EUROPESE
COMMISSIE

Brussel, 5.7.2016
COM(2016) 410 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Versterken van het Europese cyberbeveiligingssysteem

en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche

1. INLEIDING/CONTEXT

Elke dag berokkenen cyberveiligheidsincidenten het Europese bedrijfsleven en onze economie ernstige economische schade. Dergelijke incidenten ondermijnen het vertrouwen van burgers en ondernemingen in de digitale samenleving. Diefstal van bedrijfsgeheimen, zakelijke informatie en persoonsgegevens, verstoring van diensten – die soms van vitaal belang zijn – en van infrastructuur veroorzaken jaarlijks honderden miljarden euro verlies[1]. Dit kan ook een impact hebben op de grondrechten van burgers en de maatschappij in het algemeen.

De Strategie inzake cyberbeveiliging van de Europese Unie[2] van 2013 (EU-cyberbeveiligingsstrategie), de richtlijn netwerk- en informatiebeveiliging[3] – die binnenkort wordt aangenomen – en Richtlijn 2013/40/EU over aanvallen op informatiesystemen zijn tot dusver de belangrijkste beleidsinstrumenten van de EU op het gebied van cyberbeveiliging. Voorts beschikt de EU over een aantal gespecialiseerde entiteiten, zoals het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) bij Europol en het computercrisisteam (CERT-EU). Bovendien is onlangs een aantal sectorale initiatieven gelanceerd (bv. op het gebied van energie en vervoer) om de cyberbeveiliging in een aantal kritieke sectoren te verbeteren.

Ondanks die positieve ontwikkelingen blijft de EU kwetsbaar voor cyberincidenten, die de digitale eengemaakte markt en het economisch en maatschappelijk leven als geheel kunnen ondermijnen. De impact ervan reikt bovendien soms verder dan de economie. Bij hybride bedreigingen[4] worden cyberaanvallen op een gecoördineerde wijze gecombineerd met andere acties om een land te destabiliseren of politieke instellingen aan te vallen.

De afhandeling van een grootschalig cyberincident waarbij meerdere lidstaten tegelijk worden getroffen, kan de EU in de problemen brengen. In samenhang met de mededelingen over de bestrijding van hybride bedreigingen en over de Europese veiligheidsagenda[5] bekijkt de Commissie hoe de EU moet inspelen op de voortdurend wijzigende situatie op het gebied van cyberbeveiliging en welke extra maatregelen moeten worden genomen om de weerbaarheid en de paraatheid van de EU bij incidenten te versterken.

Voorts werkt de Commissie aan de industriële capaciteit op het gebied van cyberbeveiliging in de EU. Hoewel Europa niet de volledige waardeketen op het gebied van digitale technologieën kan aansturen, moet het ervoor zorgen dat minstens bepaalde essentiële capaciteiten worden ontwikkeld en behouden. Het aanbieden van goederen en diensten die een maximaal niveau van cyberbeveiliging waarborgen, biedt kansen voor de Europese cyberbeveiligingsbranche en kan uitgroeien tot een aanzienlijk concurrentievoordeel. Naar verwachting wordt de wereldmarkt voor cyberbeveiliging één van de snelst groeiende

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; juni 2014.*
[2] JOIN(2013) 1 final.
[3] COM(2013) 48 final.
[4] JOIN(2016) 18 final.
[5] COM(2016) 230 final.

segmenten van de ICT-sector[6]. Om ervoor te zorgen dat de EU op dit gebied een leiderspositie verwerft, moet een sterke cultuur inzake de beveiliging van gegevens, waaronder persoonsgegevens, worden opgebouwd en werk worden gemaakt van een doelmatige respons bij incidenten. Deze inspanningen zullen de EU veel aantrekkelijker maken voor investeerders en dragen op die manier bij tot de verwezenlijking van de ambitieuze doelstellingen van de digitale eengemaakte markt om groei en banen te creëren.

Het bereiken van de bovenstaande doelstellingen vergt een sterke inzet, met name door:

i) Nauwere samenwerking om de paraatheid te versterken en cyberincidenten aan te pakken

De bestaande en afgesproken samenwerkingsmechanismen moeten worden versterkt om de weerbaarheid en paraatheid van de EU te verbeteren, ook bij een eventuele pan-Europese cyberveiligheidscrisis. Die samenwerkingsmechanismen moeten omvattend zijn en alle stadia van incidenten bestrijken: van preventie tot vervolging. Met het oog op een effectieve samenwerking tussen de lidstaten en de praktische toepassing van beveiligingseisen voor kritieke exploitanten moeten ook robuuste technische oplossingen worden ontwikkeld door de cyberbeveiligingsbranche.

Tegelijk moet permanent worden ingezet op de ontwikkeling van sectoroverschrijdende synergieën en de stroomlijning van cybervereisten in alle relevante EU-beleidsterreinen om de weerbaarheid van kritieke cybervoorzieningen in de hele Unie te waarborgen. De Commissie zal bekijken of de EU-strategie voor cyberbeveiliging van 2013 in de nabije toekomst moet worden bijgewerkt.

ii) Aanpakken van knelpunten op de Europese eengemaakte markt voor cyberbeveiliging

In haar strategie voor een digitale eengemaakte markt (DSM)[7] heeft de Commissie erkend dat de snel ontwikkelende technologieën en oplossingen voor online netwerkbeveiliging nog steeds bepaalde leemtes vertonen. Uit marktonderzoek blijkt tegelijk dat het aanbod van cyberbeveiligingsproducten en -diensten op de interne EU-markt nog steeds geografisch versnipperd is.[8] In deze mededeling worden een aantal marktgerichte beleidsmaatregelen geschetst om die leemtes en knelpunten aan te pakken.

iii) Ondersteunen van de industriële capaciteiten op het gebied van cyberbeveiliging

In de EU-cyberbeveiligingsstrategie en DSM-strategie heeft de Commissie zich ertoe verbonden het toegenomen aanbod aan producten en diensten van de Europese cyberbeveiligingsbranche te promoten. Daarom werkt zij aan een besluit dat het pad effent voor een contractuele regeling inzake publiek-private samenwerking (cPPP) voor cyberbeveiliging, die op haar beurt de opstap moet vormen tot een vooruitstrevende Europese onderzoeks- en innovatie-agenda op het gebied van cyberbeveiliging, waarmee onze concurrentiepositie wordt versterkt.

