te verspreiden of andere kwaadwillige activiteiten uit te voeren.

Hacktivist: Individuen of groepen die onbevoegd toegang verkrijgen tot informatiesystemen of netwerken voor sociale of politieke doeleinden.

Het internet der dingen: Het netwerk van alledaagse objecten die zijn uitgerust met elektronica, software en sensoren zodat zij kunnen communiceren en gegevens kunnen uitwisselen via internet.

Hybride dreiging: Een uiting van vijandige intenties door tegenstanders, waarbij gebruik wordt gemaakt van een mix van conventionele en niet-conventionele technieken voor oorlogvoering (bijv. militaire, politieke, economische en technologische methoden), om hun doelstellingen op daadkrachtige wijze na te streven.

Informatiebeveiliging: Een reeks processen en instrumenten voor de bescherming van fysieke en digitale gegevens tegen onbevoegd(e) toegang, gebruik, vrijgave, verstoring, wijziging, opname of vernietiging.

Integriteit: Het voorkomen van de ongepaste wijziging of vernietiging van informatie en het garanderen van de authenticiteit ervan.

Kritieke infrastructuur: Fysieke hulpmiddelen, diensten en voorzieningen waarvan de verstoring of vernieling ernstige gevolgen zou hebben voor de werking van de economie en de samenleving.

Malware: Malafide software. Een computerprogramma dat is ontworpen om een computer, server of netwerk te schaden.

Netwerkbeveiliging: Een onderdeel van cyberbeveiliging dat gegevens beschermt die worden verzonden via apparaten op eenzelfde netwerk, om te garanderen dat de informatie niet wordt onderschept of gewijzigd.

Ouder systeem: Een systeem, toepassing of programmeertaal die/dat achterhaald of verouderd, maar nog steeds in gebruik is, en waarvoor de aanbieder mogelijk geen upgrades of klantondersteuning, met inbegrip van beveiligingsondersteuning, meer aanbiedt.

Patching/patchen: Het aanbrengen van een reeks wijzigingen in software om deze te actualiseren, repareren of verbeteren, onder meer door vanuit beveiligingsoogpunt zwakke plekken te verhelpen.

Persoonsgegevens: Informatie die kan worden herleid naar een bepaald individu.

Phishing: De praktijk van het verzenden van e-mails die zogenaamd van een betrouwbare afzender komen om ontvangers onder valse voorwendselen aan te moedigen om op malafide links te klikken of persoonsgegevens te delen.

Ransomware: Malafide software die slachtoffers de toegang ontzegt tot een computersysteem of de bestanden onleesbaar maakt, meestal door middel van versleuteling. De aanvaller chanteert het slachtoffer vervolgens meestal door te weigeren de toegang te herstellen totdat er losgeld wordt betaald.

Skimming: Het stelen van creditcard- of debetkaartgegevens wanneer deze online worden ingevoerd.

Social engineering: In de informatiebeveiliging: psychologische manipulatie om mensen onder valse voorwendselen over te halen iets te doen of vertrouwelijke informatie te onthullen.

Tekstvectorisatie: Het proces van het omzetten van woorden, zinnen of hele documenten in numerieke vectoren zodat ze kunnen worden gebruikt door algoritmen voor machinaal leren.

Toegangsgegevens: Informatie over de in- en uitlogactiviteit van een gebruiker om toegang te krijgen tot een dienst, zoals het tijdstip, de datum en het IP-adres.

Verkiezingsinfrastructuur: Omvat IT-systemen en databanken voor campagnes, gevoelige informatie over kandidaten en systemen voor de registratie en het beheer van kiezers.

Versleuteling: Het ter bescherming omzetten van leesbare informatie in onleesbare code. Om de informatie te kunnen lezen, moet de gebruiker toegang hebben tot een geheime sleutel of een wachtwoord.

Vertrouwelijkheid: De bescherming van informatie, gegevens of activa tegen onbevoegde toegang of vrijgave.

Vertrouwensdiensten: Diensten die de rechtsgeldigheid van een elektronische transactie vergroten, zoals elektronische handtekeningen, zegels, tijdstempels, gecertificeerde levering en authenticatie van websites.

Wiper-malware: Een soort malware die is bedoeld om de harde schijf van de computer die het infecteert, volledig te wissen.

