Raad van de
Europese Unie

Brussel, 16 december 2020
(OR. en)

14133/20

Interinstitutioneel dossier:
2020/0305(NLE)

CYBER 280	**RECH 529**
JAI 1118	**COMPET 642**
JAIEX 121	**IND 273**
EJUSTICE 107	**COTER 115**
COSI 254	**ENFOPOL 350**
DATAPROTECT 154	**COPS 485**
COPEN 387	**MI 578**
TELECOM 269	**IXIM 139**
PROCIV 99	**POLMIL 201**
CSC 367	**HYBRID 48**
CIS 65	**CSCI 96**
RELEX 1019	**POLGEN 234**

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	16 december 2020
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	JOIN(2020) 18 final
Betreft:	GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

Hierbij gaat voor de delegaties document JOIN(2020) 18 final.

Bijlage: JOIN(2020) 18 final

EUROPESE
COMMISSIE

HOGE VERTEGENWOORDIGER
VAN DE UNIE VOOR
BUITENLANDSE ZAKEN
EN VEILIGHEIDSBELEID

Brussel, 16.12.2020
JOIN(2020) 18 final

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD

De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT EN DE RAAD

De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

I. INLEIDING: EEN CYBERCRIMINALITEITSBESTENDIGE DIGITALE TRANSFORMATIE IN EEN OMGEVING VAN COMPLEXE BEDREIGINGEN

Cyberbeveiliging vormt een wezenlijk onderdeel van de veiligheid van de Europeanen. Of het nu gaat om verbonden apparaten, elektriciteitsnetwerken, luchtvaartuigen, overheidsdiensten of ziekenhuizen die zij gebruiken of bezoeken, mensen moeten in de wetenschap kunnen verkeren dat zij steeds beschermd zijn tegen cyberdreigingen. De Europese economie, democratie en samenleving zijn meer dan ooit afhankelijk van veilige, betrouwbare digitale hulpmiddelen en connectiviteit. Cyberbeveiliging is dan ook van essentieel belang om een veerkrachtig, groen en digitaal Europa op te bouwen.

Vervoer, energie en gezondheid, telecommunicatie, financiën, veiligheid, democratische processen, ruimtevaart en defensie berusten in grote mate op netwerk- en informatiesystemen die steeds meer onderling verbonden zijn. Verschillende sectoren zijn sterk van elkaar afhankelijk omdat netwerk- en informatiesystemen voor hun werking op hun beurt afhankelijk zijn van een continue elektriciteitsvoorziening. Er zijn nu al meer verbonden apparaten dan er mensen zijn op deze planeet, en hun aantal zal naar verwachting stijgen tot 25 miljard in 2025[1]: een kwart van deze apparaten zal zich in Europa bevinden. De digitalisering van arbeidspatronen is door de COVID-19-pandemie in een stroomversnelling terechtgekomen: 40 % van de werknemers in de EU is overgeschakeld op telewerk, en dit zal naar verwachting blijvende effecten hebben op het dagelijkse leven[2]. Dit maakt ons kwetsbaarder voor cyberaanvallen[3]. Verbonden voorwerpen worden vaak naar de consument verzonden met bekende zwakke plekken, die het aanvalsoppervlak voor kwaadwillige cyberactiviteiten verder vergroten[4]. Het industriële landschap in de EU is steeds meer gedigitaliseerd en verbonden; dat betekent ook dat cyberaanvallen veel grotere gevolgen kunnen hebben voor bedrijfstakken en ecosystemen dan in het verleden.

---

[1] Raming door GSMA, een brancheorganisatie voor de telecom; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf De International Data Corporation voorspelt 42,6 miljard verbonden machines, sensoren en camera's; https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[2] In een enquête die in juni 2020 werd gehouden, gaf 47 % van de bedrijfsleiders aan voornemens te zijn om werknemers voltijds te laten telewerken, zelfs indien het mogelijk wordt om terug naar het werk te komen; 82 % van hen was van plan om telewerken op zijn minst deeltijds toe te laten; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Een van de schadelijkste malwareprogramma's tot nu toe, Mirai, bracht botnets van meer dan 600 000 apparaten tot stand die meerdere grote websites in Europa en in de Verenigde Staten verstoorden.

De diverse bedreigingen worden verder aangescherpt door de geopolitieke spanningen over het mondiale, open internet en over de controle over technologieën in de gehele toeleveringsketen[5]. Die spanningen komen tot uiting in het feit dat steeds meer natiestaten digitale grenzen opwerpen. Beperkingen van en voor het internet bedreigen de mondiale, open cyberspace, maar ook de rechtsstaat, de grondrechten, de vrijheid en de democratie – de kernwaarden van de EU. Cyberspace wordt steeds vaker misbruikt voor politieke en ideologische doeleinden, en de toenemende polarisering op internationaal niveau staat een doeltreffend multilateralisme in de weg. Hybride bedreigingen vormen een combinatie van desinformatiecampagnes en cyberaanvallen op infrastructuur, economische processen en democratische instellingen en kunnen zo fysieke schade berokkenen, op onrechtmatige wijze toegang krijgen tot persoonsgegevens, bedrijfs- of staatsgeheimen stelen, wantrouwen zaaien en de sociale samenhang verzwakken. Dergelijke activiteiten ondermijnen de internationale veiligheid en stabiliteit en de voordelen van cyberspace voor de economische, sociale en politieke ontwikkeling.

Kwaadwillige aanvallen op kritieke infrastructuur vormen ook een belangrijk risico wereldwijd[6]. Het internet is gedecentraliseerd opgezet, het heeft geen centrale structuur en kent een multistakeholdergovernance. Het heeft exponentiële toenames van de verkeersvolumes weten op te vangen terwijl het voortdurend het doelwit was van kwaadwillige pogingen om de werking te verstoren[7]. Tegelijkertijd worden de kernfuncties van het mondiale, open internet steeds meer bevraagd, zoals het Domain Name System (DNS) en essentiële internetdiensten voor communicatie en hosting, toepassingen en gegevens. Die diensten zijn steeds meer geconcentreerd bij een klein aantal particuliere bedrijven[8]. Daardoor zijn de Europese economie en samenleving kwetsbaar voor verstorende geopolitieke of technische gebeurtenissen die de kern van het internet of een of meer van die bedrijven treffen. Door het toenemende gebruik van het internet en de veranderende patronen vanwege de pandemie is eens te meer gebleken hoe kwetsbaar toeleveringsketens zijn die van die digitale infrastructuur afhankelijk zijn.

Bezorgdheid over de veiligheid is een belangrijke ontmoedigende factor voor het gebruik van onlinediensten[9]. Ongeveer twee vijfde van de gebruikers in de EU heeft beveiligingsproblemen ervaren en drie vijfde acht zich niet in staat om zichzelf te

---

[5] Met inbegrip van elektronische onderdelen, gegevensanalyses, snellere en slimmere netwerken dankzij 5G en wat daarna komt, versleuteling, kunstmatige intelligentie (KI) en nieuwe paradigma's op het gebied van computers en gegevensverwerking, zoals blockchain, cloud-to-edge en kwantumcomputing.

[6] Wereld Economisch Forum, Global Risks Report 2020.

[7] De pandemie heeft tot een stijging van het internetverkeer van 60 % geleid, zo stelt de Organisatie voor Economische Samenwerking en Ontwikkeling; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Het Orgaan van Europese regulerende instanties voor elektronische communicatie en de Commissie publiceren regelmatig verslagen over de status van de internetcapaciteit tijdens de lockdownmaatregelen vanwege het coronavirus. Volgens een verslag van Enisa nam het totale aantal DDoS-aanvallen (Distributed Denial of Service) tijdens het derde kwartaal van 2019 met 241 % toe ten opzichte van het derde kwartaal van 2018. De intensiteit van DDoS-aanvallen neemt toe: de grootste aanval ooit vond plaats in februari 2020 en bereikte een piekverkeer van 2,3 terabit per seconde. Bij de "CenturyLink-panne" in augustus 2020 zorgde een routeringsprobleem bij de Amerikaanse internetaanbieder voor een daling van het mondiale internetverkeer met 3,5 %; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/nl/data/dataset/S2249_92_2_499_ENG

beschermen tegen cybercriminaliteit[10]. Een derde heeft de afgelopen drie jaar frauduleuze e-mails of telefoontjes gekregen waarin om persoonsgegevens werd gevraagd, maar 83 % heeft nooit melding gemaakt van cybercriminaliteit. Een op acht bedrijven werd al getroffen door een cyberaanval[11]. Meer dan de helft van de pc's van bedrijven en consumenten die één keer met malware zijn geïnfecteerd, wordt binnen een jaar opnieuw geïnfecteerd[12]. Elk jaar gaan honderden miljoenen gegevens verloren door gegevenslekken; de gemiddelde kosten van een lek voor een enkele onderneming stegen in 2018 tot meer dan 3,5 miljoen EUR[13]. De effecten van een cyberaanval staan vaak niet alleen en kunnen een kettingreactie op gang brengen in de gehele economie en samenleving, die miljoenen individuen treft[14].

Het onderzoek naar nagenoeg alle soorten criminaliteit heeft een digitale component. In 2019 was het gemelde aantal incidenten verdrievoudigd in vergelijking met het jaar daarvoor. Het aantal nieuwe malwareprogramma's – het vaakst gebruikte middel om een cyberaanval uit te voeren – wordt op 700 miljoen geraamd[15]. De jaarlijkse kosten van cybercriminaliteit voor de wereldeconomie werden in 2020 op 5,5 biljoen EUR geraamd, twee keer zoveel als in 2015[16]. Dit komt neer op de grootste overdracht van economische rijkdom ooit, meer nog dan de mondiale drugshandel. Voor één groot incident, de aanval met de WannaCry-ransomware in 2017, werden de kosten voor de wereldeconomie op meer dan 6,5 miljoen EUR geraamd[17].

Digitale diensten en de financiële sector worden het vaakst het doelwit van cyberaanvallen, naast de publieke sector en de verwerkende sector, en toch blijft de cyberparaatheid bij bedrijven en individuen beperkt en zijn zij zich niet goed bewust van het probleem[18]. Daarnaast is er een groot tekort aan cyberbeveiligingsvaardigheden bij de beroepsbevolking[19]. In 2019 waren er 450 cyberbeveiligingsincidenten waarbij Europese kritieke infrastructuur betrokken was, zoals financiële infrastructuur of energie-infrastructuur[20]. Gezondheidszorgorganisaties en -werkers werden tijdens de pandemie bijzonder zwaar getroffen. Nu technologie onlosmakelijk verbonden is met de fysieke wereld,

---

[10] Index van de digitale economie en maatschappij voor 2020; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/nl/data/dataset/S2249_92_2_499_ENG

[11] Persmededeling van Eurostat, "ICT security measures taken by vast majority of enterprises in the EU", 6/2020 – 13 januari 2020. "Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation"; WEF, The Global Risks Report 2020.

[12] Bron: Comparitech.

[13] Annual Cost of a Data Breach Report, 2020 Ponemon Institute, en op basis van een kwantitatieve analyse van 524 recente lekken in 17 geografische regio's en 17 bedrijfstakken; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Verslag van het Gemeenschappelijk Centrum voor onderzoek (JRC), "Cybersecurity, our digital anchor"; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Bron: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Bron: Cyence.

[18] Ondernemingen, en vooral kmo's, zijn zich ook weinig bewust van de risico's van de cyberdiefstal van bedrijfsgeheimen; PwC, Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets, 2018.

[19] Zie Enisa Threat Landscape 2020. Zie ook Verizon Data Breach Investigations Report 2020; https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

brengen cyberaanvallen het leven en welzijn van de meest kwetsbaren in gevaar[21]. Meer dan twee derde van de ondernemingen, in het bijzonder kmo's, worden als "leken" op het gebied van cyberbeveiliging beschouwd, en Europese ondernemingen worden geacht minder goed voorbereid te zijn dan ondernemingen in Azië en Amerika[22]. In Europa blijven naar schatting 291 000 functies voor cyberbeveiligingsprofessionals niet ingevuld. Het aanwerven en opleiden van cyberbeveiligingsdeskundigen is een langzaam proces dat meer cyberbeveiligingsrisico's met zich brengt voor organisaties[23].

De EU beschikt niet over voldoende collectieve situationele kennis over cyberdreigingen. De reden daarvoor is dat nationale autoriteiten niet systematisch informatie verzamelen en delen – in tegenstelling tot de particuliere sector – die de staat van de cyberbeveiliging in de EU zou kunnen helpen beoordelen. Slechts een fractie van de incidenten wordt door de lidstaten gemeld, en informatie wordt niet systematisch of volledig gedeeld[24]; cyberaanvallen zijn mogelijk maar één facet van gecoördineerde kwaadwillige aanvallen op Europese samenlevingen. De wederzijdse operationele bijstand tussen de lidstaten is momenteel beperkt, en er zijn geen operationele mechanismen tussen de lidstaten en de instellingen, agentschappen en organen van de EU voor grootschalige, grensoverschrijdende cyberincidenten of crises[25].

Het is dan ook van essentieel belang om de cyberbeveiliging te verbeteren opdat mensen innovatie, connectiviteit en automatisering zouden vertrouwen en in hun voordeel zouden gebruiken en om de grondrechten en fundamentele vrijheden, waaronder het recht op eerbiediging van de persoonlijke levenssfeer en op bescherming van persoonsgegevens, en de vrijheid van meningsuiting en van informatie te waarborgen. Cyberbeveiliging is absoluut noodzakelijk voor de netwerkconnectiviteit en het mondiale, open internet waarop de transformatie van de economie en de samenleving in de jaren 2020 gestoeld moet zijn. Zij draagt bij aan betere vaardigheden en banen, flexibelere werkplekken, efficiëntere en duurzamere landbouw en vervoer en een vlottere, billijkere toegang tot gezondheidsdiensten. Zij draagt ook bij aan de transitie naar schonere energie in het kader van de Europese Green Deal[26], via grensoverschrijdende netwerken en slimme meters en door onnodige dubbele opslag van gegevens te voorkomen. Tot slot is cyberbeveiliging van essentieel belang voor de internationale veiligheid en stabiliteit en voor de ontwikkeling van economieën, democratieën en samenlevingen wereldwijd. Regeringen, ondernemingen en individuen moeten digitale hulpmiddelen daarom op een verantwoordelijke, veiligheidsbewuste manier gebruiken. Het bewustzijn van en de aandacht voor cyberbeveiliging moeten aan de basis liggen van de digitale transformatie van dagelijkse bezigheden.