[6] Zie SWD(2016) 216.
[7] COM(2015) 192 final.
[8] Zie SWD(2016) 216.

2. VERSTERKEN VAN DE SAMENWERKING, KENNIS EN CAPACITEIT

De EU-strategie inzake cyberbeveiliging en met name de geplande NIB-richtlijn[9], opent perspectieven voor een betere Europese samenwerking tussen de lidstaten. De snelle en daadwerkelijke tenuitvoerlegging van de richtlijn is van cruciaal belang voor de digitalisering van het economisch en maatschappelijk leven (ook rekening houdend met de cloud, het internet der dingen en machine-machinecommunicatie), de toenemende internationale interactie en de snelle ontwikkeling van het cyberdreigingslandschap[10]. In die context moet de EU zich voorbereiden op een eventuele grootschalige cybercrisis[11] met bijvoorbeeld meerdere gelijktijdige aanvallen op kritieke informatiesystemen in verschillende lidstaten[12].

Samenwerking op EU-niveau is derhalve essentieel voor de aanpak van zowel kleinschalige incidenten, die zich mogelijk kunnen uitbreiden, als een grootschalige cyberaanval tegen een groot aantal lidstaten tegelijk. De EU moet de cyberdimensie integreren in de bestaande mechanismen voor crisismanagement. Voorts moet zij zorgen voor effectieve samenwerking en snelle mechanismen voor informatie-uitwisseling tussen sectoren en lidstaten om dergelijke incidenten aan te pakken en te beheersen. Deze mechanismen moeten coherent werken en op die manier bijdragen tot de strijd tegen terrorisme, georganiseerde misdaad en cybercriminaliteit. Dit moet de EU in staat stellen beter met haar internationale partners samen te werken om effectief op te treden tegen mondiale bedreigingen en incidenten.

2.1. Een optimale samenwerking op het gebied van cyberbeveiliging en Enisa 2.0

De Computer Security Incident Response Teams (CSIRT's), die verantwoordelijk zijn voor een snelle reactie op cyberbedreigingen en -incidenten, vormen een cruciaal onderdeel van de op grond van de richtlijn cyberbeveiliging vereiste nationale capaciteit. Deze teams worden gebundeld in een CSIRT-netwerk, dat belast wordt met de bevordering van de effectieve operationele samenwerking bij specifieke cyberveiligheidsincidenten en de uitwisseling van informatie over risico's. Voorts voorziet de richtlijn in de oprichting van een samenwerkingsgroep om de strategische samenwerking tussen de lidstaten te ondersteunen en te faciliteren en onderling vertrouwen op te bouwen.

Gezien de aard en veelzijdigheid van cyberdreigingen, moedigt de Commissie de lidstaten aan de NIB-samenwerkingsmechanismen maximaal te benutten en tevens de grensoverschrijdende samenwerking inzake de paraatheid voor een grootschalig cyberincident te versterken. Extra samenwerking in het licht van grote cyberincidenten is gebaat bij een gecoördineerde aanpak van de crisissamenwerking tussen de verschillende elementen van het cyber-ecosysteem. Die aanpak kan worden vertaald in een "blauwdruk", die ook de synergieën en samenhang met bestaande mechanismen voor crisismanagement[13] waarborgt. Een en ander moet daarna regelmatig worden getest door middel van cyber- en andere

[9] Op grond van de richtlijn cyberbeveiliging zullen de lidstaten, om de cyberbeveiligingsrisico's aan te pakken, een inventaris moeten maken van de exploitanten van essentiële diensten op het gebied van energie, vervoer, financiën en gezondheid en zullen zij ervoor moeten zorgen dat bepaalde verleners van digitale diensten passende maatregelen nemen om zich tegen dergelijke risico's te wapenen.
[10] Zie SWD(2016) 216.
[11] Zie bv. het Enisa-rapport: Common practices of EU-level crisis management and applicability to cyber crises (april 2016).
[12] Zie SWD(2016) 216.
[13] Met name de geïntegreerde regeling politieke crisisrespons, m.i.v. het besluit over de regelingen voor de toepassing van de solidariteitsclausule door de Unie (24 juli 2014) en de besluitvormingsprocedure in het kader van het gemeenschappelijk veiligheids- en defensiebeleid.

crisismanagementoefeningen. Daarbij zal ook een beroep worden gedaan op EU-instanties zoals het Enisa, CERT-EU en het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) bij Europol, en op de in het kader van het CSIRT-netwerk ontwikkelde tools. In de eerste helft van 2017 zal de Commissie een blauwdruk voor die samenwerking voorstellen aan de samenwerkingsgroep, het CSIRT-netwerk en andere belanghebbenden.

Op EU-niveau is er reeds kennis en deskundigheid op het gebied van cyberbeveiliging beschikbaar, maar die is versnipperd en niet gestructureerd. Om de NIB-samenwerkingsmechanismen te ondersteunen moet die informatie worden gebundeld in een "informatiehub", zodat ze op verzoek ter beschikking van de lidstaten kan worden gesteld. Die hub zou de spil worden voor de uitwisseling van informatie tussen de EU-instellingen en de lidstaten. Een vlottere toegang tot beter gestructureerde informatie over cyberbeveiligingsrisico's en potentiële remedies moet de lidstaten helpen hun capaciteit te versterken en praktijken op elkaar af te stemmen, en uiteindelijke de algemene weerbaarheid tegen aanvallen versterken. De Commissie, met steun van het Enisa, CERT-EU en met de deskundigheid van het Gemeenschappelijk Centrum voor Onderzoek, zal de oprichting en duurzaamheid van de hub faciliteren.