[1] In de EU-ontwerpwet inzake cyberbeveiliging wordt cyberbeveiliging gedefinieerd als alle activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers ervan en getroffen personen tegen cyberdreigingen te beschermen. Naar verwachting zal de wet begin 2019 worden goedgekeurd door het Europees Parlement en de Raad.

[2] Europol, *Internet Organised Crime Threat Assessment 2017*.

[3] European Cyber Security Organisation (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, juni 2016.

[4] Europees Parlement, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, studie voor de Commissie LIBE, september 2015.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 januari 2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018*.

[7] Europol, *Ibid.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, incidenteel paper nr. 2/18, februari 2018.

[9] De Staat van de Unie 2017 van de voorzitter van de Europese Commissie.

[10] Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down*, persbericht, 25 april 2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017*.

[12] Informatieblad van de Europese Commissie over cyberbeveiliging, september 2017.

[13] Het kan onder meer om de volgende kosten gaan: inkomstenderving; kosten van het repareren van beschadigde systemen; prikkels om klanten over te halen om te blijven; hogere verzekeringspremies; hogere kosten voor bescherming (nieuwe systemen, medewerkers, opleidingen); kosten van potentiële boetes of rechtszaken.

[14] NTT Security, *Risk:Value 2018 Report*.

[15] De *Wannacry*-ransomware benutte zwakke punten in een protocol van Microsoft Windows, waardoor alle computers op afstand konden worden overgenomen. Microsoft had al wel een correctie uitgebracht nadat het bedrijf de zwakke plek had ontdekt, maar honderdduizenden computers waren nog niet geactualiseerd en vele daarvan raakten vervolgens besmet. Bron: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19 december 2017.

[16] Europese Commissie, *Europeans' attitudes towards cybersecurity*, Speciale Eurobarometer 464a, september 2017. Begin 2019 wordt naar verwachting een vervolgonderzoek gepubliceerd.

[17] Het Verdrag van Boedapest is een bindend internationaal richtsnoer voor landen die wetgeving tegen cybercriminaliteit ontwikkelen. Het biedt een kader voor internationale samenwerking tussen de staten die er partij bij zijn. Momenteel wordt de EU vertegenwoordigd door de Commissie, de Raad van de Europese Unie, Europol, Enisa en Eurojust.

[18] Europese Commissie, *Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace*, JOIN(2013) 1 final, 7 februari 2013.

[19] Europese Commissie, *De Europese veiligheidsagenda*, COM(2015) 185 final, 28 april 2015.

[20] Europese Commissie, *Strategie voor een digitale eengemaakte markt voor Europa*, COM(2015) 192 final, 6 mei 2015.

[21] EDEO, *Gedeelde visie, gemeenschappelijk optreden: een sterker Europa. Een integrale strategie voor het buitenlands en veiligheidsbeleid van de Europese Unie*, juni 2016.

[22] Centrum voor Europese Beleidsstudies, *Strengthening the EU's Cyber Defence Capabilities — Report of a CEPS Task Force*, november 2018.

[23] De malware achter de Wannacry-aanval met ransomware, die door de Verenigde Staten, het VK en Australië wordt toegeschreven aan Noord-Korea, werd oorspronkelijk ontwikkeld en bewaard door het nationale veiligheidsagentschap van de VS om in een later stadium van de zwakke plekken in Windows te kunnen profiteren. Bron: A. Greenberg, ibid., WIRED, 19 december 2017. Naar aanleiding van de aanvallen veroordeelde Microsoft het bewaren van informatie over zwakke plekken in software door overheden en riep het bedrijf nogmaals op tot een digitaal Verdrag van Genève.

[24] Land, zee, lucht en ruimte zijn de eerste vier.

[25] EU-beleidskader voor cyberdefensie (update 2018), 14413/18, 19 november 2018.

[26] Europese Commissie/Europese Dienst voor extern optreden, *Gezamenlijk kader voor de bestrijding van hybride bedreigingen: een reactie van de Europese Unie*, JOIN(2016) 18 final, 6 april 2016.

[27] Gemeenschappelijke verklaring van de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie, 8 juli 2016 en 10 juli 2018.

[28] Europese Commissie/Europese Dienst voor extern optreden, *Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU*, JOIN(2017) 450 final, 13 september 2017.