[21] Ransomware is al gebruikt om ziekenhuizen aan te vallen en gezondheidsgegevens te pakken te krijgen, bv. in Roemenië (juni 2020), Düsseldorf (september 2020) en Vastaamo (oktober 2020).
[22] PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.
[23] Agentschap van de EU voor cyberbeveiliging, Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees, en de gegevensbank voor hoger onderwijs van Enisa, december 2019.
[24] De lidstaten zijn verplicht om aan de samenwerkingsgroep een samenvattend jaarverslag over te leggen voor de kennisgevingen die zij ontvangen uit hoofde van artikel 10, lid 3, van de richtlijn inzake beveiliging van netwerk- en informatiesystemen in de Unie (Richtlijn (EU) 2016/1148).
[25] Er worden standaardwerkwijzen toegepast voor de wederzijdse bijstand tussen leden van het netwerk van CSIRT's.
[26] De Europese Green Deal, COM(2019) 640 final.

De nieuwe EU-strategie inzake cyberbeveiliging voor het digitale tijdperk vormt een cruciaal aspect van de digitale toekomst van Europa vormgeven[27], het herstelplan voor Europa van de Commissie[28], de strategie voor de veiligheidsunie 2020-2025[29], de integrale strategie voor het buitenlands en veiligheidsbeleid van de EU[30] en de strategische agenda 2019-2024 van de Europese Raad[31]. In de strategie is uiteengezet hoe de EU haar mensen, ondernemingen en instellingen zal beschermen tegen cyberdreigingen, hoe zij de internationale samenwerking zal bevorderen en hoe zij het voortouw zal nemen bij het beveiligen van een mondiaal en open internet.

II. MONDIAAL DENKEN, EUROPEES OPTREDEN

Deze strategie moet een mondiaal, open internet verzekeren, met duidelijke waarborgen om de risico's voor de veiligheid en de grondrechten en fundamentele vrijheden van de mensen in Europa aan te pakken. De strategie bouwt voort op de vorderingen die zijn gemaakt bij de vorige strategieën en bevat concrete voorstellen voor de uitrol van **drie belangrijke instrumenten – regelgevings-, investerings- en beleidsinstrumenten –** om **drie gebieden voor EU-actie aan te pakken – (1) veerkracht, technologische soevereiniteit en leiderschap, (2) de opbouw van operationele capaciteit om te voorkomen, af te schrikken en te reageren en (3) het bevorderen van een mondiale, open cyberspace.** De EU is vastberaden om deze strategie te ondersteunen, via **ongeziene investeringen in de digitale transitie van de EU gedurende de komende zeven jaar** – het investeringsniveau zou wel vier keer zo hoog kunnen zijn als voordien – als onderdeel van het nieuwe technologie- en industriebeleid en de agenda voor herstel[32].

Cyberbeveiliging moet in al die digitale investeringen worden geïntegreerd, in het bijzonder in investeringen in sleuteltechnologieën zoals kunstmatige intelligentie (KI), versleuteling en kwantumcomputing, via stimulansen, verplichtingen en benchmarks. Dit kan de groei van de Europese cyberbeveiligingssector stimuleren en de nodige zekerheid bieden om de buitengebruikstelling van oude systemen te vergemakkelijken. Het Europees Defensiefonds (EDF) zal Europese cyberdefensie-oplossingen ondersteunen, als onderdeel van de Europese technologische en industriële defensiebasis. Cyberbeveiliging is opgenomen in externe financieringsinstrumenten om onze partners te ondersteunen, met name in het instrument voor nabuurschapsbeleid, ontwikkeling en internationale samenwerking. Door misbruik van technologieën te voorkomen, kritieke infrastructuur te beschermen en de integriteit van toeleveringsketens te verzekeren, kan de EU ook voldoen aan de normen, regels en beginselen inzake verantwoordelijk staatsgedrag van de VN[33].

---

[27] De digitale toekomst van Europa vormgeven, COM(2020) 67 final.
[28] Het moment van Europa: herstel en voorbereiding voor de volgende generatie (COM(2020) 98 final).
[29] De EU-strategie voor de veiligheidsunie 2020-2025, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/nl/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#
[32] Investeringen in de gehele toeleveringsketen voor digitale technologie, die bijdragen aan de digitale transitie of aan oplossingen voor de uitdagingen die eruit voortvloeien, dienen ten minste 20 % uit te maken – 134,5 miljard EUR – van de faciliteit voor herstel en veerkracht, die 672,5 miljard EUR aan subsidies en leningen omvat. In het meerjarig financieel kader voor 2021-2027 is voorzien in EU-financiering voor cyberbeveiliging in het kader van het programma Digitaal Europa, en voor onderzoek naar cyberbeveiliging in het kader van Horizon Europa, waarbij bijzondere aandacht wordt geschonken aan steun voor kmo's. De totale financiering zou kunnen oplopen tot 2 miljard EUR, plus investeringen door de lidstaten en door het bedrijfsleven.
[33] https://undocs.org/A/70/174

1. VEERKRACHT, TECHNOLOGISCHE SOEVEREINITEIT EN LEIDERSCHAP

De kritieke infrastructuur en essentiële diensten van de EU zijn steeds meer van elkaar afhankelijk en steeds meer gedigitaliseerd. Alle op het internet aangesloten dingen in de EU, of het nu gaat om geautomatiseerde auto's, industriële controlesystemen of huishoudelijke apparaten, en de hele toeleveringsketen om die dingen aan te bieden, moeten beveiligd zijn door hun ontwerp, bestand zijn tegen cyberincidenten en snel kunnen worden gepatcht als er zwakke plekken worden ontdekt. Dat is van fundamenteel belang om de particuliere en de publieke sector in de EU de mogelijkheid te bieden om te kiezen voor de veiligste infrastructuur en diensten. De komende tien jaar krijgt de EU de kans om de leiding te nemen in de ontwikkeling van veilige technologieën in de gehele toeleveringsketen. Om de veerkracht te verzekeren en de industriële en technologische capaciteit op het gebied van cyberbeveiliging te vergroten moeten alle nodige regelgevings-, investerings- en beleidsinstrumenten worden ingezet. Cyberbeveiliging door ontwerp voor industriële processen, activiteiten en apparaten kan de risico's beperken en zou de kosten voor zowel ondernemingen als voor de ruimere samenleving kunnen drukken en zo de veerkracht kunnen vergroten.

1.1 Veerkrachtige infrastructuur en kritieke diensten

EU-regels inzake de beveiliging van netwerk- en informatiesystemen (NIS) vormen de kern van de interne markt voor cyberbeveiliging. De Commissie stelt voor om die regels te hervormen in een herziene NIS-richtlijn om de **cyberveerkracht te verhogen voor alle relevante particuliere en publieke sectoren die een belangrijke rol vervullen in de economie en de samenleving[34].** De herziening is nodig om de inconsistenties op de interne markt weg te nemen, door het toepassingsgebied, de eisen inzake beveiliging en melding van incidenten, het nationale toezicht en de handhaving en de capaciteiten van de bevoegde autoriteiten op elkaar af te stemmen.

Een hervormde NIS-richtlijn zal de basis vormen voor specifiekere regels die ook noodzakelijk zijn voor strategisch belangrijke sectoren, zoals energie, vervoer en gezondheid. Om een samenhangende aanpak te verzekeren, zoals aangekondigd in de strategie voor de veiligheidsunie 2020-2025, wordt de hervormde richtlijn samen voorgesteld met een herziening van de regelgeving inzake de veerkracht van kritieke infrastructuur[35]. Energietechnologieën met digitale componenten en de beveiliging van de bijbehorende toeleveringsketen zijn belangrijk voor de continuïteit van essentiële diensten en voor de strategische controle over kritieke energie-infrastructuur. De Commissie zal daarom maatregelen voorstellen, waaronder een "netwerkcode" tot vaststelling van regels voor cyberbeveiliging bij grensoverschrijdende elektriciteitsstromen, die tegen eind 2022 moeten worden aangenomen. De financiële sector moet eveneens zijn digitale operationele veerkracht versterken en ervoor zorgen dat alle soorten ICT-gerelateerde verstoringen en bedreigingen kunnen worden weerstaan, zoals de Commissie heeft voorgesteld[36]. Wat vervoer betreft, heeft de Commissie bepalingen inzake cyberbeveiliging[37] ingevoegd in EU-regelgeving inzake de

[34] [*verwijzing naar voorgestelde NIS-richtlijn invoegen*]
[35] [verwijzing naar *voorstel* voor een richtlijn betreffende de veerkracht van kritieke entiteiten invoegen]
[36] Voorstel voor een verordening inzake digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014, COM/2020/595 final.
[37] Uitvoeringsverordening 2019/1583 van de Commissie.

beveiliging van de luchtvaart en zal zij zich blijven inzetten om de cyberveerkracht voor alle vervoerswijzen te vergroten. Het vergroten van de cyberveerkracht van **democratische processen en instellingen** vormt een wezenlijk onderdeel van het actieplan voor Europese democratie om vrije verkiezingen, het democratische debat en het pluralisme van de media te vrijwaren en te bevorderen[38]. Tot slot zal de Commissie met het oog op de beveiliging van infrastructuur en diensten in het kader van het toekomstige ruimtevaartprogramma de strategie inzake cyberbeveiliging van Galileo uitdiepen voor de volgende generatie wereldwijde satellietnavigatiesystemen en andere nieuwe componenten van het ruimtevaartprogramma[39].

1.2 Een Europees cyberschild bouwen

Nu de connectiviteit toeneemt en cyberaanvallen steeds gesofisticeerder worden, vervullen centra voor informatie-uitwisseling en -analyse of ISAC's een waardevolle functie, ook op sectoraal niveau, doordat zij de uitwisseling van informatie over cyberdreigingen tussen diverse belanghebbenden mogelijk maken[40]. Netwerken en computersystemen moeten daarnaast voortdurend gemonitord en geanalyseerd worden om inbraken en onregelmatigheden in real-time te detecteren. Veel particuliere ondernemingen, overheidsorganisaties en nationale autoriteiten hebben daarom Computer Security Incident Response Teams (CSIRT's) en Security Operations Centres (SCO's) opgezet.

Security Operations Centres zijn van cruciaal belang om logboeken te verzamelen[41] en verdachte gebeurtenissen op de communicatienetwerken die zij monitoren te isoleren. Dat doen zij door signalen en patronen te identificeren en kennis over bedreigingen te extraheren uit de grote hoeveelheden gegevens die moeten worden beoordeeld. Zij hebben bijgedragen aan het opsporen van activiteiten van kwaadwillige uitvoerbare programma's en hebben zo cyberaanvallen helpen in te perken. Het werk dat in deze centra moet worden uitgevoerd, is erg veeleisend en moet snel gebeuren; KI en in het bijzonder technieken voor machineleren kunnen daarom belangrijke ondersteuning bieden aan de mensen die zich hiermee bezighouden[42].

De Commissie stelt voor om een **netwerk van Security Operations Centres op te bouwen in de EU[43]** en om de verbetering van de bestaande centra en de oprichting van nieuwe centra te ondersteunen. Zij zal ook de opleiding en de ontwikkeling van de vaardigheden van het personeel van deze centra ondersteunen. Zij zou op basis van een behoeftenanalyse bij de

---

[38] Mededeling over het actieplan voor Europese democratie (COM(2020) 790. In het kader van dit plan zullen het Europees samenwerkingsnetwerk voor verkiezingen en de verkiezingsnetwerken van de lidstaten de inzet van gezamenlijke teams van deskundigen ondersteunen om bedreigingen – waaronder cyberdreigingen – voor verkiezingsprocessen tegen te gaan; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_nl

[39] Dit omvat het nieuwe initiatief inzake satellietcommunicatie voor de overheid (Govsatcom) en ruimteschroot (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[41] Opdat rechtshandhavingsinstanties en het gerechtelijke apparaat deze logboeken als bewijsmateriaal kunnen gebruiken.

[42] Bron: enquête van Ponemon Institute Research, "Improving the Effectiveness of the SOC, 2019"; zie voor studies inzake het gebruik van KI in Security Operation Centres bijvoorbeeld: Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecur 2**,** 20 (2019).

[43] Er zullen nadere regelingen worden uitgewerkt inzake governance, de werkingsbeginselen en de financiering van deze centra en hoe zij een aanvulling zullen vormen op de bestaande structuren, zoals de digitale innovatiehubs.

relevante belanghebbenden, uitgevoerd met de ondersteuning van het Agentschap van de EU voor cyberbeveiliging (Enisa), meer dan 300 miljoen EUR kunnen vastleggen om publiek-private en grensoverschrijdende samenwerking te ondersteunen bij de opzet van nationale en sectorale netwerken, waarbij ook kmo's betrokken worden, op basis van passende bepalingen inzake governance, gegevensuitwisseling en beveiliging.

De lidstaten worden aangemoedigd om mee te investeren in dit project. De centra zouden de gedetecteerde signalen dan efficiënter kunnen delen en met elkaar in verband kunnen brengen en kwaliteitsvolle inlichtingen over bedreigingen tot stand kunnen brengen die met de ISAC's en de nationale autoriteiten kunnen worden gedeeld, om zo een volledigere situationele kennis te vergaren. Het zou de bedoeling zijn om in verschillende fasen zoveel mogelijk centra in de gehele EU op elkaar aan te sluiten om collectieve kennis tot stand te brengen en beste praktijken te delen. De centra zullen steun krijgen om de detectie en analyse van incidenten en de reactiesnelheid te verbeteren met behulp van geavanceerde capaciteiten op het gebied van KI en machineleren, aangevuld met infrastructuur voor supercomputing die in de EU wordt ontwikkeld door de Europese gemeenschappelijke onderneming voor high performance computing[44].