Bovendien moet op EU-niveau een gewone adviesgroep op hoog niveau[14] op het gebied van cyberbeveiliging worden ingesteld, samengesteld uit deskundigen en beleidsmakers uit de sector, academici, het maatschappelijk middenveld en andere relevante organisaties. Via deze groep zou de Commissie voor haar cyberbeveiligingsbeleid en eventuele regelgevende of andere beleidsmaatregelen op een open en transparante wijze een beroep kunnen doen op externe deskundigheid en input. De groep zou een aanvulling vormen op en aansluiten bij de andere structuren op het gebied van cyberbeveiliging[15].

Bovendien moet de Commissie uiterlijk op 20 juni 2018 een evaluatie van het Enisa maken en moet de eventuele wijziging of verlenging van het mandaat van het Enisa uiterlijk 19 juni 2020[16] worden vastgesteld. In het licht van het huidige cyberbeveiligingslandschap, wil de Commissie werk maken van die evaluatie en, afhankelijk van de resultaten daarvan, zo snel mogelijk een voorstel indienen.

Bij de beoordeling van de eventuele behoefte aan een wijziging van het mandaat van het Enisa moet de Commissie rekening houden met de hierboven omschreven knelpunten inzake cyberbeveiliging en met de algemene inspanningen om de samenwerking en kennisuitwisseling te versterken. Dit proces biedt de gelegenheid om te bekijken of het Agentschap moet worden versterkt zodat het de lidstaten op duurzame wijze kan ondersteunen bij het opbouwen van weerbaarheid op het gebied van cyberbeveiliging. Bij de denkoefening over het mandaat van het Enisa moet bovendien rekening worden gehouden met de nieuwe verantwoordelijkheden van het Agentschap op grond van de NIB-richtlijn, de

[14] Deskundigengroepen van de Commissie vallen onder de horizontale voorschriften die zijn vastgesteld bij Besluit C(2016)3301 van de Commissie.
[15] Bv. het NIB-platform, cPPP op het gebied van cyberbeveiliging en sectorale platforms zoals het EECSP (Energy Expert Cyber Security Platform). Er moet ook een link worden gelegd met de in de mededeling over de digitalisering van het Europese bedrijfsleven aangekondigde rondetafelconferentie op hoog niveau: COM(2016) 180 final.
[16] Verordening (EU) nr. 526/2013 tot intrekking van Verordening (EG) nr. 460/2004.

nieuwe beleidsdoelstellingen ter ondersteuning van de cyberbeveiligingsbranche (DSM-strategie en in het bijzonder het cPPP), de veranderende behoeften voor de beveiliging van kritieke sectoren en ten slotte de nieuwe uitdagingen in verband met grensoverschrijdende incidenten, onder meer de gecoördineerde respons op cybercrises.

De Commissie:

- komt in de eerste helft van 2017 met een blauwdruk voor Europese samenwerking bij de aanpak van grootschalige cyberincidenten;
- faciliteert het opzetten van een informatiehub voor de uitwisseling van informatie tussen de EU-instanties en de lidstaten;
- richt een adviesgroep op hoog niveau op inzake cyberbeveiliging; en
- rondt tegen eind 2017 de evaluatie van het Enisa af. Bij die evaluatie wordt bekeken of het mandaat van het Enisa moet worden gewijzigd of uitgebreid en wordt getracht zo snel mogelijk een voorstel in te dienen.

2.2 Sterker inzetten op onderwijs, opleiding en oefeningen op het gebied van cyberbeveiliging

De juiste vaardigheden en opleiding om cyberbeveiligingsincidenten te voorkomen en de impact daarvan op te vangen of te beperken, zijn enkele cruciale elementen om weerstand op te bouwen inzake cyberbeveiliging.

Op dit moment leveren het Enisa en de Europese groep voor opleiding in verband met cybercriminaliteit (ECTEG) in samenwerking met het Europees Centrum voor de bestrijding van cybercriminaliteit en de Europese Politieacademie (Cepol), allemaal een belangrijke bijdrage tot de opbouw van capaciteit – ook op forensisch gebied – door de opstelling van handboeken en door de organisatie van opleidingen en oefeningen op het gebied van cyberbeveiliging.

Tegelijk is de cyberruimte een zich snel veranderend domein waar capaciteiten voor tweeërlei gebruik een cruciale rol spelen. Daarom is het noodzakelijk civiel-militaire samenwerking op te zetten en synergieën te ontwikkelen op het gebied van opleiding en oefeningen om de EU weerbaarder te maken en beter te wapenen tegen incidenten.

Om op die behoefte in te spelen en als volgende stap na de vaststelling van de NIB-richtlijn en het EU-beleidskader voor cyberdefensie[17], zullen de diensten van de Commissie, in samenwerking met de lidstaten, de Europese Dienst voor extern optreden (EDEO), het Enisa en andere betrokken EU-organen[18], een onderwijs-, opleidings- en oefenplatform op het gebied van cyberbeveiliging opzetten dat de synergieën tussen burgerlijke en militaire opleidingen zal bevorderen.

De Commissie:

- creëert in nauwe samenwerking met de lidstaten, het Enisa, de EDEO en andere

[17] Op 18 november 2014 aangenomen door de Raad Buitenlandse Zaken van de Europese Unie, doc. 15585/14.
[18] Zoals de Europese Veiligheids- en defensieacademie, EC3, Cepol en het Europees Defensieagentschap.

betrokken EU-organen een opleidingsplatform op het gebied van cyberbeveiliging.