[29] 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 (PB L 194 van 19.7.2016, blz. 1).

[30] 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.

[31] Deze zijn geïntegreerd in de structuren voor samenwerking die op grond van de richtlijn zijn opgericht, het CSIRT-network (een netwerk dat bestaat uit door de EU-lidstaten aangewezen CSIRT's en CERT-EU; Enisa treedt als gastheer op voor het secretariaat) en de Samenwerkingsgroep (ondersteunt en vergemakkelijkt de strategische samenwerking en informatie-uitwisseling tussen lidstaten; de Commissie treedt als gastheer op voor het secretariaat).

[32] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

[33] Europese Commissie, *Voorstel voor een Verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")*, COM(2017) 477 final, 13 september 2017.

[34] Europese Commissie, *Voorstel voor een verordening van het Europees Parlement en de Raad betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken*, COM(2018) 225 final, 17 april 2018.

[35] Europese Commissie, *Voorstel voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures*, COM(2018) 226 final, 17 april 2018.

[36] Europese Commissie, *Voorstel voor een verordening van het Europees Parlement en de Raad tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra*, COM(2018) 630 final, 12 september 2018.

[37] H. Carrapico en A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, vol. 55, nr. 6, 2017.

[38] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017.

[39] Onderzoeksdienst van het Europees Parlement, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects*, PE 603.948, december 2017.

[40] ENISA, *An evaluation framework for Cyber Security Strategies*, 27 november 2014.

[41] Een uitzondering hierop is artikel 14 ("Toetsing en statistieken") van Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.

[42] Europees Economisch en Sociaal Comité, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, maart 2018. Taakgroep CEPS-ECRI, Cybersecurity in Finance: Getting the policy mix right!, juni 2018.

[43] 24 van de 28 nationale rekenkamers hebben aan de enquête deelgenomen.

[44] Gebaseerd op beginselen en vanuit technologisch oogpunt zo neutraal mogelijk.

[45] Wetenschappelijk adviesmechanisme van de Europese Commissie Wetenschappelijk advies 2/2017, 24 maart 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, september 2018. European Centre for Political Economy, ibid., Occasional paper No 2/18, februari 2018.

[47] Europese Commissie, *Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud*, COM(2015) 634 final, 9 december 2015.

[48] Europese Commissie, *Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de onlineverkoop en andere verkoop op afstand van goederen*, COM(2017) 635 final, 9 december 2015.

[49] Nederlandse Cyber Security Raad, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, 2016.

[50] Centrum voor Europese Beleidsstudies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges — Report of a CEPS Task Force*, juni 2018.

[51] Europese Commissie, *De NIS-richtlijn ten volle benutten — naar de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie*, COM(2017) 476 final/2, 4 oktober 2017.

[52] Europol, ibid., 2017.

[53] Raad van de Europese Unie, *Eindverslag over de zevende wederzijdse evaluatieronde inzake "De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit"*, 12711/1/17 REV 1, 9 oktober 2017.

[54] Europese Commissie, Effectbeoordeling bij het document "Voorstel voor een richtlijn betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten", SWD/2017/0298 final, 13 september 2017. In december 2018 werd politieke overeenstemming bereikt over de nieuwe wet, die naar verwachting begin 2019 zal worden aangenomen.

[55] Europol, ibid., 2017.

[56] C-362/14 Maximillian Schrems tegen Data Protection Commissioner (Ierland), 6 oktober 2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13 maart 2017.

[58] Europese Commissie, *Assessment of the EU 2013 Cybersecurity Strategy*, SWD(2017) 295 final, 13 september 2017.

[59] Onderzoeksdienst van het Europees Parlement, *Briefing: EU Legislation in Progress — Review of dual-use export controls*, PE589.832.

[60] European Parliament resolution, *Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries*, (2014/2232(INI)), 8 september 2015. Goederen en diensten voor tweeërlei gebruik, waaronder software en technologie, kunnen zowel voor civiele als voor militaire doeleinden worden gebruikt.

[61] De openbaar beschikbare informatie wordt opgeslagen in de WHOIS-databank, die wordt beheerd door ICANN (Internet Corporation for Assigned Names and Numbers). ICANN houdt het systeem van domeinnamen bij. Misbruik van domeinnamen vergemakkelijkt cybercriminaliteit.