Dit netwerk zal via een duurzame samenwerking tijdig waarschuwingen over cyberbeveiligingsincidenten uitsturen naar autoriteiten en naar alle betrokken belanghebbenden, waaronder de gezamenlijke cybereenheid (zie punt 2.1). **Het zal fungeren als een echt cyberbeveiligingsschild voor de EU**, met een robuust net van uitkijktorens die potentiële bedreigingen kunnen detecteren voordat zij grootschalige schade aanrichten.

1.3 Een uitstekend beveiligde communicatie-infrastructuur

De satellietcommunicatie voor de overheid van de EU[45], een onderdeel van het ruimtevaartprogramma, zal goed beveiligde, kostenefficiënte capaciteiten voor satellietcommunicatie aanreiken om de door de EU en haar lidstaten beheerde beveiligings- en veiligheidskritieke missies en operaties te verzekeren, met inbegrip van missies en operaties die worden beheerd door nationale beveiligingsactoren en instellingen, agentschappen en organen van de EU.

De lidstaten hebben zich ertoe verbonden met de Commissie samen te werken aan de uitrol van beveiligde kwantumcommunicatie-infrastructuur (QCI) voor Europa[46]. De QCI zal overheidsinstanties een gloednieuwe manier bieden om vertrouwelijke informatie door te geven met behulp van een uitstekend beveiligde vorm van versleuteling om cyberaanvallen af te wenden, gebouwd met Europese technologie. Deze infrastructuur zal twee belangrijke componenten omvatten: de bestaande terrestrische glasvezelcommunicatienetwerken, die strategische sites op nationaal en grensoverschrijdend niveau met elkaar verbinden, en onderling verbonden satellieten in de ruimte die de gehele EU bestrijken, met inbegrip van de

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking
[45] GOVSATCOM is een onderdeel van het ruimtevaartprogramma van de Unie.
[46] De meeste lidstaten hebben de EuroQCI-verklaring ondertekend en de ontwikkeling en uitrol van infrastructuur zullen plaatsvinden in 2021-2027, met financiering uit Horizon Europa en Digitaal Europa en van het Europees Ruimteagentschap, mits passende governanceregelingen worden vastgesteld; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

overzeese gebieden[47]. Het initiatief om nieuwe, beter beveiligde vormen van versleuteling te ontwikkelen en uit te rollen en om nieuwe manieren te vinden om kritieke communicatie- en data-activa te beschermen kan de veiligheid van gevoelige informatie, en daarmee ook van kritieke infrastructuur, helpen waarborgen.

In dat verband, en met het oog op de toekomst, zal de Commissie de mogelijke uitrol van een multi-orbitaal beveiligd connectiviteitssysteem bestuderen. Dat systeem zou voortbouwen op Govsatcom en op de QCI en zou baanbrekende technologieën bevatten (kwantum, 5G, KI, edge-computing) die voldoen aan het meest restrictieve kader voor cyberbeveiliging, om diensten te ondersteunen die beveiligd zijn door hun ontwerp, waaronder betrouwbare, beveiligde en kosteneffectieve connectiviteit en versleutelde communicatie voor kritieke overheidsactiviteiten.

1.4 De volgende generatie mobiele breedbandnetwerken beveiligen

EU-burgers en -ondernemingen die geavanceerde en innovatieve toepassingen op basis van **5G en toekomstige generaties van netwerken** gebruiken, dienen te profiteren van de hoogste beveiligingsnormen. Samen met de Commissie en met de steun van Enisa hebben de lidstaten met de EU-toolbox voor 5G[48] van januari 2020 een omvattende, objectieve, op risico's gebaseerde aanpak van 5G-cyberbeveiliging tot stand gebracht die gebaseerd is op een beoordeling van mogelijke risicobeperkingsplannen en de identificatie van de meest doeltreffende maatregelen. De EU bestendigt bovendien haar capaciteiten op het gebied van 5G en wat daarna komt om afhankelijkheid van externe spelers te voorkomen en een duurzame, diverse toeleveringsketen te bevorderen.

In december 2020 heeft de Commissie een verslag over de effecten van de aanbeveling van 26 maart 2019 inzake de cyberbeveiliging van 5G-netwerken gepubliceerd[49]. Daaruit bleek dat er aanzienlijke vorderingen waren gemaakt sinds de toolbox werd overeengekomen en dat de meeste lidstaten goed op weg zijn om een aanzienlijk deel van de uitvoering van de toolbox in de nabije toekomst te voltooien, zij het met enige verschillen en resterende lacunes zoals reeds vastgesteld in het voortgangsverslag dat in juli 2020 werd gepubliceerd[50].

In oktober 2020 heeft de Europese Raad de EU en de lidstaten verzocht om "ten volle gebruik te maken van de toolbox voor 5G-cyberbeveiliging" en "voor essentiële voorzieningen die in de gecoördineerde EU-risicobeoordelingen zijn aangemerkt als kritiek en gevoelig, de

[47] De ontwikkeling van een ruimtecomponent is van essentieel belang om punt-naar-puntverbindingen over lange afstand (>1000 km) tot stand te brengen die niet kunnen worden ondersteund met grondinfrastructuur. Door de eigenschappen van de kwantummechanica te benutten zal de QCI de partijen in eerste instantie in staat stellen om op veilige wijze willekeurige geheime sleutels te delen die kunnen worden gebruikt om boodschappen te versleutelen en te ontsleutelen. Er zal eveneens test- en conformiteitsinfrastructuur worden uitgerold om na te gaan of Europese kwantumcommunicatie-apparaten en -systemen in overeenstemming zijn met de QCI-infrastructuur en om hun certificering en validering te controleren alvorens zij in de QCI worden geïntegreerd. De QCI zal zo worden ontworpen dat zij aanvullende toepassingen ondersteunt naarmate zij de nodige technologische maturiteit bereiken. Het huidige proefproject OpenQKD (https://openqkd.eu/) is een voorloper van die test- en conformiteitsinfrastructuur.

[48] Mededeling over de uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox (COM(2020) 50).

[49] Verslag van de Commissie over het effect van Aanbeveling van de Commissie van 26 maart 2019 betreffende de cyberbeveiliging van 5G-netwerken, 15 december 2020.

[50] Verslag van de NIS-samenwerkingsgroep over de uitvoering van de toolbox van 24 juli 2020.

desbetreffende beperkingen toe te passen op aanbieders met een hoog risico, op basis van gemeenschappelijke objectieve criteria"[51].

Met het oog op de toekomst dienen de EU en haar lidstaten ervoor te zorgen dat de geïdentificeerde risico's op passende en gecoördineerde wijze zijn beperkt, in het bijzonder met betrekking tot de doelstelling om de blootstelling aan aanbieders met een hoog risico tot een minimum te beperken en afhankelijkheid van die aanbieders op nationaal en Unieniveau te voorkomen, en dat alle nieuwe belangrijke ontwikkelingen of risico's in aanmerking worden genomen. De lidstaten wordt verzocht de toolbox ten volle te gebruiken bij hun investeringen in digitale capaciteiten en connectiviteit.

Op basis van het verslag over de effecten van de aanbeveling van 2019 spoort de Commissie de lidstaten ertoe aan om de uitvoering van de belangrijkste maatregelen van de toolbox sneller af te ronden, tegen het tweede kwartaal van 2021. Zij verzoekt de lidstaten eveneens om samen te blijven toezien op de gemaakte vorderingen en om de verdere onderlinge afstemming van benaderingen te verzekeren. Op EU-niveau zullen drie belangrijke doelstellingen worden nagestreefd om dat proces te ondersteunen: de risicobeperkingsbenaderingen in de gehele EU meer gelijklopend maken, een voortdurende uitwisseling van kennis en capaciteitsopbouw ondersteunen en de veerkracht van de toeleveringsketen en andere strategische beveiligingsdoelstellingen van de EU bevorderen. Concrete maatregelen met betrekking tot deze kerndoelstellingen zijn beschreven in het desbetreffende aanhangsel bij deze mededeling.

De Commissie zal nauw blijven samenwerken met de lidstaten om deze doelstellingen en maatregelen in de praktijk te brengen, met de steun van Enisa (zie bijlage).

De EU-toolbox voor 5G heeft bovendien belangstelling gewekt in niet-EU-landen die momenteel hun eigen benaderingen ontwikkelen om hun communicatienetwerken te beveiligen. De diensten van de Commissie zijn klaar om samen met de Europese Dienst voor extern optreden en het netwerk van EU-delegaties op verzoek aanvullende informatie over hun omvattende, objectieve, op risico's gebaseerde aanpak te verstrekken aan autoriteiten overal ter wereld.

1.5 Een internet van beveiligde dingen

Elk verbonden ding heeft zwakke plekken die kunnen worden uitgebuit, met mogelijk grootschalige gevolgen. De internemarktregels bevatten waarborgen tegen onbeveiligde producten en diensten. De Commissie werkt al aan het verzekeren van **transparante beveiligingsoplossingen en certificaten in het kader van de cyberbeveiligingsverordening** en aan stimulansen voor veilige producten en diensten, zonder toegevingen te doen op het vlak van prestaties[52]. Zij zal in het eerste kwartaal van

[51] EUCO 13/20, buitengewone bijeenkomst van de Europese Raad (1 en 2 oktober 2020) – Conclusies.

[52] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening). De cyberbeveiligingsverordening bevordert ICT-certificering op EU-niveau, met een Europees kader voor cyberbeveiligingscertificering voor de vaststelling van vrijwillige Europese cyberbeveiligingscertificeringsregelingen teneinde een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de Unie te waarborgen, alsmede om versnippering van de interne markt wat betreft cyberbeveiligingscertificeringsregelingen in de Unie te vermijden. Tegelijkertijd zijn "ratingbedrijven" voor cyberbeveiliging gewoonlijk buiten de EU gevestigd en is er weinig transparantie en toezicht; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

2021 haar eerste voortschrijdende werkprogramma van de Unie vaststellen (dat ten minste om de drie jaar moet worden bijgewerkt) om de sector, de nationale autoriteiten en de normalisatie-instanties in staat te stellen zich voor te bereiden op toekomstige Europese certificeringsregelingen voor cyberbeveiliging[53]. Naarmate het internet der dingen zich uitbreidt, is het noodzakelijk om afdwingbare regels te versterken, zowel om de algemene veerkracht te verzekeren als om cyberbeveiliging te stimuleren.

De Commissie zal een omvattende aanpak overwegen, met eventuele **nieuwe horizontale regels om de cyberbeveiliging te verbeteren voor alle verbonden producten en gerelateerde diensten die op de interne markt in de handel worden gebracht**[54]. Dergelijke regels zouden een **nieuwe zorgvuldigheidsplicht voor de fabrikanten van verbonden apparaten** kunnen omvatten om zwakke plekken in software aan te pakken, onder meer door software- en beveiligingsupdates te blijven aanbieden en ervoor te zorgen dat persoonsgegevens en andere gevoelige gegevens aan het einde van de levensduur worden verwijderd. Die regels zouden het initiatief inzake "het recht om verouderde software te actualiseren" in het actieplan voor een circulaire economie kracht bijzetten en een aanvulling vormen op lopende maatregelen voor specifieke soorten producten, zoals verplichte vereisten voor toegang tot de markt voor bepaalde draadloze producten (via de vaststelling van een gedelegeerde handeling uit hoofde van de richtlijn betreffende radioapparatuur[55]) en de doelstelling om vanaf juli 2022 cyberbeveiligingsvoorschriften voor motorvoertuigen in te voeren voor alle nieuwe voertuigtypen[56]. Zij zouden bovendien voortbouwen op de voorgestelde herziening van de regels inzake de algemene productveiligheid, waarin cyberbeveiligingsaspecten niet rechtstreeks aan bod komen[57].

1.6 Meer beveiliging van het mondiale internet

Een reeks kernprotocollen en ondersteunende infrastructuur verzekert de werking en integriteit van het internet wereldwijd[58]. Tot die reeks behoren onder meer het DNS en zijn hiërarchische, gedelegeerde systeem van zones, te beginnen met de rootzone (bovenaan in de hiërarchie) en de 13 DNS-rootservers[59] waarvan het wereldwijde web afhankelijk is. De Commissie is voornemens **een noodplan uit te werken, ondersteund met EU-financiering, voor de omgang met extreme scenario's die de integriteit en stabiliteit van het wereldwijde DNS-rootsysteem aantasten**. Zij zal samenwerken met Enisa, de lidstaten, de

[53] Vereist uit hoofde van artikel 47, lid 5, van de cyberbeveiligingsverordening.
[54] In de Raadsconclusies wordt verzocht om horizontale maatregelen inzake de cyberbeveiliging van verbonden apparaten; 13629/20, 2 december 2020.
[55] Richtlijn 2014/53/EU.
[56] Dit volgt uit het VN-reglement dat in juni 2020 is goedgekeurd; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
[57] Herziening van de huidige regels inzake de algemene productveiligheid (Richtlijn 2001/95/EG); er zijn ook aangepaste regels inzake de aansprakelijkheid van producenten in de digitale context voorgesteld binnen de werkingssfeer van het EU-rechtskader inzake aansprakelijkheid.
[58] "De openbare kern van het open internet, namelijk de belangrijkste protocollen en infrastructuur, die een mondiaal publiek goed zijn, vormt de essentiële functionaliteit van het internet als geheel en ondersteunt de normale werking ervan. Enisa dient de beveiliging van de openbare kern van het open internet en de stabiliteit van zijn werking te ondersteunen, met inbegrip van, maar niet beperkt tot, cruciale protocollen (met name DNS, BGP en IPv6), de werking van het domeinnaamsysteem (waaronder de werking van alle topniveaudomeinen) en de werking van de 'root zone'"; overweging 23 van de cyberbeveiligingsverordening.
[59] https://www.iana.org/domains/root/servers

twee exploitanten van DNS-rootservers in de EU[60] en de multistakeholdergemeenschap om te beoordelen welke rol deze exploitanten spelen in het waarborgen van een internet dat in alle omstandigheden wereldwijd toegankelijk blijft.