2.3. Aanpakken van sectoroverschrijdende afhankelijkheden en de weerbaarheid van vitale openbare netwerkinfrastructuur

Bij de beoordeling van risico's en de impact van een grootschalig cyberincident is de grens- of sectoroverschrijdende afhankelijkheid een doorslaggevende factor. Een ernstig cyberincident in één sector of lidstaat kan een directe of indirecte invloed hebben op of zich uitbreiden naar andere sectoren of lidstaten.

Grens- en sectoroverschrijdende samenwerking faciliteert de uitwisseling van informatie en deskundigheid en bevordert derhalve de paraatheid en weerbaarheid. Via het Europees programma voor de bescherming van kritieke infrastructuur heeft de Commissie ondersteuning verleend voor de werkzaamheden in diverse sectoren om een beter inzicht te verwerven in de onderlinge afhankelijkheden[19].

Tegelijk is de bekwaamheid van elke afzonderlijke sector om cyberincidenten te detecteren, er zich op voor te bereiden en ze aan te pakken een noodzakelijke vereiste voor de aanpak van sectoroverschrijdende risico's. De Commissie zal een beoordeling maken van de risico's die voortvloeien uit cyberincidenten in sterk onderling afhankelijke sectoren in binnen en buitenland, met name in sectoren die onder de NIB-richtlijn vallen, waarbij rekening wordt gehouden met de internationale ontwikkelingen[20]. Op basis van die beoordeling zal de Commissie bepalen of er voor die kritieke sectoren behoefte is aan verdere specifieke regels en/of richtsnoeren inzake de paraatheid voor cyberrisico's.

Op Europees niveau kunnen de sectorale Activiteitencentra[21] voor de informatiemaatschappij (ISAC's) en de overeenkomstige CSIRT's een cruciale rol spelen in de voorbereiding en respons op cyberincidenten. Om de effectieve informatiedoorstroming over wijzigende bedreigingen te waarborgen en de respons op cyberincidenten te faciliteren, moeten de ISAC's worden aangespoord tot samenwerking met het CSIRT-netwerk waarin de NIB-richtlijn voorziet en met het Europees Centrum voor de bestrijding van cybercriminaliteit bij Europol, het CERT-EU en de bevoegde rechtshandhavingsinstanties.

Voor de uitwisseling van informatie tussen belanghebbenden en autoriteiten tijdens de volledige levenscyclus van cyberrisico’s moeten de deelnemers erop kunnen vertrouwen dat zij niet aansprakelijk zullen worden gesteld. De Commissie heeft geconstateerd dat een aantal problemen bedrijven ervan weerhouden waardevolle informatie over dreigingen uit te wisselen met collega's, andere sectoren of de autoriteiten, met name over de grenzen heen. In het belang van een betere uitwisseling van informatie over cyberdreigingen tracht de Commissie die bezwaren aan te pakken en te verlichten.

Betrouwbare rapportagekanalen die de vertrouwelijkheid waarborgen, zijn essentieel om bedrijven aan te moedigen cyberdiefstal van bedrijfsgeheimen te melden. Hierdoor zou het

[19] SWD(2013) 318.

[20] Bv. de routekaart inzake cyberbeveiliging van het Europees Agentschap voor de veiligheid van de luchtvaart, werkzaamheden van de Internationale Organisatie voor de Burgerluchtvaart en de Internationale Maritieme Organisatie.

[21] Zie bijvoorbeeld de European Energy Isac (http://www.ee-isac.eu).

mogelijk worden de schade voor het Europese bedrijfsleven (die tevens tot een verlies aan omzet en werkgelegenheid leidt) en onderzoeksinstellingen te monitoren en in kaart te brengen. Die informatie zal ook helpen om passende beleidsmaatregelen te ontwikkelen. Met steun van het Enisa, het Bureau voor intellectuele eigendom van de Europese Unie (EUIPO) en EC3 bij Europol, zal de Commissie – in overleg met particuliere belanghebbenden – kanalen opzetten waar cyberdiefstal van bedrijfsgeheimen vrijwillig kan worden gemeld en waar de vertrouwelijkheid wordt gewaarborgd. Dit moet het mogelijk maken op EU-niveau geanonimiseerde en geaggregeerde gegevens te verzamelen. Die kunnen vervolgens worden gedeeld met de lidstaten als input voor hun diplomatieke inspanningen en voorlichtingsacties om de immateriële activa van de EU te beschermen tegen cyberaanvallen.

Om de sectorale cyberbeveiliging te bevorderen, zal de Commissie er ook voor pleiten de cyberveiligheidsdimensie mee te nemen bij de ontwikkeling van sectorale EU-beleidsmaatregelen.

Ten slotte is er voor de overheid een taak weggelegd bij de controle van de integriteit van essentiële internetinfrastructuur om problemen op te sporen en de partij die verantwoordelijk is voor die netwerken — waar nodig — attent te maken op zwakheden en bijstand te verlenen bij het wegwerken daarvan. De nationale regelgevende instanties kunnen een beroep doen op de CSIRT's voor regelmatig scans van de openbare netwerkinfrastructuur. Op basis hiervan kunnen zij exploitanten aanmoedigen de bij die scans geconstateerde lacunes of zwakheden weg te werken.

De Commissie zal derhalve onderzoeken onder welke juridische en organisatorische voorwaarden de nationale regelgevende instanties — in samenwerking met nationale cyberbeveiligingsinstanties — de mogelijkheid kunnen krijgen de CSIRT's te verzoeken de openbare netwerkinfrastructuur op regelmatige basis te onderwerpen aan een kwetsbaarheidscontrole. De nationale CSIRT's moeten worden aangemoedigd om binnen het CSIRT-netwerk samen te werken op het gebied van goede praktijken inzake de monitoring van netwerken en de preventie van grootschalige incidenten te faciliteren.