[62] Artikel 3, NIS-richtlijn, ibid.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, 10 september 2015.

[64] Het Witte Huis, *Cybersecurity spending fiscal year 2019*.

[65] Europese Commissie, *Werkdocument van de diensten van de Commissie: Impact Assessment Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027"*, SWD(2018) 305 final, 6 juni 2018.

[66] Den Haag Centrum voor Strategische Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, december 2016.

[67] Europese Commissie, ibid., COM(2018) 630 final, 12 september 2018.

[68] Onderzoeksdienst van het Europees Parlement, afdeling Wetenschappelijke Toekomstverkenningen, *Achieving a sovereign and trustworthy ICT industry in the EU*, december 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem*, 31 juli 2017.

[70] Onderzoeksdienst van het Europees Parlement, afdeling Wetenschappelijke Toekomstverkenningen, ibid., december 2017.

[71] Ibid.

[72] Europese Commissie, *Impact assessment on the proposed research competence centre and network of national coordination centres*, SWD(2018) 403 final (Part 1/4), 12 september 2018.

[73] Europese Commissie, ibid., COM(2018) 630 final, 12 september 2018.

[74] Speciaal verslag nr. 13/2018 van de ERK: "Aanpak van radicalisering die tot terrorisme leidt".

[75] De cijfers die in dit onderdeel worden vermeld, komen uit openbaar beschikbare documenten van de Commissie, met uitzondering van het bedrag van 42 miljoen EUR uit paragraaf ***51***, dat rechtstreeks door de Commissie aan ons is doorgegeven.

[76] Horizon 2020 is het onderzoeks- en innovatieprogramma van de EU met een begroting van 80 miljard EUR, dat de innovatie-unie ondersteunt en waarmee wordt beoogd het mondiale concurrentievermogen van de EU veilig te stellen.

[77] Maatschappelijke uitdaging 7 van Horizon 2020, "Veilige en innovatieve samenlevingen: de vrijheid en veiligheid van Europa en haar burgers beschermen".

[78] We hebben de H2020-projecten uit de CORDIS-gegevensreeks geanalyseerd. We hebben tekstvectorisatie toegepast op de beschrijving van elk project aan de hand van de cyberbeveiligingstaxonomie van het JRC (zie ***tekstvak 5*** in het volgende hoofdstuk), om projecten te vinden die waarschijnlijk verband houden met cyberbeveiliging. We hebben de resultaten vervolgens handmatig gecontroleerd en geanalyseerd.

[79] European Cyber Security Organisation, *ECS cPPP Progress Monitoring Report 2016-2017*, 29 oktober 2018.

[80] Artikel 9, lid 2, NIS-richtlijn, ibid.

[81] GLACY+ (the Global Action on Cybercrime+) is een gezamenlijk project met de Raad van Europa. In het kader van dit project worden twaalf landen in Afrika, de Aziatisch-Pacifische regio, alsook Latijns-Amerika en het Caribisch gebied gesteund, die op hun beurt weer als hubs kunnen dienen en hun ervaringen kunnen delen met andere landen in hun regio.

[82] Het Europees Centrum voor politieke strategie (EPSC), de denktank van de Commissie, heeft gewezen op het risico van het ontstaan van een "digitale blinde vlek" als de kloof tussen de EU en de Westelijke Balkan blijft groeien. Landen als China en Rusland investeren grote bedragen in de regio, waardoor het risico ontstaat dat de EU als cyberspeler wordt verdrongen. Bron: EPSC, *Engaging with the Western Balkans: an investment in Europe's security*, 17 mei 2018.

[83] Europese Investeringsbank, *The EIB Group Operating Framework and Operational Plan 2018*, 12 december 2017. Op het moment dat dit document werd opgesteld, was er geen verdere informatie beschikbaar.

[84] Europese Commissie, *Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van het programma Digitaal Europa voor de periode 2021-2027*, COM(2018) 434 final, 6 juni 2018.

[85] Europese Commissie, *Verordening (EU) 2018/1092 van het Europees Parlement en de Raad van 18 juli 2018 tot instelling van het industrieel ontwikkelingsprogramma voor de Europese defensie ter ondersteuning van het concurrentievermogen en de innovatieve capaciteit van de defensie-industrie van de Unie* (PB L 200 van 7.8.2018, blz. 30). In aanvulling hierop werd in 2017 een voorbereidende actie voor defensieonderzoek opgezet, met een totale begroting van 90 miljoen EUR voor de periode 2017-2019, die wordt gefinancierd in het kader van H2020. Het is onduidelijk of hier cybergerelateerde uitgaven onder vallen.