Opdat een client toegang zou krijgen tot een bepaalde bron onder een bepaalde domeinnaam op het internet, moet het verzoek van die client (gewoonlijk een uniform resource locator of URL) worden vertaald in een IP-adres (een proces dat "resolving" wordt genoemd), onder verwijzing naar DNS-naamservers. Mensen en organisaties in de EU zijn echter steeds meer afhankelijk van een klein aantal openbare DNS-resolvers die worden geëxploiteerd door entiteiten buiten de EU. Die consolidering van DNS-resolutie in handen van een paar bedrijven[61] maakt het resolutieproces zelf kwetsbaar in geval van belangrijke gebeurtenissen die een grote aanbieder treffen en maakt het moeilijker voor de EU-autoriteiten om mogelijke kwaadwillige cyberaanvallen en grote geopolitieke en technische incidenten aan te pakken[62].

Om de beveiligingsproblemen waarmee marktconcentratie gepaard gaat te beperken, zal de Commissie relevante belanghebbenden, waaronder EU-bedrijven, internetaanbieders en browserleveranciers, aanmoedigen om een strategie voor diversificatie van de DNS-resolutie aan te nemen. De Commissie is eveneens voornemens bij te dragen aan beveiligde internetconnectiviteit door de ontwikkeling van een openbare **Europese dienst voor DNS-resolutie** te ondersteunen**.** Dit "DNS4EU"-initiatief zal een alternatieve, Europese dienst aanbieden om toegang te krijgen tot het mondiale internet. DNS4EU zal transparant zijn, in overeenstemming zijn met de meest recente normen en regels inzake beveiliging, gegevensbescherming en privacy door ontwerp en privacy door standaardinstellingen, en deel uitmaken van de Europese Industriële Alliantie voor gegevens en cloud[63].

De Commissie zal voorts samen met de lidstaten en de sector **de toepassing versnellen van essentiële internetstandaarden, waaronder IPv6**[64] **en gevestigde standaarden voor internetbeveiliging, en goede praktijken voor DNS, routering en e-mailbeveiliging**[65], eventueel door middel van regelgevingsmaatregelen zoals een Europese uitdovingsclausule voor IPv4 om de markt aan te sturen indien er onvoldoende vooruitgang wordt gemaakt met de toepassing van de desbetreffende standaarden en praktijken. De EU dient (bijvoorbeeld in het kader van de EU-Afrikastrategie[66]) de uitvoering van die standaarden in partnerlanden te bevorderen als manier om de ontwikkeling van het mondiale, open internet te ondersteunen en gesloten, op controles gebaseerde internetmodellen tegen te gaan. Tot slot zal de Commissie nagaan of er behoefte is aan een mechanisme voor een meer systematische

[60] De door Netnod geëxploiteerde i.root-servers in Zweden, en de door RIPE NCC geëxploiteerde k.root-servers in Nederland.
[61] Consolidation in the DNS resolver market – how much, how fast how dangerous? (), Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services ( ).
[62] Er zijn ook aanwijzingen dat DNS-gegevens kunnen worden gebruikt voor het opstellen van profielen, hetgeen gevolgen heeft voor het recht op de bescherming van de persoonlijke levenssfeer en het recht op gegevensbescherming.
[63] Gezamenlijke verklaring: "Building the next generation cloud for businesses and the public sector in the EU"; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe
[64] De uitrol van IPv6 staat ondertussen al verder, nu er steeds minder IPv4-adressen overblijven en de kosten voor dergelijke adressen toenemen. De uitrol van IPv6 binnen de EU is echter ongelijk.
[65] Het gaat bijvoorbeeld om DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE en normen en goede praktijken op het gebied van routering, zoals de Mutually Agreed Norms for Routing Security (MANRS).
[66] Gezamenlijke mededeling "Naar een brede strategie met Afrika", 9.3.2020 JOIN(2020) 4 final.

monitoring en verzameling van gebundelde gegevens over het internetverkeer en aan advies over mogelijke verstoringen[67].

1.7 Een versterkte aanwezigheid in de toeleveringsketen voor technologie

Met de geplande financiële ondersteuning voor een cyberbeveiligde digitale transformatie gedurende het meerjarig financieel kader 2021-2027 heeft de EU een unieke kans om haar middelen te bundelen om een impuls te geven aan haar industriestrategie[68] en haar leiderschap op het gebied van digitale technologieën en cyberbeveiliging in de gehele digitale toeleveringsketen (met inbegrip van gegevens en cloud, processortechnologieën van de volgende generatie, uitstekend beveiligde connectiviteit en 6G-netwerken), in overeenstemming met haar waarden en prioriteiten. Overheidsingrijpen dient te berusten op de instrumenten van het regelgevingskader voor overheidsopdrachten van de EU en de belangrijke projecten van gemeenschappelijk Europees belang. Voorts kan ingrijpen door de overheid particuliere investeringen ontgrendelen via publiek-private partnerschappen (onder meer door voort te bouwen op de ervaringen van het contractuele publiek-private partnerschap voor cyberbeveiliging en de uitvoering ervan via de Europese organisatie voor cyberbeveiliging), durfkapitaal ter ondersteuning van kmo's of industriële allianties en strategieën inzake technologiecapaciteiten.

Er zal ook bijzondere aandacht worden geschonken aan het instrument voor technische ondersteuning[69] en aan het best mogelijke gebruik van de meest recente cyberbeveiligingstools door kmo's – in het bijzonder diegene die niet binnen het toepassingsgebied van de herziene NIS-richtlijn vallen –, onder meer via specifieke activiteiten in het kader van de digitale innovatiehubs in het programma Digitaal Europa. Het doel is een soortgelijk bedrag aan investeringen door de lidstaten los te maken, dat moet worden bijgepast door de sector in het kader van een mede door de lidstaten bestuurd partnerschap binnen het voorgestelde **kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en netwerk van nationale coördinatiecentra (CCCN)**. Het CCCN dient, met input van de sector en de academische wereld, een sleutelrol te spelen in de ontwikkeling van de technologische soevereiniteit van de EU op het gebied van cyberbeveiliging, door de nodige capaciteit op te bouwen om gevoelige infrastructuur zoals 5G te beveiligen en de afhankelijkheid van andere regio's ter wereld voor de meest cruciale technologieën te beperken.

De Commissie is van plan om, mogelijk binnen het CCCN, de ontwikkeling van een gericht masterprogramma inzake cyberbeveiliging te ondersteunen en bij te dragen aan een gemeenschappelijk Europees stappenplan voor onderzoek en innovatie op het gebied van cyberbeveiliging na 2020. Investeringen via het CCCN zouden ook voortbouwen op de samenwerking op het gebied van onderzoek en ontwikkeling via netwerken van kenniscentra voor cyberbeveiliging, door de beste onderzoeksteams in Europa in contact te brengen met de sector om gemeenschappelijke onderzoeksagenda's te ontwerpen en uit te voeren, in overeenstemming met het stappenplan van de Europese organisatie voor cyberbeveiliging[70].

---

[67] Een dergelijk "waarnemingscentrum voor het internet" zou binnen de werkingssfeer van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging kunnen vallen; Voorstel voor een verordening 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.

[68] Mededeling over een nieuwe industriestrategie voor Europa, COM(2020) 102 final.

[69] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=COM:2020:0409:FIN

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies

De Commissie zal blijven vertrouwen op de onderzoekswerkzaamheden van Enisa en Europol en zal, in het kader van Horizon Europa, ook steun blijven verlenen aan individuele internetinnovatoren die beveiligde communicatietechnologieën ontwikkelen die de privacy ten goede komen en die gebaseerd zijn op open-source software en hardware, zoals momenteel al gebeurt in het kader van het initiatief voor het internet van de volgende generatie.

1.8 Een Europese beroepsbevolking met cybervaardigheden

De inspanningen van de EU om de vaardigheden van de beroepsbevolking bij te spijkeren, het beste cyberbeveiligingstalent te ontwikkelen, aan te trekken en te behouden en te investeren in onderzoek en innovatie van wereldklasse vormen een belangrijke component van de bescherming tegen cyberdreigingen in het algemeen. Dit gebied biedt een enorm potentieel. Er moet dan ook bijzondere aandacht worden geschonken aan het ontwikkelen, aantrekken en behouden van meer divers talent. Het bijgewerkte actieplan voor digitaal onderwijs zal het bewustzijn inzake cyberbeveiliging vergroten bij individuen, in het bijzonder bij kinderen en jongeren, en bij organisaties, in het bijzonder bij kmo's[71]. Het zal ook de participatie van vrouwen in het onderwijs in STEM-disciplines (wetenschap, technologie, engineering en wiskunde) en in ICT-banen aanmoedigen, alsook bij- en omscholing om digitale vaardigheden te verwerven. Daarnaast zal de Commissie samen met het Bureau voor intellectuele eigendom van de EU bij Europol, Enisa, de lidstaten en de particuliere sector bewustmakingstools en -richtsnoeren ontwikkelen om de veerkracht van EU-bedrijven **in de context van door het internet mogelijk gemaakte diefstal van intellectuele eigendom** te vergroten[72].

Onderwijs – met inbegrip van beroepsonderwijs en -opleiding (VET), bewustmaking en oefeningen – dient ook de vaardigheden op het gebied van cyberbeveiliging en cyberdefensie op EU-niveau verder te vergroten. Daartoe dienen de betrokken EU-actoren, zoals Enisa, het Europees Defensieagentschap (EDA) en de Europese Veiligheids- en defensieacademie (EVDA)[73], synergieën na te streven tussen hun respectieve werkzaamheden.

Strategische initiatieven

De EU dient te zorgen voor:

- de goedkeuring van de herziene NIS-richtlijn;
- regelgevingsmaatregelen voor een internet van beveiligde dingen;
- 4,5 miljard EUR aan publieke en particuliere investering in de periode van 2021-2027, via de investering door het CCCN in cyberbeveiliging (met name via het programma Digitaal Europa, Horizon Europa en de herstelfaciliteit);
- een EU-netwerk van Security Operation Centres met KI-ondersteuning en een uitstekend beveiligde communicatie-infrastructuur die gebruikmaakt van kwantumtechnologieën;
- de grootschalige toepassing van cyberbeveiligingstechnologieën via specifieke

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_nl
[72] https://ec.europa.eu/commission/presscorner/detail/nl/IP_20_2187
[73] Via het platform voor onderwijs, opleiding, evaluatie en oefeningen op cybergebied (ETEE).

ondersteuning voor kmo's via de digitale innovatiehubs;

- de ontwikkeling van een EU-dienst voor DNS-resolutie, als veilig en open alternatief voor EU-burgers, -bedrijven en -overheidsdiensten om toegang te krijgen tot het internet, en
- de voltooiing van de uitvoering van de toolbox voor 5G-cyberbeveiliging tegen het tweede kwartaal van 2021 (zie bijlage).

2. OPBOUWEN VAN OPERATIONELE CAPACITEIT OM TE VOORKOMEN, TEGEN TE GAAN EN TE REAGEREN

Cyberincidenten, hetzij per ongeluk, hetzij opzettelijk door toedoen van criminelen, statelijke en andere niet-statelijke actoren, kunnen enorme schade aanrichten. De omvang en complexiteit ervan, waarbij vaak diensten van derden, hardware en software worden geëxploiteerd om een uiteindelijk doelwit te treffen, maken het moeilijk tegengewicht te bieden voor de collectieve dreigingsomgeving van de EU zonder het systematisch en allesomvattend delen van informatie en samenwerken aan een gezamenlijk antwoord. **Via de volledige uitvoering van regelgevingshulpmiddelen, mobilisatie en samenwerking** streeft de EU ernaar de lidstaten te ondersteunen bij de verdediging van hun burgers, alsook hun economische belangen en belangen van nationale veiligheid, met volledige naleving van de grondrechten en fundamentele vrijheden en de rechtsstaat. Verscheidene gemeenschappen, die bestaan uit netwerken, instellingen, organen en agentschappen van de EU, evenals autoriteiten van lidstaten, zijn verantwoordelijk voor het voorkomen, ontmoedigen en tegengaan van en reageren op cyberdreigingen, door hun respectieve instrumenten en initiatieven te gebruiken[74]. Deze gemeenschappen omvatten: (i) NIS-autoriteiten, zoals CSIRT's en disaster response; (ii) rechtshandhavings- en gerechtelijke instanties; (iii) cyberdiplomatie; en (iv) cyberdefensie.

2.1 Een gezamenlijke cybereenheid

Een gezamenlijke cybereenheid zou dienst doen als een virtueel en fysiek platform voor samenwerking voor de verschillende cyberbeveiligingsgemeenschappen in de EU, met de nadruk op operationele en technische coördinatie tegen grote grensoverschrijdende cyberincidenten en -bedreigingen.

De gezamenlijke cybereenheid zou een belangrijke stap voorwaarts zijn richting de voltooiing van het **Europees kader voor crisisbeheer inzake cyberbeveiliging**. Zoals uiteengezet in de politieke richtsnoeren van de voorzitter van de Commissie[75] moet de eenheid de lidstaten en instellingen, organen en agentschappen van de EU in staat stellen de bestaande structuren, hulpbronnen en capaciteiten ten volle te benutten en een "**behoefte aan**

[74] Waaronder steun van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) bij operationele samenwerking en crisisbeheer; het netwerk van CSIRT's; het Cyber Crises Liaison Organisation Network (CyCLONe, wordt EU-CyCLONe zoals voorgesteld krachtens de herziene NIS-richtlijn); de NIS-samenwerkingsgroep; "rescEU"; het Europees Centrum voor de bestrijding van cybercriminaliteit en de Joint Cybercrime Action Task Force binnen Europol en het Law Enforcement Emergency Response Protocol; het inlichtingen- en situatiecentrum van de Europese Unie (EU INTCEN) en het "instrumentarium voor cyberdiplomatie"; de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC); de cyberprojecten onder de permanente gestructureerde samenwerking (PESCO), met name de "Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity" (CRRT).