De Commissie:

- ondersteunt het opzetten van Europese samenwerking tussen de sectorale centra voor de uitwisseling en analyse van informatie, bevordert samenwerking tussen die centra en de CSIRT's en pakt de belemmeringen aan die marktdeelnemers ervan weerhouden informatie te delen;
- onderzoekt het strategisch/systeemrisico als gevolg van cybercriminaliteit in sectoren die binnen en over de nationale grenzen heen onderling sterk afhankelijk zijn;
- bekijkt of er behoefte is aan extra regels en/of richtsnoeren inzake de paraatheid van kritieke sectoren ten aanzien van cyberrisico's en formuleert desgevallend voorstellen;
- zet in samenwerking met het Enisa, het EUIPO en het EC3 confidentiële kanalen op voor de vrijwillige melding van cyberdiefstal van bedrijfsgeheimen;
- bevordert de integratie van cyberbeveiliging in de Europese sectoriële

beleidsmaatregelen; en

- onderzoekt onder welke voorwaarden de nationale autoriteiten de CSIRT's kunnen verzoeken regelmatige controles van belangrijke netwerkinfrastructuur uit te voeren.

3. AANPAKKEN VAN KNELPUNTEN OP DE EUROPESE EENGEMAAKTE MARKT VOOR CYBERBEVEILIGING

Europa heeft behoefte aan hoogwaardige, betaalbare en interoperabele producten en oplossingen op het gebied van cyberbeveiliging. Het aanbod van producten en diensten voor ICT-beveiliging blijft binnen de interne markt geografisch echter zeer versnipperd. Enerzijds maakt dit het voor Europese ondernemingen moeilijk om op nationaal, Europees en mondiaal niveau te concurreren; anderzijds hebben burgers en bedrijven hierdoor slechts toegang tot een beperkte keuze aan levensvatbare en bruikbare cyberbeveiligingstechnologieën[22].

De Europese cyberbeveiligingsbranche heeft zich van oudsher grotendeels ontwikkeld op basis van de nationale vraag van de overheid, onder meer op het gebied van defensie. De meeste Europese defensieleveranciers hebben een afdeling cyberbeveiliging opgericht[23]. Daarnaast is er een groot aantal innovatieve kmo's ontstaan, zowel in speciale/nichemarkten (bijvoorbeeld versleutelde systemen) als in gevestigde markten met nieuwe bedrijfsmodellen (bv. antivirussoftware).

Bedrijven ondervinden echter moeite om te groeien op buitenlandse markten. Het gebrek aan vertrouwen in "buitenlandse" oplossingen kwam tijdens alle raadplegingen van de Commissie[24] als essentiële factor naar voren. Bijgevolg worden opdrachten doorgaans toegekend aan bedrijven uit eigen land en is het voor veel bedrijven moeilijk om de schaalvoordelen te bereiken die hun concurrentiepositie zowel op de eengemaakte markt als op wereldschaal zouden versterken.

Andere lacunes waar de eengemaakte markt voor cyberbeveiliging mee kampt, zijn het ontbreken van interoperabele oplossingen (technische normen), praktijken (procesnormen) en EU-wijde certificeringsmechanismen. Cyberbeveiliging werd in dit verband genoemd als één van de ICT-normalisatieprioriteiten voor de digitale eengemaakte markt[25].

De beperkte groeiperspectieven voor ondernemingen op de interne cyberbeveiligingsmarkt leiden tot talrijke fusies en overnames door niet-Europese investeerders[26]. Terwijl die trend het innovatievermogen van de Europese ondernemers op het gebied van cyberbeveiliging aantoont, ontstaat hierdoor ook een risico op het verlies van Europese knowhow en deskundigheid, en op een braindrain.

Er zijn dringend maatregelen nodig om de verdere integratie van de eengemaakte markt voor cyberbeveiligingsproducten en -diensten te bevorderen zodat de invoering van praktische en betaalbare oplossingen wordt gefaciliteerd.

[22] Zie SWD(2016) 216.
[23] Zie SWD(2016) 216.
[24] Zie SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Zie SWD(2016) 216.

Het gebrek aan vertrouwen tussen het Europese bedrijfsleven en de institutionele actoren kan worden overwonnen door samenwerking in een vroeg stadium van de levenscyclus te bevorderen: binnen de cyberbeveiligingsbranche zelf, tussen leveranciers en afnemers; en op sectoroverschrijdend niveau tussen bedrijven die al cyberbeveiligingsoplossingen hebben aangekocht of dat waarschijnlijk zullen doen.

Tegelijkertijd wordt de ontwikkeling van producten, diensten en technologieën voor tweeërlei gebruik in Europa steeds belangrijker. Een toenemend aantal oplossingen vinden vanuit de civiele markt hun weg naar de defensiemarkt[27]. In de aanloop naar het geplande Europese defensieactieplan, is de Commissie van plan verdere maatregelen te nemen om de civiel-militaire synergieën op Europees niveau verder te bevorderen.

3.1 Certificering en labeling

Certificering is belangrijk om het vertrouwen en de veiligheid van producten en diensten op te krikken. Dit geldt ook voor nieuwe systemen die intensief gebruik maken van digitale technologieën en die een hoog beveiligingsniveau vergen, zoals onderling communicerende en zelfrijdende auto's, elektronische gezondheidszorg en besturingssystemen voor industriële automatisatie (IACS) of slimme netwerken.