[86] De publicatie van een afzonderlijk briefingdocument van de ERK over EU-defensie staat gepland voor 2019.

[87] De EC3 van Europol, Enisa, de EDEO, het Europees Defensieagentschap en CERT-EU hebben samen 159 medewerkers in dienst. In dit totale aantal is het personeel dat zich bezighoudt met cyberkwesties bij de Europese Commissie of in de lidstaten niet meegerekend. Bron: Centrum voor Europese Beleidsstudies, ibid., november 2018.

[88] *ENISA-evaluatie*, 2017.

[89] Europol heeft in zijn meerjarenplan voor 2018-2020 verzocht om een jaarlijkse uitbreiding van het personeelsbestand met 70 tijdelijke functionarissen, maar voor 2018 werd slechts een stijging van 26 functionarissen goedgekeurd. In het volgende meerjarenplan voor 2019-2021

gaat Europol uit van een meer bescheiden stijging, wetende dat een verzoek om veel meer middelen niet zal worden ingewilligd. Bron: Raadpleging inzake het ontwerp voor een meerjarige programmering voor 2019-2021, ingediend bij de gezamenlijke parlementaire controlegroep, A 000834, 1 februari 2018.

[90] *ENISA-evaluatie*, 2017. Tussen 2014 en 2016 ging ongeveer 80 % van de operationele begroting van Enisa naar uitbestede studies.

[91] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, december 2017.

[92] ISACA (voorheen bekend onder de naam Information Systems Audit and Control Association), *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2e editie, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017*, blz. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy en H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, juli 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*, 21 februari 2018.

[96] Een forum voor samenwerking tussen de Europese Bankautoriteit, de Europese Autoriteit voor effecten en markten en de Europese Autoriteit voor verzekeringen en bedrijfspensioenen.

[97] Europese Autoriteit voor effecten en markten, *Joint Committee report on risks and vulnerabilities in the EU financial system*, april 2018.

[98] Enisa, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs*, december 2015.

[99] Het mechanisme voor wetenschappelijk advies van de Commissie heeft gewezen op het aanzienlijke en unieke niveau van overeenstemming tussen de EU-lidstaten met betrekking tot de fundamentele beginselen en waarden en het gedeelde strategische belang die samen de kern kunnen vormen van een doeltreffende EU-governance inzake cyberbeveiliging. Bron: Wetenschappelijk advies 2/2017, 24 maart 2017.

[100] Verenigde Staten, China, Japan, Zuid-Korea, India en Brazilië.

[101] Europese Veiligheids- en defensieacademie (T. Renard en A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence*, 23 november 2018.

[102] Raad van de Europese Unie, *Actieplan voor de uitvoering van de conclusies van de Raad over de gezamenlijke mededeling aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU"*, 15748/17, 12 december 2017.

[103] Europese Commissie, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, 21 november 2018.

[104] Antwoord van commissaris Gabriel op een schriftelijke vraag van het Parlement (E-004294-17), 28 juni 2017.

[105] Raad van de Europese Unie, *Annual Report on the Implementation of the Cyber Defence Policy Framework*, 15870/17, 19 december 2017.

[106] Besluiten 2015/443, 2015/444 en 2017/46 regelen de beveiliging van de communicatie- en informatiesystemen van de Commissie. Bij besluit C(2018) 7706 van de Commissie van 21 november 2018 is een Raad voor informatietechnologie en cyberbeveiliging opgericht, waarin de eerdere IT-raad en de Stuurgroep informatiesysteembeveiliging werden samengevoegd.

[107] Europees Economisch en Sociaal Comité, ibid., maart 2018.

[108] Europees Parlement, ibid., september 2015.

[109] De Fusiecel voor analyse van hybride bedreigingen werd in 2016 opgericht binnen het Inlichtingen- en situatiecentrum van de EU, dat onder de EDEO valt. De cel ontvangt en analyseert geclassificeerde en openbaar beschikbare informatie van verschillende belanghebbenden over hybride dreigingen.