[75] "Een Unie die streeft naar meer: Mijn agenda voor Europa", Politieke richtsnoeren voor de volgende Europese Commissie 2019-2024 volgens kandidaat-voorzitter van de Europese Commissie Ursula von der Leyen.

delen"-mentaliteit te bevorderen. Zij zou de middelen verstrekken om de vooruitgang te consolideren die tot nog toe is geboekt bij de uitvoering van de Aanbeveling van 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises ("blauwdruk")[76]. Het zou ook de kans bieden om de samenwerking rond de architectuur van de blauwdruk verder te versterken en de geboekte vooruitgang te benutten, met name binnen de NIS-samenwerkingsgroep en het CyCLONe-netwerk.

Hierdoor kunnen **twee belangrijke hiaten** worden aangepakt die momenteel de kwetsbaarheden vergroten en inefficiënties veroorzaken in de reactie op grensoverschrijdende dreigingen en incidenten die de Unie treffen. Ten eerste hebben burgerlijke, diplomatieke, rechtshandhavings- en cyberbeveiligings**gemeenschappen** nog geen gezamenlijke ruimte om een gestructureerde samenwerking te stimuleren en een operationele en technische samenwerking te vergemakkelijken. Ten tweede konden de relevante belanghebbenden op het gebied van cyberbeveiliging het volledige **potentieel** van operationele samenwerking en wederzijdse bijstand binnen bestaande netwerken en gemeenschappen nog niet benutten. Dit omvat de afwezigheid van een platform dat operationele samenwerking met de privésector mogelijk maakt. De eenheid moet de coördinatie verbeteren en versnellen en de EU de kans geven het hoofd te bieden aan en te reageren op grootschalige cyberincidenten en -crises.

De gezamenlijke cybereenheid zou geen bijkomend, op zichzelf staand orgaan zijn, noch zou het invloed hebben op de bevoegdheden van nationale cyberbeveiligingsautoriteiten of EU-deelnemers. De eenheid zou eerder dienst doen als een backstop waarbij de deelnemers steun en expertise bij elkaar kunnen vinden, vooral in gevallen waarin verscheidene cybergemeenschappen nauwer moeten samenwerken. Tegelijkertijd blijkt uit recente gebeurtenissen dat de EU haar ambitie- en paraatheidsniveau moet vergroten om het landschap en de realiteiten van cyberdreigingen het hoofd te kunnen bieden. Als onderdeel van hun bijdrage aan de gezamenlijke cybereenheid zullen de EU-actoren (de Commissie alsook de agentschappen en organen van de EU) dan ook klaar zijn om hun middelen en capaciteiten aanzienlijk op te drijven, om hun paraatheid en veerkracht te vergroten.

De gezamenlijke cybereenheid zou drie belangrijke doelstellingen vervullen. Ten eerste zou zij **paraatheid** in alle cyberbeveiligingsgemeenschappen verzekeren; ten tweede zou zij via het delen van informatie zorgen voor een permanent situationeel **bewustzijn**; ten derde zou zij een gecoördineerde **reactie** en een gecoördineerd herstel versterken. Om deze doelstellingen te behalen moet de eenheid verder bouwen op welomschreven **blokken en doelstellingen**, zoals het waarborgen van **het veilig en snel delen van informatie**, het verbeteren van de **samenwerking** tussen de deelnemers, zoals interactie tussen de lidstaten en relevante EU-entiteiten, de totstandbrenging van gestructureerde **partnerschappen met een vertrouwde industriebasis** en het vergemakkelijken van een gestructureerde benadering voor **samenwerking met externe partners**. Daartoe zou de eenheid, op basis van in kaart gebrachte beschikbare bekwaamheden op nationaal en EU-niveau, de ontwikkeling van een samenwerkingskader kunnen vergemakkelijken.

Om van de gezamenlijke cybereenheid het hart van de operationele samenwerking inzake cyberbeveiliging van de EU te maken, zal de Commissie samenwerken met de lidstaten en met de relevante instellingen, organen en agentschappen van de EU, waaronder Enisa, CERT-EU en Europol, om een **incrementele en inclusieve benadering** te bevorderen, waarbij de bevoegdheden en mandaten van alle betrokkenen volledig worden gerespecteerd.

[76]Aanbeveling ("blauwdruk") C(2017) 6100 final van 13.9.2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.

Overeenkomstig deze benadering zou de eenheid kunnen bijdragen aan een nauwere samenwerking tussen de onderdelen van een specifieke cybergemeenschap, als die onderdelen dat noodzakelijk achten.

Er worden vier belangrijke stappen voorgesteld om de gezamenlijke cybereenheid tot stand te brengen:

- *definiëren*, door de beschikbare bekwaamheden op nationaal en EU-niveau in kaart te brengen;
- *voorbereiden*, door een kader voor gestructureerde samenwerking en bijstand tot stand te brengen;
- *ontplooien*, door het kader ten uitvoer te leggen met gebruikmaking van de middelen die de deelnemers ter beschikking stellen zodat de gezamenlijke cybereenheid operationeel wordt;
- *uitbreiden*, door een capaciteit voor gecoördineerde reactie te versterken met inbreng van de industrie en van de partners.

Verder bouwend op de resultaten van het overleg met de lidstaten en met de instellingen, organen en agentschappen van de EU[77] zal de Commissie, met betrokkenheid van de Hoge Vertegenwoordiger, overeenkomstig zijn bevoegdheden, tegen februari 2021 het proces, de mijlpalen en de planning voorstellen voor het **definiëren, voorbereiden, ontplooien en uitbreiden van de gezamenlijke cybereenheid**.

2.2 Cybercriminaliteit aanpakken

Onze afhankelijkheid van onlinetools heeft het aanvalsoppervlak voor cybercriminelen exponentieel doen toenemen en heeft geleid tot een situatie waarin het onderzoek naar zowat alle soorten criminaliteit een digitale component bevat. Bovendien worden cruciale onderdelen van onze samenleving bedreigd door cyberactoren en door mensen die cybertools gebruiken om hun illegale handelingen te plannen en uit te voeren. Er zijn dan ook nauwe banden met het algemene veiligheidsbeleid van de EU; dat komt tot uiting in de cyberelementen in haar strategie voor de veiligheidsunie van 2020 en in de agenda voor terrorismebestrijding van de EU[78].

Cybercriminaliteit doeltreffend aanpakken is een cruciale factor bij het verzekeren van cyberbeveiliging: afschrikking kan niet worden bereikt via veerkracht alleen: overtreders moeten ook geïdentificeerd en vervolgd worden. Het is dan ook essentieel om de samenwerking en uitwisseling tussen cyberbeveiligingsactoren en rechtshandhaving te stimuleren. Daarom hebben Europol en Enisa op EU-niveau reeds een sterke samenwerking opgebouwd waar zij gezamenlijke conferenties en workshops hebben georganiseerd. Zij hebben ook gezamenlijke verslagen overgelegd aan de Commissie, de lidstaten en andere belanghebbenden inzake cyberbeveiligingsbedreigingen en technologische uitdagingen. De Commissie zal deze geïntegreerde benadering blijven ondersteunen om een samenhangende

[77] Overleg van lidstaten (ook tijdens de Blue OLEx20-oefening waarbij de hoofden van nationale cyberbeveiligingsautoriteiten samenkwamen), instellingen, organen en agentschappen van de EU dat plaatsvond tussen juli en november 2020.
[78] Mededeling A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9.12.2020, COM(2020) 795 final.

en doeltreffende reactie te verzekeren, die gebaseerd is op een allesomvattend informatiebeeld.

Eén belangrijk element van die reactie is dat de EU en de nationale autoriteiten de capaciteit van de rechtshandhaving moeten uitbreiden om cybercriminaliteit te onderzoeken. Daarbij moet zij de grondrechten volledig respecteren en het vereiste evenwicht tussen verscheidene rechten en belangen nastreven. De EU moet cybercriminaliteit kunnen aanpakken via volledig uitgevoerde wetgeving die geschikt is voor haar doel. Daarbij moet de nadruk vooral liggen op de bestrijding van seksueel misbruik van kinderen online en op digitaal onderzoek, waaronder criminaliteit op het "darknet". De rechtshandhaving moet volledig toegerust zijn voor digitaal onderzoek. Daarom zal de Commissie een actieplan naar voren schuiven om de digitale capaciteit voor rechtshandhavingsinstanties te verbeteren, door hen de nodige vaardigheden en hulpmiddelen aan te reiken. Daarnaast zal Europol zijn rol als expertisecentrum verder uitbouwen om nationale rechtshandhavingsinstanties te ondersteunen bij de bestrijding van gedigitaliseerde en digitale criminaliteit, door bij te dragen aan de definitie van gezamenlijke forensische normen (via het innovatielab en de innovatiehub van Europol). Voor al deze activiteiten is een gepaste opname door de lidstaten nodig, die worden aangemoedigd om gebruik te maken van de nationale programma's van het Fonds voor interne veiligheid en om projecten voor te stellen als reactie op oproepen tot het indienen van voorstellen als onderdeel van de thematische faciliteit.

De Commissie zal alle gepaste middelen gebruiken, waaronder inbreukprocedures, om ervoor te zorgen dat de richtlijn van 2013 over aanvallen op informatiesystemen[79] volledig wordt omgezet en uitgevoerd, met inbegrip van de verstrekking van statistieken door de lidstaten. Hierdoor zal het misbruik van domeinnamen beter kunnen worden voorkomen, inclusief, indien gepast, voor de verspreiding van illegale inhoud, en wordt de beschikbaarheid van correcte registratiegegevens nagestreefd door te blijven samenwerken met de Internet Corporation for Assigned Names and Numbers (ICANN) en andere belanghebbenden in het systeem van internetgovernance, met name via de werkgroep openbare veiligheid van het Governmental Advisory Committee van de ICANN. Daarom wordt in het voorstel in de herziene NIS-richtlijn gestreefd naar het bijhouden van correcte en volledige databanken van domeinnamen en registratiegegevens, of "WHOIS-gegevens", en naar het verstrekken van wettelijke toegang tot dergelijke gegevens omdat ze essentieel zijn om de veiligheid, stabiliteit en veerkracht van de DNS te verzekeren.

De Commissie zal ook blijven verder werken om gepaste kanalen te verstrekken en regels te verduidelijken om grensoverschrijdende toegang te verkrijgen tot elektronisch bewijsmateriaal voor strafrechtelijk onderzoek (dat is nodig in 85 % van de onderzoeken; 65 % van het totale aantal verzoeken gaat naar providers die in een andere jurisdictie gevestigd zijn), door de goedkeuring en daaropvolgende uitvoering van het "pakket e-bewijsmateriaal" en praktische maatregelen te vergemakkelijken[80]. De snelle goedkeuring door het Europees Parlement en de Raad van de voorstellen inzake elektronisch bewijsmateriaal is van groot belang zodat rechtshandhavers over een efficiënt instrument

[79] Richtlijn 2013/40/EU over aanvallen op informatiesystemen.

[80] COM(2018) 225 en 226; C(2020) 2779 final. Met name het SIRIUS-project kreeg onlangs bijkomende financiering krachtens het partnerschapsinstrument om kanalen te verbeteren om wettelijke grensoverschrijdende toegang te krijgen tot elektronisch bewijsmateriaal voor strafrechtelijk onderzoek (dat is nodig in 85 % van de onderzoeken; 65 % van het totale aantal verzoeken gaat naar providers die in een andere jurisdictie gevestigd zijn), en om regels vast te stellen op internationaal niveau.

kunnen beschikken. Aangezien elektronisch bewijsmateriaal leesbaar moet zijn, zal de Commissie verder werken aan de ondersteuning van de rechtshandhavingscapaciteit op het gebied van digitaal onderzoek. Daarbij hoort ook omgaan met encryptie wanneer dit opduikt tijdens strafrechtelijk onderzoek, terwijl zij haar functie inzake de bescherming van de grondrechten en cyberbeveiliging ten volle behoudt.

2.3 Instrumentarium voor cyberdiplomatie van de EU

De EU gebruikt haar **instrumentarium voor cyberdiplomatie**[81] om kwaadaardige cyberactiviteiten te voorkomen, te ontmoedigen, tegen te gaan en erop te reageren. Na de invoering van het wettelijk kader voor gerichte beperkende maatregelen tegen cyberaanvallen in mei 2019[82] stelde de EU een lijst op van zes personen en drie entiteiten die verantwoordelijk waren voor of betrokken waren bij cyberaanvallen waarvan de EU en haar lidstaten het doelwit waren onder het regime in juli 2020[83]. In oktober 2020 werden nog eens twee personen en één orgaan in de lijst opgenomen[84]. Kwaadaardige cyberactiviteiten, waaronder smeulende, moeten worden aangepakt door een doeltreffende en allesomvattende gezamenlijke diplomatieke reactie van de EU; daarbij moet het volledige arsenaal aan maatregelen die op EU-niveau beschikbaar zijn, worden gebruikt.

Voor een snelle en doeltreffende gezamenlijke diplomatieke reactie van de EU is een solide, gedeeld situationeel bewustzijn nodig. Ook moet het mogelijk zijn snel een gezamenlijk standpunt van de EU voor te bereiden. De Hoge Vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid zal de oprichting van een **EU-werkgroep voor cyberintelligentie van de lidstaten** die zetelt in het inlichtingen- en situatiecentrum van de Europese Unie (INTCEN) aanmoedigen en vergemakkelijken om strategische samenwerking inzake inlichtingen over cyberdreigingen en -activiteiten te bevorderen. Deze werkzaamheden zullen het situationele bewustzijn en de besluitvorming over een gezamenlijke diplomatieke reactie verder ondersteunen. De werkgroep moet samenwerken met bestaande structuren[85] waaronder, indien nodig, degene die de ruimere bedreiging van hybride en buitenlandse tussenkomst bestrijken, om situationeel bewustzijn te verzamelen en te beoordelen.

---

[81] https://www.consilium.europa.eu/nl/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] Besluit van de Raad (CFSP) 2019/797 van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 129I van 17.5.2019, blz. 13); en Verordening (EU) 2019/796 van Raad
van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 129I van 17.5.2019, blz. 1).

[83] Besluit van de Raad (CFSP) 2020/1127 van 30 juli 2020 tot wijziging van Besluit (CFSP) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (ST/9564/2020/INIT) (PB L 246 van 30.7.2020, blz. 12); en Uitvoeringsverordening van de Raad (EU) 2020/1125 van 30 juli 2020 tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (ST/9568/2020/INIT) (PB L 246 van 30.7.2020, blz. 4).