Er worden nieuwe nationale initiatieven genomen om strenge eisen op het gebied van cyberbeveiliging vast te stellen voor ICT-componenten van traditionele infrastructuur, onder meer certificeringsvoorschriften. Hoewel dit belangrijk is, bestaat het risico dat de versnippering en interoperabiliteitsproblemen op de eengemaakte markt toenemen. Slechts in enkele lidstaten bestaan er effectieve regelingen voor de veiligheidscertificering van ICT-producten[28]. Hierdoor moet een ICT-leverancier soms verschillende certificeringsprocedures doorlopen om zijn producten in verschillende lidstaten te kunnen verkopen. In het slechtste geval mogen ICT-producten of -diensten die in één lidstaat aan de cyberbeveligingseisen voldoen, in een andere lidstaat niet op de markt worden gebracht.

Om tot een werkende eengemaakte cyberbeveiligingsmarkt te komen, moet een kader voor de veiligheidscertificering van ICT-producten en -diensten gericht zijn op de volgende doelstellingen: i) een breed gamma aan ICT-systemen, -producten en -diensten bestrijken; ii) in alle 28 lidstaten van toepassing zijn, en iii) op elk cyberbeveiligingsniveau van toepassing zijn; rekening houden met de internationale ontwikkelingen.

Daartoe zal de Commissie een speciale werkgroep oprichten voor de veiligheidscertificering van ICT-producten en -diensten, samengesteld uit deskundigen uit de lidstaten en de sector. Het is de bedoeling in samenwerking met het Enisa en het Gemeenschappelijk Centrum voor onderzoek tegen eind 2016 een routekaart op te stellen waarin wordt nagegaan of tegen eind 2017 een voorstel kan worden ingediend voor de invoering van een Europees kader voor ICT-veiligheidscertificering. In dit verband zal de Commissie ook rekening houden met

[27] In 2013 vertegenwoordigden producten voor tweeërlei gebruik reeds bijna 20 % van de totale EU-uitvoer (in waarde), met inbegrip van het handelsverkeer binnen de EU.

[28] Zie SWD(2016) 216 voor de overeenkomst van de groep van hoge ambtenaren inzake informatiesystemen (Besluit van de Raad van 31 maart 1992 (92/242/EEG) en andere bestaande regelingen, bijvoorbeeld Commercial Product Assurance in het Verenigd Koninkrijk en Certification Sécuritaire de Premier Niveau in Frankrijk.)

Verordening (EG) nr. 2008/765 en de certificeringsbepalingen van de algemene verordening gegevensbescherming (Verordening (EU) 2016/679[29]).

Het proces voorziet in een brede raadpleging en effectbeoordeling. Op die manier kan de Commissie verschillende opties onderzoeken voor het certificeringskader voor ICT-producten en -diensten. Zij zal ook onderzoek doen naar de ICT-veiligheidscertificering in de infrastructuursectoren (bv. luchtvaart, spoorwegen en de automobielsector) en in specifieke certificerings- en valideringsmechanismen voor technologie die rijp is voor marktintroductie (bv. cyberbeveiliging van besturingssystemen voor industriële automatisatie[30], het internet der dingen en cloudcomputing). Er wordt ook gekeken naar de lacunes in de bovengenoemde Europese ICT-certificeringsregeling.

Certificering zal zoveel mogelijk gebeuren op basis van internationaal erkende normen en worden ontwikkeld in overleg met internationale partners.

De Commissie zal ook nagaan hoe ICT-beveiligingscertificering het best kan worden geïntegreerd in toekomstige sectorspecifieke regelgeving, onder meer wat de veiligheidsaspecten betreft.

Naast mogelijke regelgevende opties, zal zij ook bekijken of een facultatief en "zacht" Europees, commercieel gericht, cyberbeveiligingslabel voor ICT-producten kan worden ingevoerd. Bovenop de certificering moet een dergelijk label de cyberbeveiligingsdimensie in commerciële producten leesbaarder maken, waardoor hun concurrentiepositie op de eengemaakte en wereldmarkt wordt versterkt. Daarbij zal rekening worden gehouden met de lopende sectorale en horizontale initiatieven van de sector, zowel aan de vraag- als de aanbodzijde.

Er zal nauw overleg worden gepleegd met de overheid zodat daarna met gemeenschappelijke specificaties kan worden gewerkt en in overheidsopdrachten naar de certificering kan worden verwezen. De Commissie zal ook toezien op het gebruik van relevante certificeringseisen bij overheidsopdrachten op nationaal niveau, met name voor sectorale systemen (energie, vervoer, gezondheidszorg, openbaar bestuur enz.) en daarover verslag uitbrengen.

De Commissie:

- stelt vóór eind 2016 een routekaart op voor een eventueel voorstel voor een Europees kader voor de veiligheidscertificering van ICT, dat uiterlijk eind 2017 moet worden ingediend, en voor het onderzoeken van de haalbaarheid en gevolgen van een "zacht" Europees kader voor een cyberbeveiligingslabel;
- gaat na of de ICT-beveiligingscertificering binnen de bestaande sectorspecifieke certificerings-/valideringsmechanismen lacunes vertoont en stelt indien nodig maatregelen voor om die weg te werken;

[29] Bij Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens zijn gedragscodes vastgesteld met het oog op de correcte toepassing van de regels inzake gegevensbescherming en ten behoeve van de certificeringsmechanismen voor alle beginselen inzake gegevensbescherming, waaronder de beveiliging van gegevens bij de verwerking van persoonsgegevens.

[30] Zie de voorstellen van de themagroep van het ERNCIP over "Cyber security of Industrial Control Systems", op https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

- integreert in voorkomend geval de veiligheidscertificering van ICT-producten in toekomstige sectorspecifieke wetgevingsvoorstellen;
- stimuleert de betrokkenheid van overheden om het gebruik van certificering en gemeenschappelijke specificaties bij overheidsopdrachten te faciliteren; en
- ziet toe op het gebruik van relevante certificeringseisen bij overheidsopdrachten en commerciële contracten en brengt over drie jaar verslag uit over de situatie op de markt.