[110] ENISA, *National-level Risk Assessments: An Analysis Report*, november 2013.

[111] Europese Commissie, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act*, SWD(2017) 500 final (deel 1/6), 13 september 2017.

[112] Europese Commissie, ibid., COM(2018) 403 final, 12 september 2018.

[113] Résaux IP Européens Network Coordination Centre, het regionale internetregister voor Europa dat toezicht houdt op de toewijzing en registratie van “internet number resources”.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs*, november 2012.

[115] Het Centre for Cyber Safety and Education, in samenwerking met Booz Allen Hamilton, Alta Associates en Frost & Sullivan, *2017 Global Information Security Workforce Study — Benchmarking Workforce Capacity and Response to Cyber Risk*.

[116] Europees Economisch en Sociaal Comité, ibid., maart 2018.

[117] Brits Hogerhuis, *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK’s Critical National Infrastructure, Second Report of Session 2017–19*, 16 juli 2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime*, 7021/17, 13 maart 2017.

[119] Europol/Eurojust, ibid., 7021/17, 13 maart 2017.

[120] Europese Commissie, ibid., COM(2018) 403 final, 12 september 2018.

[121] CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022*, 20 november 2018.

[122] Bijvoorbeeld samenwerking tussen de EDEO, lidstaten en agentschappen en organen als Cepol, ECTEG of het EDSC.

[123] ENISA, *Stock-taking of information security training needs in critical sectors*, december 2017.

[124] Europese groep voor opleiding in verband met cybercriminaliteit.

[125] Europese Commissie, Dertiende voortgangsverslag over de totstandkoming van een echte en doeltreffende Veiligheidsunie, COM(2018) 46 final, 24 januari 2018.

[126] Gebaseerd op opmerkingen uit het Speciaal verslag nr. 14/2018, ibid.

[127] Resolutie van het Europees Parlement van 13 juni 2018 over cyberdefensie (2018/2004(INI)) Raad van de Europese Unie, ibid., 15870/17, 19 december 2017.

[128] Zwitserland, Fyrom, Oekraïne, Bosnië-Herzegovina, Kosovo (deze benaming laat de standpunten over de status van Kosovo onverlet en is in overeenstemming met UNSCR 1244 en het advies van het IGH over de onafhankelijkheidsverklaring van Kosovo), Turkije en de Verenigde Staten.

[129] Europol, *Internet Organised Crime Threat Assessment 2018*.

[130] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman en S. Furman, *Security Fatigue*, "IT Professional", vol. 18, nr. 5, 2016, blz. 26-32. Zie ook NIST.

[132] European Commission/European External Action Service, *Het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen*, JOIN(2018) 16 final, 13 juni 2018.

[133] Bijvoorbeeld de buitenbedrijfstelling van AlphaBay en Hansa als gevolg van gezamenlijke operaties geleid door de FBI en de Nederlandse nationale politie, met steun van Europol. Dit waren de twee grootste marktplaatsen voor de handel in illegale goederen als drugs, vuurwapens en middelen voor cybercriminaliteit, zoals malware. Bron: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure*, persbericht, 29 mei 2018.

[134] Europese Commissie, ibid., COM(2018) 403 final, 12 september 2018.

[135] Raad van de Europese Unie, ibid., 12711/17 REV 1, 9 oktober 2017.

[136] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017.

[137] European Commissie/Europese Dienst voor extern optreden, ibid., JOIN(2018) 16, 13 juni 2018.

[138] Europese Commissie, SWD(2017) 500 final, 13 september 2017.

[139] *Memorandum van overeenstemming — ENISA, EDA, Europol EC3 en CERT-EU*; 23 mei 2018.

[140] Europese Commissie, oproep tot inschrijving: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap*, 27 oktober 2017.

[141] Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union, 2 augustus 2016. Defensie maakt geen deel uit van het mandaat van de taskforce.

[142] Raad van de Europese Unie, *EU cybersecurity roadmap*, 8901/17, 11 mei 2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues*, 5e editie, november 2017.

[144] Technische verslagen JRC, European Cybersecurity Centres of Expertise Map: *Definitions and Taxonomy.* Impact assessment on the proposed Research Competence Centre and Network of National Coordination Centres, SWD(2018) 403 final, 12 september 2018.

[145] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017.