[84] Besluit van de Raad (CFSP) 2020/1537 van 22 oktober 2020 tot wijziging van Besluit (CFSP) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 351I van 22.10.2020, blz. 5); en Uitvoeringsverordening (EU) 2020/1536 van de Raad van 22 oktober 2020 tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 351I van 22.10.2020, blz. 1).

[85] Zoals de EU Single Intelligence Analysis Capacity (SIAC), en, indien nodig, de relevante projecten die zijn vastgesteld in hoofde van PESCO, evenals het systeem voor vroegtijdige waarschuwing (RAS) van 2018 dat werd opgezet om de EU te ondersteunen bij haar algemene benadering tot het aanpakken van desinformatie.

Om de EU beter toe te rusten om kwaadaardig gedrag in cyberspace te voorkomen, te ontmoedigen, tegen te gaan en erop te reageren zal de Hoge Vertegenwoordiger, met de betrokkenheid van de Commissie en overeenkomstig haar bevoegdheden, een voorstel indienen waarmee de EU haar **houding tegenover cyberafschrikking** verder kan definiëren. Verder bouwend op het werk onder het instrumentarium voor cyberdiplomatie tot nog toe moet de houding bijdragen tot verantwoord gedrag van de staat en tot samenwerking in cyberspace; zij moet ook bijzondere richting geven aan het tegengaan van deze cyberaanvallen die de grootste gevolgen hebben, met name degene die onze kritieke infrastructuur, democratische instellingen en processen treffen[86], evenals aanvallen op toeleveringsketens en gedigitaliseerde diefstal van intellectueel eigendom. In de houding moet worden geschetst hoe de EU en de lidstaten hun politieke, economische, diplomatieke, wettelijke en strategische communicatiehulpmiddelen optimaal kunnen inzetten tegen kwaadaardige cyberactiviteiten. Ook moet worden uitgelegd hoe de EU en de lidstaten hun bekwaamheid om kwaadaardige cyberactiviteiten tegen te gaan, kunnen vergroten. Daarnaast streeft de Hoge Vertegenwoordiger er, samen met de Commissie en de Raad, naar om **bijkomende maatregelen te overwegen in het kader van het instrumentarium voor cyberdiplomatie**, waaronder de mogelijkheid voor verdere opties voor beperkende maatregelen en door onderzoek te doen naar **stemmingen met gekwalificeerde meerderheid (QMV) voor de opstelling van lijsten onder het regime van horizontale sancties tegen cyberaanvallen.** Daarnaast moet de EU verdere inspanningen leveren om **de samenwerking met internationale partners te versterken**, waaronder de NAVO, om het gedeelde begrip van het bedreigingslandschap te bevorderen, samenwerkingsmechanismen te ontwikkelen en gezamenlijke diplomatieke reacties te identificeren.

De Hoge Vertegenwoordiger zal, met de betrokkenheid van de Commissie, ook een update voorstellen van de **richtlijnen voor de tenuitvoerlegging van het instrumentarium voor cyberdiplomatie**[87], onder andere met het oog op het vergroten van de doeltreffendheid van het besluitvormingsproces, en blijft regelmatig oefeningen organiseren en beoordelingen houden over het instrumentarium voor cyberdiplomatie. Daarnaast moet de EU het **instrumentarium voor cyberdiplomatie verder integreren in de crisismechanismen van de EU** en streven naar synergieën met inspanningen om hybride bedreigingen, desinformatie en buitenlandse inmenging tegen te gaan krachtens het gezamenlijk kader voor de bestrijding van hybride bedreigingen[88] en het Europees actieplan voor democratie. In deze context moet de EU nadenken over de interactie tussen het instrumentarium voor cyberdiplomatie en het mogelijke gebruik van artikel 42, lid 7, VEU en artikel 222 VWEU[89].

2.4 Cyberdefensiecapaciteit vergroten

De EU en de lidstaten moeten hun bekwaamheid om cyberdreigingen te voorkomen en erop te reageren, vergroten overeenkomstig het ambitieniveau van de EU dat is afgeleid van de globale strategie van de EU van 2016[90]. Hiertoe zal de Hoge Vertegenwoordiger, in samenwerking met de Commissie, een **doorlichting voorstellen van het beleidskader voor**

[86] Met name door te streven naar synergieën met de initiatieven krachtens het Europees actieplan voor democratie.
[87] 13007/17.
[88] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52016JC0018&from=NL
[89] Respectievelijk de clausule betreffende het gemeenschappelijk veiligheids- en defensiebeleid en de solidariteitsclausule.
[90] Conclusies van de Raad over de uitvoering van de integrale EU-strategie op het gebied van veiligheid en defensie (14149/16).

cyberdefensie (CDPF) om een verdere coördinatie en samenwerking tussen de EU-actoren[91] te vergroten, en ook met en tussen de lidstaten, ook wat betreft de missies en operaties van het gemeenschappelijk veiligheids- en defensiebeleid (CSDP). Het CDPF moet het ophanden zijnde strategisch kompas[92] informeren en ervoor zorgen dat cyberbeveiliging en cyberdefensie verder worden geïntegreerd in de ruimere veiligheids- en defensieagenda.

In 2018 identificeerde de EU cyberspace als een domein van operaties[93]. Een ophanden zijnde **"militaire visie en strategie over cyberspace als een domein van operaties"** door het Militair Comité van de Europese Unie moet nader definiëren hoe cyberspace als domein van operaties militaire missies en operaties van het CSDP mogelijk maakt. Het **militaire CERT-netwerk**[94], dat is opgericht door het Europees Defensieagentschap (EDA), zal verder bijdragen tot een significante toename van de samenwerking tussen de lidstaten. Daarnaast zal het Agentschap van de Europese Unie voor het ruimtevaartprogramma, en in het bijzonder het Galileo-centrum voor de beveiligingscontrole, worden versterkt en zal zijn mandaat worden uitgebreid tot andere kritieke activa van het ruimtevaartprogramma. Op die manier wordt de cyberbeveiliging verzekerd van kritieke ruimte-infrastructuren die onder de verantwoordelijkheid van het ruimtevaartprogramma vallen.

De EU en de lidstaten moeten impulsen blijven geven voor de **ontwikkeling van ultramoderne cyberdefensiecapaciteiten** via verschillende EU-beleidsonderdelen en -instrumenten, met name de CDPF en, indien gepast, verder bouwend op het werk van het EDA. Hiervoor is een sterke nadruk op de ontwikkeling en het gebruik van cruciale technologieën vereist zoals KI, encryptie en kwantumcomputing. Overeenkomstig de vermogensontwikkelingprioriteiten van de EU van 2018[95] en op basis van de bevindingen van het eerste verslag van de gecoördineerde jaarlijkse evaluatie inzake defensie (CARD)[96] moet de EU de samenwerking tussen de lidstaten inzake **onderzoek naar cyberdefensie, innovatie en vermogensontwikkeling** verder stimuleren en de lidstaten aanmoedigen om het potentieel van de **permanente gestructureerde samenwerking (PESCO)[97] en het EDF[98] volledig te benutten.**

Het ophanden zijnde **actieplan van de Commissie inzake synergieën tussen de burger-, defensie- en ruimtevaartindustrie**, dat tijdens het eerste kwartaal van 2021 zal worden voorgesteld, zal acties omvatten om verder synergieën te ondersteunen op het niveau van

[91] Met name de EDEO, met inbegrip van de Militaire Staf van de EU (EUMS), de Europese Veiligheids- en defensieacademie (EVDA), de Commissie, en EU-agentschappen, met name het Europees Defensieagentschap (EDA).
[92] Conclusies van de Raad over veiligheid en defensie van 17 juni 2020 (8910/20).
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/nl/pdf
[94] De oprichting van een militair CERT-netwerk van de EU beantwoordt aan een doelstelling die geïdentificeerd is in het beleidskader voor cyberdefensie van 2018 en streeft naar het bevorderen van actieve interactie en informatie-uitwisseling tussen militaire CERT's van de EU-lidstaten.
[95] In juni 2018 kwamen de lidstaten in het bestuur van het EDA overeen de samenwerking inzake defensie te begeleiden op EU-niveau.
[96] Goedgekeurd door de ministers van defensie in het bestuur van het EDA in november 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)
[97] Er zijn momenteel verscheidene cybergerelateerde PESCO-projecten, met name het platform voor het delen van informatie over cyberdreigingen en respons op incidenten, snellereactieteams bij cyberincidenten en wederzijdse bijstand op het gebied van cyberbeveiliging, de cyberacademie en innovatiehub van de EU en het Coördinatiecentrum voor het cyber- en informatiedomein (CIDCC).
[98] Krachtens het EDF heeft de Commissie reeds kansen geïdentificeerd voor potentiële samenwerkende onderzoeks- en ontwikkelingsacties inzake cyberdefensie, gericht op het versterken van samenwerking, innovatiecapaciteit en het concurrentievermogen van de defensie-industrie.

programma's, technologieën, innovatie en startups, overeenkomstig de governance van de respectieve programma's[99].

Daarnaast moeten er relevante synergieën en interfaces worden ontwikkeld tussen cyberdefensie-initiatieven die worden doorgetrokken naar andere kaders, waaronder cybergerelateerde samenwerkingsprojecten[100] door de lidstaten onder PESCO, en met de cyberbeveiligingsstructuren van de EU, om het delen van informatie en wederzijdse ondersteuning te bevorderen.

Strategische initiatieven

De EU zou het volgende moeten doen:

- het Europees crisisbeheerkader voor cyberbeveiliging voltooien en het proces, de mijlpalen en de tijdlijn voor de oprichting van de gezamenlijke cybereenheid bepalen;
- de uitvoering van de agenda voor cybercriminaliteit krachtens de strategie voor de veiligheidsunie verder zetten;
- de totstandbrenging van een werkgroep cyberinlichtingen, die zetelt in het INTCEN van de EU, aanmoedigen en vergemakkelijken;
- de houding van de EU inzake cyberafschrikking bevorderen om kwaadaardige cyberactiviteiten te voorkomen, te ontmoedigen, tegen te gaan en erop te reageren;
- het beleidskader voor cyberdefensie doorlichten;
- de ontwikkeling van een "militaire visie en strategie over cyberspace als een domein van operaties" van de EU voor militaire missies en operaties van het CSDP vergemakkelijken;
- synergieën tussen de burger-, defensie- en ruimtevaartindustrie ondersteunen; en
- de cyberbeveiliging van cruciale ruimtevaartinfrastructuren onder het ruimtevaartprogramma versterken.

3. EEN WERELDWIJDE EN OPEN CYBERSPACE BEVORDEREN

De EU moet blijven samenwerken met internationale partners om een politiek model en een visie op cyberspace te bevorderen die gestoeld zijn op de rechtsstaat, de mensenrechten, de fundamentele vrijheden en de democratische waarden die wereldwijd zorgen voor sociale, economische en politieke ontwikkeling en bijdragen aan een veiligheidsunie. Internationale samenwerking is essentieel om cyberspace mondiaal, open, stabiel en veilig te houden. Hiertoe moet de EU blijven samenwerken met derde landen, met internationale organisaties en met de multistakeholdergemeenschap om een samenhangend en holistisch cyberbeleid te ontwikkelen, waarin bewustzijn van de toenemende verwevenheid tussen de economische aspecten van nieuwe technologieën, binnenlandse veiligheid en het buitenlands, veiligheids- en defensiebeleid centraal staat. Als een sterk economisch en handelsblok dat gebaseerd is op

[99] Zoals Horizon Europa, Digitaal Europa en het EDF.
[100] https://pesco.europa.eu/

democratische kernwaarden, respect voor de rechtsstaat en de grondrechten is de EU ook uitstekend geplaatst om internationale normen en standaarden te definiëren.

3.1. EU-leiderschap inzake standaarden, normen en kaders in cyberspace

Naar meer internationale normalisatie

Om haar visie op cyberspace op internationaal niveau te bevorderen en te verdedigen, moet de EU **haar betrokkenheid bij en leiderschap inzake internationale normalisatieprocessen opvoeren en haar vertegenwoordiging in internationale en Europese normalisatieorganen en in andere organisaties voor de ontwikkeling van standaarden verbeteren**[101]. Naarmate digitale technologieën zich in sneltempo ontwikkelen, worden internationale standaarden steeds belangrijker als aanvulling op traditionele regelgevingsinspanningen op gebieden zoals KI, de cloud, kwantumcomputing en kwantumcommunicatie. Internationale normalisatie wordt in toenemende mate gebruikt door derde landen om hun politieke en ideologische agenda door te duwen, en dat strookt vaak niet met de waarden van de EU. Daarnaast is er een toenemend risico op concurrerende kaders voor internationale normalisatie, en dat leidt tot versnippering.

Internationale standaarden vorm geven op de gebieden van opkomende technologieën en de kerninternetarchitectuur overeenkomstig de EU-waarden is essentieel om te verzekeren dat het internet wereldwijd en open blijft, dat in technologieën de mens en de privacy centraal staan en dat het gebruik ervan wettig, veilig en ethisch is. Als onderdeel van haar ophanden zijnde normalisatiestrategie moet de EU haar **doelstellingen voor internationale normalisatie** definiëren en proactief en gecoördineerd campagne voeren om deze op internationaal niveau bekend te maken. Er moet worden gestreefd naar een sterkere samenwerking en de lasten moeten worden gedeeld met gelijkgestemde partners en Europese belanghebbenden.