3.2. Meer investeringen in cyberbeveiliging in Europa en ondersteunen van het mkb

Hoewel de innovatie in de Europese cyberbeveiligingsbranche zich snel ontwikkelt, is er in de EU nog steeds te weinig draagvlak voor investeringen in cyberbeveiliging. Binnen het mkb zijn er heel wat innoverende ondernemingen, maar vaak beschikken ze niet over de mogelijkheden om hun activiteiten uit te breiden. Dit komt onder meer door het gebrek aan gemakkelijk beschikbare middelen om hen vanaf een vroeg ontwikkelingsstadium te ondersteunen. Bedrijven hebben in Europa bovendien slechts beperkte toegang tot durfkapitaal, en hun marketingbudget om hun naambekendheid te vergroten, of in te spelen op uiteenlopende normen of bindende voorschriften, is ontoereikend.

Tegelijkertijd is de samenwerking tussen de actoren op het gebied van cyberbeveiliging vrij fragmentarisch en moeten er meer inspanningen worden geleverd om de economische concentratie te versterken en nieuwe waardeketens[31] te ontwikkelen.

Om in Europa de investeringen in cyberbeveiliging aan te zwengelen en het mkb te ondersteunen, moet financiering beter toegankelijk worden. Er moet ook steun worden verleend voor de ontwikkeling van wereldwijd concurrerende cyberbeveiligingsclusters en -expertisecentra binnen gunstige regionale ecosystemen voor digitale groei. Die steun moet worden gekoppeld aan de tenuitvoerlegging van strategieën voor slimme specialisatie en andere EU-instrumenten zodat de Europese cyberbeveiligingsbranche er meer profijt uit haalt.

De Commissie zal focussen op de bewustmaking van de cybergemeenschap van de financieringsmogelijkheden op Europees, nationaal en regionaal niveau (zowel via horizontale instrumenten als specifieke oproepen[32]) via de bestaande instrumenten en kanalen, zoals het Enterprise Europe Network.

De Commissie zal bovendien samen met de Europese Investeringsbank (EIB) en het Europees Investeringsfonds (EIF) bekijken hoe de toegang tot financiering kan worden vergemakkelijkt. Dit kan in de vorm van investeringen van eigen vermogen en quasi-eigen vermogen, leningen, projectgaranties of tegengaranties aan tussenpersonen, bijvoorbeeld door

[31] Zie SWD(2016) 216.
[32] Zie bv. de multisectorale oproep 2016 tot het indienen van voorstellen in het kader van de financieringsfaciliteit voor Europese verbindingen en de COSMO-oproepen 2016 in verband met het programma voor de internationalisering van clusters

het opzetten van een investeringsplatform cyberbeveiliging in het kader van het Europees Fonds voor strategische investeringen[33].

Daarnaast zal de Commissie, in samenspraak met belangstellende lidstaten of regio's, onderzoeken of er een platform voor slimme specialisatie op het gebied van cyberbeveiliging kan worden opgericht[34]. Dat platform zou helpen bij de coördinatie en planning van de strategieën inzake cyberbeveiliging en een strategische samenwerking tussen belanghebbenden in regionale ecosystemen tot stand brengen. Die aanpak moet ervoor zorgen dat de cyberbeveiligingsbranche toegang krijgt tot de mogelijkheden van de bestaande Europese structuur- en investeringsfondsen.

In het algemeen pleit de Commissie voor cyberbeveiliging door ontwerp. Zij zal erop toezien dat de cyberbeveiligingsvoorschriften consequent worden toegepast bij alle grote investeringen in infrastructuur die een digitale component bezitten en waarvoor uit Europese fondsen medefinanciering wordt verleend. Daartoe zal de Commissie de relevante eisen stapsgewijs opnemen in de regels voor openbare aanbestedingen en programma's.

De Commissie:

- wendt de bestaande instrumenten ter ondersteuning van het mkb aan om de bestaande financieringsmechanismen beter bekend te maken binnen de cyberbeveiligingsbranche;
- maakt meer gebruik van de EU-tools en -instrumenten om innovatieve mkb-bedrijven te ondersteunen bij het zoeken naar synergieën tussen de civiele en defensiepijler van de cyberveiligheidsmarkt[35];
- onderzoekt samen met de EIB en het EIF hoe de toegang tot investeringen kan worden gefaciliteerd, bv. door middel van een specifiek investeringsplatform of andere instrumenten voor cyberbeveiliging;
- creëert een platform voor slimme specialisatie op het gebied van cyberbeveiliging ter ondersteuning van lidstaten en regio's die willen investeren in de cyberbeveiliging (RIS3); en
- bevordert de filosofie van "veiligheid door ontwerp" bij grote investeringen in infrastructuur met een digitale component en waarvoor medefinanciering wordt verleend uit EU-fondsen.

[33] In het kader van het Europees Fonds voor strategische investeringen (EFSI) kan steun worden verleend voor individuele projecten, hetzij direct, hetzij indirect via investeringsplatforms. Die platforms kunnen bijdragen aan de financiering van kleinere projecten en middelen uit verschillende bronnen bundelen om gediversifieerde investeringen met een geografische of thematische focus mogelijk te maken.
[34] Zie de instrumenten voor slimme specialisatie (RIS3): http://s3platform.jrc.ec.europa.eu/.
[35] Het Enterprise Europe Network en het Europees netwerk van defensiegerelateerde regio's zullen regio's bijvoorbeeld nieuwe kansen bieden voor grensoverschrijdende samenwerking op het gebied van tweeërlei gebruik, met name op het vlak van cyberbeveiliging, en voor het mkb om deel te nemen aan bemiddelingsactiviteiten.