[146] Europese Commissie, ibid., COM(2018) 403 final, 12 september 2018.

[147] Zo wordt het ISAC voor Europese financiële instellingen onder meer gevormd door vertegenwoordigers van de financiële sector, nationale CERT's, wetshandhavingsinstanties, Enisa, Europol, de Europese Centrale Bank, de Europese Betalingsraad en de Europese Commissie.

[148] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 14 februari 2018.

[149] Raad van de Europese Unie, ibid., 12711/17 REV 1, 9 oktober 2017.

[150] https://www.europol.europa.eu/empact.

[151] Uit een studie die Accenture in 2018 in 15 landen uitvoerde, kwam naar voren dat 87 % van de gerichte cyberaanvallen wordt voorkomen: *2018 State of Cyber Resilience*, 10 april 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy*, politieke blog Universiteit van Oxford, 14 september 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective*, IT Pro, 14 juli 2017.

[154] Europees Economisch en Sociaal Comité, *Ibid.*, maart 2018.

[155] Europese Commissie, *Achtste voortgangsverslag over de totstandkoming van een echte en doeltreffende Veiligheidsunie*, COM(2017) 354 final, 29 juni 2017.

[156] Zie de verschillende publicaties van de NIS-samenwerkingsgroep.

[157] PSD2: tweede richtlijn betalingsdiensten; ECB/GTM: Europese Centrale Bank/gemeenschappelijk toezichtsmechanisme; Target 2: geautomatiseerd trans-Europees “real-time” bruto-vereveningssysteem (2e generatie), Verordening (EU) nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Bron: Taakgroep CEPS-ECRI, ibid., juni 2018.

[158] Europese Commissie, *Aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises*, C(2017) 6100 final, 13 september 2017.

[159] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017. Er zijn verschillende mechanismen voor crisisbeheer, waaronder de geïntegreerde EU-regeling politieke crisisrespons (IPCR), Argus (het crisisresponsmechanisme van de Commissie), het crisisresponsmechanisme van de EDEO, het Uniemechanisme voor civiele bescherming en het EU-wetshandhavingsprotocol voor respons in noodsituaties.

[160] Daarnaast kan dit er ook toe leiden dat er een beroep wordt gedaan op artikel 42, lid 7, van het Verdrag betreffende de Europese Unie (clausule inzake wederzijdse bijstand) of op artikel 222 van het Verdrag betreffende de werking van de Europese Unie (solidariteitsclausule).

[161] Europese Commissie/Europese Dienst voor extern optreden, ibid., JOIN(2018) 16, 13 juni 2018. In december 2018 was in de media sprake van vermeende hacks van het diplomatieke communicatienetwerk van de EDEO, COREU (bron: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran*; 18 december 2018). Deze kwestie wordt momenteel onderzocht.

[162] Ook moet de samenwerking op het gebied van vroegtijdige waarschuwingen en wederzijdse bijstand verder worden ontwikkeld: *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*, 10085/18, 26 juni 2018.

[163] Onderzoeksdienst van het Europees Parlement, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act*, PE 614.643, september 2018.

[164] Europees Economisch en Sociaal Comité, ibid., maart 2018.

[165] Raad van de Europese Unie, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks*, 14893/18, december 2018.

[166] Snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging; platform voor het delen van informatie over cyberdreigingen en respons op incidenten. Bron: Raad van de Europese Unie, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects — Overview*, 19 november 2018.

[167] Raad van de Europese Unie, Conclusies over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten, 9916/17, 7 juni 2017.

[168] Raad van de Europese Unie, *Conclusies van de Raad over cyberdiplomatie*, 6122/55, 11 februari 2015.

[169] Raad van de Europese Unie, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[170] Het aanwijzen van de verantwoordelijken van een incident blijft een soeverein politiek besluit van de lidstaten, en attributie is niet voor alle maatregelen op grond van het instrumentarium nodig.

[171] Het instrumentarium heeft niet geresulteerd in gezamenlijke actie; de individuele lidstaten namen het Amerikaanse standpunt over.

[172] Raad van de Europese Unie, *Conclusies over kwaadwillige cyberactiviteiten*, 7925/18, 16 april 2018.