Verantwoord gedrag van de staat in cyberspace bevorderen

De EU blijft samenwerken met internationale partners om een wereldwijde, open, stabiele en veilige cyberspace te bevorderen waar het **internationaal recht, met name het Handvest van de Verenigde Naties (VN)**[102]**, wordt geëerbiedigd en de vrijwillige, niet-bindende normen, regels en beginselen van verantwoord gedrag van de staat**[103] worden nageleefd. Nu een effectief multilateraal debat over internationale veiligheid in cyberspace steeds minder vlot verloopt, hebben de EU en de lidstaten een duidelijke behoefte aan een meer proactieve houding in de discussies binnen de VN en andere relevante internationale fora. De EU is het best geplaatst om **de standpunten van de lidstaten in internationale fora te bevorderen, te coördineren en te consolideren** en moet **een EU-standpunt ontwikkelen over de toepassing van het internationaal recht in cyberspace**. De Hoge Vertegenwoordiger streeft er, samen met de lidstaten, ook naar hun inclusieve en op

[101] Enkele voorbeelden zijn de International Organisatie voor normalisatie (ISO), de Internationale Elektrotechnische Commissie (IEC), de Internationale Unie voor Telecommunicatie (ITU), het Europees Comité voor Normalisatie(CEN), het Europees Comité voor elektrotechnische normalisatie (CENELEC), het Europees Instituut voor Telecommunicatienormen (ETSI), de Internet Engineering Task Force (IETF), het 3rd Generation Partnership Project (3GPP) en het Institute of Electrical and Electronics Engineers (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Zoals weerspiegeld in de relevante verslagen van de groepen van regeringsexperts op het gebied van informatie en telecommunicatie in de context van internationale veiligheid (UNGGE's), ondersteund door de Algemene Vergadering van de Verenigde Naties, met name de verslagen van 2015, 2013 en 2010.

consensus gebaseerde voorstel voor een politiek engagement over een **actieprogramma ter bevordering van verantwoord gedrag van de staat in cyberspace (PoA)**[104] voor te leggen aan de VN. Verder bouwend op het bestaande acquis zoals dat wordt gesteund door de Algemene Vergadering van de VN[105] biedt het PoA een platform voor samenwerking en voor de uitwisseling van beste praktijken binnen de VN en stelt het voor een mechanisme tot stand te brengen om de normen van verantwoord gedrag van de staat in de praktijk te brengen en capaciteitsopbouw te bevorderen. Bovendien streeft de Hoge Vertegenwoordiger ernaar de uitvoering van **maatregelen om het vertrouwen** tussen landen **op te bouwen**, aan te moedigen, ook door beste praktijken op regionaal en multilateraal niveau te delen en bij te dragen tot regio-overschrijdende samenwerking.

Meer wereldwijde connectiviteit mag niet leiden tot censuur, massabewaking, lekken in de gegevensprivacy en repressie tegen het maatschappelijk middenveld, de academische wereld en de burgers. De EU moet het voorbeeld blijven geven als het gaat om de bescherming en bevordering van de **mensenrechten en de fundamentele vrijheden** online. Hiertoe moet de EU de verdere naleving van internationale mensenrechten en -standaarden[106] bevorderen en haar actieplan inzake mensenrechten en democratie voor 2020-2024[107] operationaliseren. Ze moet ook haar mensenrechtenrichtsnoeren inzake de vrijheid van meningsuiting online en offline[108] bevorderen door een **nieuwe stimulans over de praktische toepassing van EU-instrumenten te bieden**. De EU moet volgehouden inspanningen leveren om **mensenrechtenverdedigers, het maatschappelijk middenveld en de academische wereld die werken rond kwesties zoals cyberbeveiliging, gegevensprivacy, bewaking en onlinecensuur, te beschermen.** Hiertoe moet de EU verdere praktische begeleiding verstrekken, beste praktijken bevorderen en haar inspanningen opvoeren om misbruik van opkomende technologieën te voorkomen, met name door het gebruik van diplomatieke maatregelen waar nodig, evenals de exportcontrole van dergelijke technologieën. De EU moet ook blijven strijden voor de bescherming van de kwetsbaarste leden van de samenleving online, door wetgeving voor te stellen die kinderen beter moet beschermen tegen seksueel misbruik en seksuele uitbuiting en door een strategie rond de rechten van het kind uit te stippelen.

Het Verdrag van Boedapest inzake cybercriminaliteit

De EU blijft derde landen die wensen toe te treden tot het **Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa** ondersteunen en legt de laatste hand aan het **Tweede Aanvullend Protocol bij het Verdrag van Boedapest** dat maatregelen en waarborgen omvat die de internationale samenwerking tussen rechtshandhavings- en gerechtelijke autoriteiten moeten verbeteren, en tussen autoriteiten en dienstverleners in andere landen, en waarvoor de Commissie namens de EU deelneemt aan de onderhandelingen[109]. Het huidige initiatief voor een nieuw wettelijk instrument inzake cybercriminaliteit op VN-niveau dreigt de verdeeldheid nog te vergroten en de broodnodige

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Zoals weerspiegeld in de relevante verslagen van de groepen van regeringsexperts op het gebied van informatie en telecommunicatie in de context van internationale veiligheid (UNGGE's), ondersteund door de Algemene Vergadering van de Verenigde Naties, met name de verslagen van 2015, 2013 en 2010.

[106] Met name het VN-handvest en de Universele Verklaring van de Rechten van de Mens.

[107] https://www.consilium.europa.eu/nl/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

[109] Besluit van de Raad van juni 2019 (ref. 9116/19).

nationale hervormingen en bijbehorende capaciteitsopbouwinspanningen te vertragen, wat mogelijk een rem zet op de doeltreffende internationale samenwerking tegen cybercriminaliteit: de EU ziet geen noodzaak voor een nieuw wettelijk instrument voor cybercriminaliteit op VN-niveau. De EU blijft deelnemen aan de **multilaterale uitwisselingen over cybercriminaliteit** om de eerbied voor de mensenrechten en de fundamentele vrijheden te verzekeren via inclusiviteit en transparantie en rekening houdend met beschikbare expertise, met als doel toegevoegde waarde te leveren voor iedereen.

3.2 Samenwerking met partners en de multistakeholdergemeenschap

De EU moet **haar cyberdialogen met derde landen versterken en uitbreiden** om haar waarden en visie voor cyberspace uit te dragen, beste praktijken te delen en te streven naar een doeltreffender samenwerking. De EU moet ook **gestructureerde uitwisselingen met regionale organisaties** tot stand brengen zoals de Afrikaanse Unie, het Regionaal Forum van de Asean, de Organisatie van Amerikaanse Staten, en de Organisatie voor Veiligheid en Samenwerking in Europa. Tegelijkertijd moet de EU, waar het mogelijk en opportuun is, punten van overeenkomst trachten te vinden met andere partners op basis van kwesties van gezamenlijk belang. In samenwerking met de EU-delegaties en, indien relevant, met de ambassades van lidstaten over heel de wereld moet de EU een informeel **EU-cyberdiplomatienetwerk** vormen om de visie van de EU op cyberspace uit te dragen, informatie uit te wisselen en regelmatig overleg te plegen over ontwikkelingen in cyberspace[110].

Verder bouwend op de gezamenlijke verklaringen van 8 juli 2016[111] en 10 juli 2018[112] moet de EU de **samenwerking tussen de EU en de NAVO** blijven stimuleren, met name als het gaat over interoperabiliteitsvereisten inzake cyberdefensie. In deze context moet de EU verder ijveren voor de aansluiting van relevante CSDP-structuren bij het gefedereerde missienetwerk van de NAVO, dat indien nodig netwerkinteroperabiliteit met de NAVO en met partners mogelijk maakt. Bovendien moet de samenwerking tussen de EU en de NAVO over onderwijs, opleiding en oefeningen verder worden onderzocht, onder andere door op zoek te gaan naar synergieën tussen de Europese Veiligheids- en defensieacademie en het Cooperative Cyber Defence Centre of Excellence van de NAVO.

In overeenstemming met haar waarden staat de EU volledig achter het **multistakeholdermodel voor internetgovernance**. Geen enkele entiteit, regering of internationale organisatie mag trachten het internet te controleren. De EU moet blijven deelnemen aan fora[113] om de samenwerking te verbeteren en de bescherming van de grondrechten en fundamentele vrijheden, met name het recht op waardigheid, privacy en vrijheid van meningsuiting en informatie, te verzekeren. Om de multistakeholdersamenwerking inzake cyberbeveiligingskwesties te bevorderen streven de Commissie en de Hoge Vertegenwoordiger er, overeenkomstig hun respectieve bevoegdheden, naar **regelmatige en gestructureerde uitwisselingen met belanghebbenden** te versterken, waaronder de particuliere sector, de academische wereld en het

[110] Waar relevant zou ze ook de activiteiten van het informele digitale diplomatienetwerk van de EU kunnen benutten waarin de ministeries van buitenlandse zaken van de lidstaten vervat zitten.
[111] https://www.consilium.europa.eu/nl/press/press-releases/2016/07/08/eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/nl/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Zoals de Internet Cooperation for Assigned Names and Numbers (ICANN) en het Internet Governance Forum (IGF).

maatschappelijk middenveld. Daarbij benadrukken zij dat het, door de onderling verweven aard van cyberspace, nodig is dat alle belanghebbenden van gedachten wisselen over een wereldwijde, open, stabiele en veilige cyberspace en hun specifieke verantwoordelijkheid nemen om die te behouden. Deze inspanningen zullen waardevolle inbreng leveren voor potentiële cruciale acties op EU-niveau.

3.3. De wereldwijde capaciteiten versterken om de wereldwijde veerkracht te vergroten

Om ervoor te zorgen dat alle landen de sociale, economische en politieke vruchten van het internet en het gebruik van technologieën kunnen plukken, blijft de EU haar partners ondersteunen om hun cyberveerkracht en -capaciteiten te vergroten om cybercriminaliteit te vervolgen en cyberdreigingen aan te pakken. Om een algemene samenhang te verzekeren moet de EU een **externe agenda voor de opbouw van cybercapaciteit** ontwikkelen om deze inspanningen te sturen overeenkomstig haar externe richtsnoeren inzake de opbouw van cybercapaciteit[114] en de Agenda 2030 voor Duurzame Ontwikkeling[115]. De agenda moet optimaal gebruikmaken van de expertise van de lidstaten en relevante instellingen, organen, agentschappen en initiatieven van de EU, waaronder het netwerk voor de opbouw van cybercapaciteit van de EU[116], overeenkomstig hun respectieve mandaten. Er zal een **EU-raad voor de opbouw van cybercapaciteit** worden opgericht die relevante institutionele belanghebbenden van de EU zal omvatten en de vooruitgang zal monitoren. Daarnaast zullen er ook verdere synergieën en potentiële hiaten worden geïdentificeerd. Verder kan hij een verbeterde samenwerking met de lidstaten ondersteunen, evenals met partners uit de openbare en de particuliere sector en andere relevante internationale organen om de coördinatie van de inspanningen te verzekeren en overlappingen te vermijden.

De **opbouw van cybercapaciteit in de EU** moet zich blijven toespitsen op de westelijke Balkan en de omgeving van de EU, alsook op partnerlanden die een snelle digitale ontwikkeling doormaken. De inspanningen van de EU moeten de ontwikkeling van wetgeving en beleid van partnerlanden ondersteunen overeenkomstig relevant beleid en normen van de EU inzake cyberdiplomatie. In deze context moet in de capaciteitsopbouwinspanningen van de EU op het gebied van digitalisering cyberbeveiliging worden opgenomen als een standaardeigenschap. Hiertoe moet de EU een opleidingsprogramma uitwerken, bedoeld voor EU-personeel dat belast is met de uitvoering van externe inspanningen voor de opbouw van digitale en cybercapaciteit. De EU moet deze landen ook helpen bij het aanpakken van de toenemende uitdaging van kwaadaardige cyberactiviteiten die de ontwikkeling van hun samenlevingen en de **integriteit en veiligheid van democratische systemen** schaden, overeenkomstig de inspanningen onder het Europees actieplan voor democratie. Collegiaal leren tussen de EU-lidstaten en tussen relevante EU-agentschappen en derde landen zou in dit opzicht zeer nuttig kunnen zijn.

Ten slotte kunnen burgerlijke CSDP-missies, in de context van het burgerlijk CSDP-pact van 2018[117], ook bijdragen tot de ruimere reactie van de EU om cyberbeveiligingsuitdagingen aan te pakken, met name door de rechtsstaat in alsook de rechtshandhaving en de capaciteiten van burgerlijke besturen van partnerlanden te versterken.

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/nl/pdf

Strategische initiatieven

De EU zou het volgende moeten doen:

- een reeks doelstellingen in internationale normalisatieprocessen vastleggen en ze op internationaal niveau bevorderen;
- internationale veiligheid en stabiliteit in cyberspace bevorderen, met name via het voorstel door de EU en haar lidstaten voor een actieprogramma ter bevordering van verantwoord gedrag van de staat in cyberspace (PoA) in de Verenigde Naties;
- praktische begeleiding bieden bij de toepassing van mensenrechten en fundamentele vrijheden in cyberspace;
- kinderen beter beschermen tegen seksueel misbruik en seksuele uitbuiting, en een strategie betreffende de rechten van het kind opstellen;
- het Verdrag van Boedapest inzake cybercriminaliteit versterken en bevorderen, ook via het werk aan het tweede Aanvullend Protocol bij het Verdrag van Boedapest;
- de cyberdialoog van de EU met derde landen, regionale en internationale organisaties uitbreiden, ook via een informeel EU-cyberdiplomatienetwerk;
- de uitwisselingen met de multistakeholdergemeenschap versterken, met name door regelmatige en gestructureerde uitwisselingen met de privésector, de academische wereld en het maatschappelijk middenveld; en
- een externe agenda voor de opbouw van cybercapaciteit van de EU en een EU-raad voor de opbouw van cybercapaciteit voorstellen.

III. CYBERBEVEILIGING IN DE INSTELLINGEN, ORGANEN EN AGENTSCHAPPEN VAN DE EU

Gezien hun hoge politieke profiel, hun cruciale opdrachten om zeer gevoelige kwesties te coördineren en hun rol in het beheren van grote sommen overheidsgeld, **zijn de instellingen, organen en agentschappen van de EU regelmatig het doelwit van cyberaanvallen**, vooral cyberspionage. Het niveau van cyberveerkracht en de mogelijkheid om kwaadaardige cyberactiviteiten op te sporen en erop te reageren variëren qua maturiteit echter aanzienlijk tussen deze entiteiten. Het is dan ook noodzakelijk het algemene niveau van cyberbeveiliging te verbeteren via consequente en homogene regels.

Op het gebied van informatiebeveiliging werd er vooruitgang geboekt in de richting van meer consistentie van de **regels voor de bescherming van zowel geheime als gevoelige, niet-geheime EU-informatie**. De interoperabiliteit van geheime informatiesystemen blijft beperkt, wat een naadloze overdracht van informatie tussen de verschillende entiteiten verhindert. Er moet verdere vooruitgang worden geboekt om een interinstitutionele benadering van de behandeling van geheime EU-informatie en gevoelige, niet-geheime EU-informatie mogelijk te maken; die benadering kan ook dienen als een model voor interoperabiliteit tussen de lidstaten. Er moet ook een nullijn worden vastgelegd om de procedures met de lidstaten te vereenvoudigen. De EU moet ook haar bekwaamheid om veilig te communiceren met relevante partners verder ontwikkelen, indien mogelijk op basis van bestaande regelingen en procedures.

Zoals aangekondigd in de strategie voor de veiligheidsunie zal de Commissie dan ook voorstellen doen voor **gezamenlijke, bindende regels over informatiebeveiliging en voor gezamenlijke, bindende regels over cyberbeveiliging voor alle instellingen, organen en agentschappen van de EU in 2021**, op basis van permanente interinstitutionele besprekingen over cyberbeveiliging in de EU[118].

Door de huidige en toekomstige trends op het gebied van telewerken zullen ook verdere investeringen in veilige apparatuur, infrastructuren en hulpmiddelen, waardoor mensen op afstand kunnen werken aan gevoelige en geheime bestanden, noodzakelijk worden.

Daarnaast maken het steeds vijandiger wordende cyberdreigingslandschap en het toenemende aantal gevallen van meer gesofistikeerde cyberaanvallen tegen instellingen, organen en agentschappen van de EU de nood aan meer investeringen om tot een hoog niveau van cybermaturiteit te komen, steeds dwingender. Voor alle instellingen, organen en agentschappen van de EU wordt er een cyberbewustzijnsprogramma opgezet dat het bewustzijn en de cyberhygiëne van het personeel moet vergroten en een gezamenlijke cultuur van cyberbeveiliging moet ondersteunen.

De **versterking van CERT-EU met een verbeterd financieringsmechanisme** is noodzakelijk zodat het beter in staat is om instellingen, organen en agentschappen van de EU te helpen de nieuwe cyberbeveiligingsregels toe te passen en hun cyberveerkracht te verbeteren. Het mandaat van CERT-EU moet ook worden versterkt om het een stabiel middel aan te reiken om deze doelstellingen te behalen.

Strategische initiatieven

1. Verordening inzake informatiebeveiliging in de instellingen, organen en agentschappen van de EU
2. Verordening inzake gezamenlijke cyberbeveiligingsregels voor de instellingen, organen en agentschappen van de EU
3. Een nieuwe wettelijke basis voor CERT-EU om haar mandaat en financiering te versterken.

IV. CONCLUSIES

De gecoördineerde uitvoering van deze strategie zal bijdragen tot een cyberveilig digitaal decennium voor de EU, tot het bereiken van een veiligheidsunie en tot het versterken van de positie van de EU wereldwijd.

De EU moet het voorbeeld geven als het gaat om oplossingen en normen inzake cyberbeveiliging van wereldklasse ten behoeve van essentiële diensten en kritieke infrastructuur, en om de ontwikkeling en toepassing van nieuwe technologieën. Elke organisatie en persoon die internet gebruikt maakt deel uit van de oplossing door te zorgen voor een cyberveilige digitale transformatie.

De Commissie en de Hoge Vertegenwoordiger zullen, overeenkomstig hun respectieve bevoegdheden, de vooruitgang in het kader van deze strategie monitoren en criteria voor

[118] Regelmatige interinstitutionele besprekingen over cyberbeveiliging binnen de EU maken deel uit van ruimere uitwisselingen over de kansen en uitdagingen van digitale transformatie voor de EU-instellingen.

evaluatie ontwikkelen. Deze monitoring moet onder meer gestoeld zijn op de verslagen van Enisa en de regelmatige verslagen van de Commissie over de veiligheidsunie. De resultaten zullen bijdragen tot de doelstellingen voor het aanstaande digitale decennium[119]. Overeenkomstig hun respectieve bevoegdheden zullen de Commissie en de Hoge Vertegenwoordiger contact blijven houden met de lidstaten om praktische maatregelen vast te stellen om de vier cyberbeveiligingsgemeenschappen in de EU, namelijk kritieke infrastructuur en veerkracht van de interne markt, justitie en rechtshandhaving, cyberdiplomatie en cyberdefensie, waar nodig met elkaar te verbinden. Daarenboven zullen de Commissie en de Hoge Vertegenwoordiger blijven praten met de multistakeholdergemeenschap en daarbij benadrukken hoe belangrijk het is dat iedereen die het internet gebruikt, zijn rol speelt in het behoud van een wereldwijde, open, stabiele en veilige cyberspace, waar iedereen zijn digitale leven in alle veiligheid kan leiden.

[119] Zoals aangekondigd in het werkprogramma van de Commissie voor 2021.

Aanhangsel: Volgende stappen betreffende de cyberbeveiliging van 5G-netwerken

Op basis van de resultaten van de doorlichting van de aanbeveling van de Commissie betreffende de cyberbeveiliging van 5G-netwerken[120] moeten de volgende stappen in het gecoördineerde werk op EU-niveau toegespitst zijn op drie hoofddoelstellingen en op belangrijke acties op korte en middellange termijn die uiteengezet zijn in onderstaande tabel, uit te voeren door de autoriteiten van de lidstaten, de Commissie en Enisa.

De eerste prioriteit voor de volgende fase is het **voltooien van de uitvoering van het instrumentarium op nationaal niveau en het aanpakken van de kwesties die aangestipt zijn in het vooruitgangsverslag van juli 2020**. In deze context zouden sommige van de strategische maatregelen van het instrumentarium baat hebben bij een **betere coördinatie of informatie-uitwisseling** binnen de NIS-werkstroom, zoals reeds geïdentificeerd is in het vooruitgangsverslag; dit zou dan kunnen leiden tot de ontwikkeling van **beste praktijken of richtsnoeren**. Wat technische maatregelen betreft zou Enisa verdere ondersteuning kunnen bieden, door verder te bouwen op het werk dat het reeds heeft verricht en door bepaalde onderwerpen grondiger te onderzoeken. Het zou ook **een allesomvattend overzicht kunnen uitwerken van alle relevante richtsnoeren over de cyberbeveiligingsvereisten van 5G voor exploitanten van mobiele netwerken.**

Ten tweede benadrukten de lidstaten het belang van op de hoogte blijven van de ontwikkelingen via de **permanente monitoring van de evoluties op het gebied van technologie, 5G-architectuur, dreigingen en gebruikssituaties en toepassingen van 5G, evenals externe factoren,** om **nieuwe of opkomende risico's te kunnen identificeren en aanpakken**. Bovendien moet een aantal aspecten in de aanvankelijke risicoanalyse nader worden onderzocht, met name om te verzekeren dat zij het hele 5G-ecosysteem behelst, met inbegrip van alle relevante onderdelen van de netwerkinfrastructuur en van de 5G-toeleveringsketen. Het instrumentarium mag dan wel ontworpen zijn als een flexibel en aanpasbaar instrument, als het nodig is kunnen er op middellange termijn stappen worden ondernomen om het te verbeteren of te wijzigen, om ervoor te zorgen dat het allesomvattend en actueel blijft.

Ten derde moeten er permanent **acties op EU-niveau** worden ondernomen ter ondersteuning en aanvulling van de doelstellingen van het instrumentarium en om ze volledig te integreren in het relevante Unie- en Commissiebeleid, met name het opvolgen van de acties die door de Commissie werden aangekondigd in haar Mededeling over het instrumentarium van 29 januari 2020[121] op een brede waaier aan gebieden (bv. EU-financiering voor veilige 5G-netwerken, investeringen in 5G- en post-5G-technologieën, instrumenten voor handelsbescherming en concurrentie om verstoringen op de bevoorradingsmarkt voor 5G te vermijden enz.).

Indien gepast moeten er begin 2021 gedetailleerde regelingen en mijlpalen voor de voornaamste hieronder uiteengezette acties worden overeengekomen door de voornaamste actoren.

[120] Verslag van de Commissie over het effect van Aanbeveling 2019/534 van de Commissie van 26 maart 2019 betreffende de cyberbeveiliging van 5G-netwerken.

[121] Mededeling van de Commissie COM (2020)50, Uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox, 29 januari 2020.

Kerndoelstelling 1: Verzekeren van convergente nationale benaderingen voor effectieve risicobeperking in heel de EU		
Gebieden	**Voornaamste acties op korte en middellange termijn**	**Voornaamste actoren**
Uitvoering van het instrumentarium door de lidstaten	Vervolledigen van de uitvoering van de maatregelen die worden aanbevolen in de conclusies van het instrumentarium tegen het tweede kwartaal van 2021, met periodieke inventarisatie binnen de NIS-werkstroom.	Autoriteiten van lidstaten
Uitwisseling van informatie en beste praktijken over strategische maatregelen die verband houden met leveranciers	Intensifiëren van informatie-uitwisselingen en nadenken over mogelijke beste praktijken, in het bijzonder over: - beperkingen op risicovolle leveranciers (SM03) en maatregelen in verband met de verlening van beheerde diensten (SM04); - beveiliging en veerkracht van de toeleveringsketen, met name het opvolgen van de enquête die door BEREC werd gehouden over SM05-SM06.	Autoriteiten van lidstaten, Commissie
Capaciteitsopbouw en begeleiding over technische maatregelen	Diepgaand technisch onderzoek doen en gezamenlijke begeleiding en hulpmiddelen ontwikkelen, waaronder: - een allesomvattende en dynamische matrix van beveiligingscontroles en beste praktijken voor 5G-beveiliging; begeleiding ter ondersteuning van de uitvoering van geselecteerde technische maatregelen uit het instrumentarium.	Enisa, autoriteiten van lidstaten
Kerndoelstelling 2: Ondersteunen van continue uitwisseling van kennis en capaciteitsopbouw		
Gebieden	**Voornaamste acties op korte en middellange termijn**	**Voornaamste actoren**
Permanente kennisopbouw	Organiseren van kennisopbouwactiviteiten over technologie en aanverwante uitdagingen (open architecturen, 5G-eigenschappen – bv. virtualisering, containerisering, snijden enz.), evoluties van het dreigingslandschap, levensechte incidenten enz.	Enisa, autoriteiten van lidstaten, andere belanghebbenden
Risicobeoordelingen	Informatie over geactualiseerde nationale risicobeoordelingen bijwerken en uitwisselen	Autoriteiten van lidstaten, Commissie, Enisa
Gezamenlijke, door de EU gefinancierde projecten ter ondersteuning van de uitvoering van het instrumentarium	Verlenen van financiële steun aan projecten ter ondersteuning van de uitvoering van het instrumentarium door middel van EU-financiering, met name krachtens het programma “Digitaal Europa” (bv. capaciteitsopbouwprojecten voor nationale autoriteiten, proefopstellingen of andere geavanceerde capaciteiten enz.)	Autoriteiten van lidstaten, Commissie
Samenwerking tussen belanghebbenden	Stimuleren van samenwerking en medewerking tussen nationale autoriteiten die betrokken zijn bij 5G-cyberbeveiliging (bv. NIS-samenwerkingsgroep, cyberbeveiligingsautoriteiten, regelgevende autoriteiten van de telecomsector) en met private belanghebbenden	Autoriteiten van lidstaten, Commissie, Enisa
Kerndoelstelling 3: Bevorderen van de veerkracht van de toeleveringsketen en andere strategische beveiligingsdoelstellingen van de EU		

Gebieden	**Voornaamste acties op korte en middellange termijn**	**Voornaamste actoren**
Normalisatie	Definiëren en implementeren van een concreet actieplan om de vertegenwoordiging van de EU in normalisatie-organen te verbeteren als onderdeel van de volgende stappen van het werk van de NIS-subgroep over normalisatie, teneinde specifieke beveiligingsdoelstellingen te bereiken, waaronder de bevordering van interoperable interfaces om de diversifiëring van leveranciers te vergemakkelijken	Autoriteiten van lidstaten
Veerkracht van de toeleveringsketen	– Een grondige analyse uitvoeren van het 5G-ecosysteem en van de toeleveringsketen om belangrijke activa en potentiële kritieke afhankelijkheden beter te identificeren en te monitoren – Ervoor zorgen dat de werking van de 5G-markt en -toeleveringsketen strookt met de EU-regels inzake handel en concurrentie, zoals gedefinieerd in de mededeling van de Commissie van 29 januari, en dat er FDI-screening wordt toegepast op investeringsontwikkelingen die mogelijk invloed hebben op de 5G-waardeketen, met inachtneming van de doelstellingen van het instrumentarium – Monitoren van bestaande en verwachte markttrends en beoordelen van de risico's en opportuniteiten op het gebied van Open RAN, met name via een onafhankelijke studie	Autoriteiten van lidstaten, Commissie
Certificering	Starten met de voorbereidingen van relevant(e) plan(nen) voor de certificering van kandidaten voor belangrijke 5G-componenten en processen van leveranciers, om te helpen bepaalde risico's aan te pakken die verband houden met technische kwetsbaarheden, zoals gedefinieerd in de risicobeperkingsplannen van het instrumentarium	Commissie, Enisa, nationale autoriteiten, andere belanghebbenden
EU-capaciteiten en uitrol van veilige netwerken	– Investeren in O&I en capaciteiten, met name via het goedkeuren van het partnerschap voor slimme netwerken en diensten – Relevante beveiligingsvoorwaarden uitvoeren voor EU-financieringsprogramma's en financiële instrumenten (intern en extern), zoals aangekondigd in de mededeling van de Commissie van 29 januari	Lidstaten, Commissie, belanghebbenden uit de 5G-industrie
Externe aspecten	Ingaan op verzoeken van derde landen die de door de EU ontwikkelde instrumentariumbenadering graag zouden begrijpen en mogelijk gebruiken	Lidstaten, Commissie EDEO, EU-delegaties