4. DE EUROPESE CYBERBEVEILIGINGSBRANCHE STIMULEREN EN VOEDEN DOOR INNOVATIE – OPRICHTING VAN EEN CPPP VOOR CYBERBEVEILIGING

Om de concurrentiepositie en de innovatie van de Europese cyberbeveiligingsbranche te stimuleren wordt een contractueel publiek-privaat partnerschap (cPPP) voor cyberbeveiliging gesloten. Het cPPP zal middelen van de overheid en het bedrijfsleven bundelen om excellentie in onderzoek en innovatie te bewerkstelligen.

Het cPPP streeft naar wederzijds vertrouwen tussen de lidstaten en het bedrijfsleven door samenwerking te bevorderen vanaf de eerste stadia van het onderzoeks- en innovatieproces. Een andere doelstelling is de afstemming tussen de vraag en het beschikbare aanbod. Dit moet het bedrijfsleven inzicht verschaffen in de toekomstige eisen van eindgebruikers en sectoren, die belangrijke afnemers zijn van cyberbeveiligingsoplossingen (bv. energie, vervoer, gezondheidszorg en financiën). Hierdoor kunnen zij gemakkelijker worden betrokken bij de definiëring van gemeenschappelijke eisen inzake digitale veiligheid, privacy en gegevensbescherming voor hun sectoren.

Het cPPP voor cyberbeveiliging zal ook helpen om de beschikbare middelen maximaal te benutten, in de eerste plaats door een betere coördinatie met de lidstaten. Ten tweede wordt er beter gefocust op enkele technische prioriteiten om de cyberbeveiligingsbranche te helpen om technologische doorbraken te verwezenlijken en belangrijke toekomstige cyberbeveiligingstechnologieën onder de knie te krijgen. De ontwikkeling van open source software en open normen kan in die context bijdragen tot meer vertrouwen, transparantie en baanbrekende innovatie, en moet dan ook deel uitmaken van de investeringen die in het kader van dit cPPP worden gedaan.

De werkzaamheden in het kader van het cPPP voor cyberbeveiliging zullen ook de vruchten plukken van synergieën met andere Europese projecten, met name projecten in verband met veiligheid. Het gaat onder meer om de PPP's voor de fabrieken van de toekomst, energie-efficiënte gebouwen, 5G en big data[36], andere sectorale PPP's[37] en het initiatief voor het internet der dingen[38]. Voorts zal worden gepleit voor een nauwe afstemming met de Europese open wetenschapscloud en het Europees supercomputerinitiatief voor quantumcybertechnologieën (bv. innovatie in quantumcryptografie en quantumcomputeronderzoek).

Het cPPP voor cyberbeveiliging is gelanceerd in het kader van Horizon 2020[39], het kaderprogramma van de EU voor onderzoek en innovatie voor de periode 2014-2020. Er worden middelen bijeengebracht voor twee pijlers van het programma: leiderschap op het gebied van ontsluitende en industriële technologieën (LEIT-ICT) en maatschappelijke uitdagingen — veilige samenlevingen (SC7). De totale begroting van het cPPP bedraagt maximum 450 miljoen EUR, aangevuld met een drievoudige bijdrage vanuit het bedrijfsleven. Het thema cyberbeveiliging moet worden aangepakt en gecoördineerd met andere relevante onderdelen van Horizon 2020 (bv. energie, vervoer, de maatschappelijke

[36] Het publiek-privaat partnerschap voor 5G-infrastructuur en het publiek-privaat partnerschap voor Big Data Value
[37] Bv. SESAR of het publiek-privaat partnerschap Shift2Rail.
[38] Alliance for Internet of Things Innovation (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

uitdagingen op het gebied van gezondheidszorg, en excellentie als onderdeel van Horizon 2020). Dit zal bijdragen aan de doelstellingen van het cPPP voor cyberbeveiliging. Die coördinatie moet ook vooraf gebeuren bij de ontwikkeling van de sectorale strategieën.

Het cPPP zal op transparante wijze worden opgezet met een open en flexibele governance, aangepast aan de snel veranderende context op het gebied van cyberbeveiliging. Hierbij wordt rekening gehouden met de behoefte van de lidstaten om te overleggen over de impact van technologische veranderingen op de veilige exploitatie van nationale en grensoverschrijdende infrastructuur. Tegelijk moet het partnerschap gedurende meerdere jaren een duurzame output leveren zodat zijn doelstellingen kunnen worden verwezenlijkt.

Het cPPP wordt ondersteund door de European Cyber Security Organisation (ECSO), waarvan de samenstelling een afspiegeling zal zijn van de diversiteit op de Europese cyberbeveiligingsmarkt. Ook de nationale, regionale en lokale overheden, universiteiten, onderzoekscentra en andere belanghebbende partijen zullen er deel van uitmaken.

De Commissie:

- sluit met het bedrijfsleven een contractueel publiek-privaat partnerschap voor cyberbeveiliging, dat in het derde kwartaal van 2016 operationeel wordt;
- publiceert in het kader van Horizon 2020 in het eerste kwartaal van 2017 oproepen in verband met het cPPP voor cyberbeveiliging; en
- zorgt voor de coördinatie tussen het cPPP voor cyberbeveiliging, de Horizon 2020-instrumenten en de sectorale PPP's.

5. CONCLUSIE

In deze mededeling worden maatregelen voorgesteld om de Europese weerbaarheid op het gebied van cyberbeveiliging te versterken en een concurrerende en innovatieve cyberbeveiligingsbranche in Europa te bevorderen, zoals aangekondigd in de cyberbeveiligingsstrategie en de strategie voor de digitale eengemaakte markt. De Commissie roept het Europees Parlement en de Raad op deze aanpak te steunen.