[173] Computersystemen die worden gebruikt om processen in verschillende sectoren — zoals nutsdiensten, chemische en industriële productie, verwerking van levensmiddelen, vervoerssystemen- en knooppunten en logistieke diensten — te beheersen.

[174] ENISA, ibid., december 2017.

[175] Bijvoorbeeld openbaar bestuur, chemische en nucleaire industrieën, productie, verwerking van levensmiddelen, toerisme, logistiek en civiele bescherming.

[176] Europese Commissie, ibid., SWD(2017) 295 final, 13 september 2017.

[177] Toespraak van commissaris Jourová tijdens de plenaire zitting van het Europees Parlement over *"Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign"*, 14 november 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, 23 mei 2018.

[179] Europees Centrum voor politieke strategie (L. Past), "Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses", in: "Election Interference in the Digital Age — Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] Volgens Richtlijn 2008/114/EG van de Raad inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren.

[181] Europese Commissie, Aanbeveling betreffende electorale samenwerkingsnetwerken, onlinetransparantie, bescherming tegen cyberincidenten en bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement, C(2018) 5949 final, 12 september 2018.

[182] Conclusies van de Europese Raad, EUCO 11/15, 20 maart 2015. Er zijn hierna nog twee aanvullende taskforces opgezet, voor de Westelijke Balkan en het zuidelijk nabuurschap.

[183] In een verslag van de Atlantische Raad werd de EU verzocht, van alle lidstaten te eisen dat zij nationale deskundigen leveren aan de taskforce. Zie: D. Fried en A. Polyakova, *Democratic Defense Against Disinformation*, 5 maart 2018.

[184] In eerste instantie had de taskforce geen eigen begroting, maar in 2018 werd door het Europees Parlement 1,1 miljoen EUR toegewezen voor een voorbereidende "Stratcom Plus"-actie.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23 mei 2018.

[186] Europese Commissie, de hoge vertegenwoordiger van de EU voor buitenlandse zaken en veiligheidsbeleid, *Action Plan against Disinformation*, JOIN(2018) 36 final. In dit plan wordt aandacht besteed aan het verbeteren van de capaciteit van de EU-instellingen om desinformatie te detecteren, analyseren en aan het licht te brengen; het versterken van de gecoördineerde en gezamenlijke respons; het mobiliseren van de particuliere sector; en het vergroten van het bewustzijn en van de maatschappelijke weerbaarheid.

[187] Europese Commissie, *Bestrijding van online-desinformatie: een Europese benadering*, COM(2018) 236 final, 26 april 2018.

[188] Deze code mag niet worden verward met de gedragscode voor de bestrijding van illegale haatuitingen op internet.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, Technische verslagen JRC, JRC Digital Economy Working Paper 2018-02, april 2018.

[190] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News"),* april 2018.

[191] Europees Centrum voor politieke strategie (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats*, in: ibid, 2018.

[192] Europese Commissie, ibid., COM(2018) 403 final, 12 september 2018.

[193] De voorgestelde verordening (COM(2017) 487 final, 13 september 2018) voor de screening van buitenlandse directe investeringen, ingediend in september 2017, doorloopt momenteel de fasen van het wetgevingsproces. De verordening heeft specifiek betrekking op kritieke technologieën, waaronder kunstmatige intelligentie, cyberbeveiliging en toepassingen voor tweeërlei gebruik.

[194] European Commissie/Europese Dienst voor extern optreden, ibid., JOIN(2017) 450 final, 13 september 2017.

ERK-team

Dit briefingdocument *Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging* werd goedgekeurd door controlekamer III "Externe maatregelen, veiligheid en justitie", onder leiding van ERK-lid Bettina Jakobsen. De taak werd geleid door ERK-lid Baudilio Tomé Muguruza, ondersteund door Daniel Costa de Magalhaes, kabinetschef en Ignacio Garcia de Parada, kabinetsattaché; Alejandro Ballester-Gallardo, hoofdmanager; Michiel Sweerts, taakleider; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, controleurs en Johannes Bolkart, stagiair. Hannah Critoph verleende taalkundige ondersteuning.

Van links naar rechts: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EUROPESE REKENKAMER

Publicatiebureau

EUROPESE REKENKAMER
12, rue Alcide De Gasperi
L-1615 Luxemburg
LUXEMBURG

Tel. +352 4398-1

Inlichtingen: eca.europa.eu/nl/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors