Raad van de
Europese Unie

Brussel, 13 september 2018
(OR. en)

12104/18
ADD 5

Interinstitutioneel dossier:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

BEGELEIDENDE NOTA

van:	de heer Jordi AYET PUIGARNAU, directeur, namens de secretaris-generaal van de Europese Commissie
ingekomen:	12 september 2018
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
Nr. Comdoc.:	SWD(2018) 404 final
Betreft:	WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE SAMENVATTING VAN DE EFFECTBEOORDELING bij VOORSTEL VOOR EEN VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

Hierbij gaat voor de delegaties document SWD(2018) 404 final.

Bijlage: SWD(2018) 404 final

EUROPESE
COMMISSIE

Brussel, 12.9.2018
SWD(2018) 404 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

VOORSTEL VOOR EEN VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Samenvatting

Effectbeoordeling betreffende: Voorstel voor de oprichting van het netwerk van kenniscentra en het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging

A. Behoefte aan actie

Waarom? Wat is het probleem?

De EU beschikt vandaag nog steeds over onvoldoende technologische en industriële capaciteit om autonoom haar economie en kritieke infrastructuren te beveiligen en uit te groeien tot een wereldleider op het gebied van cyberbeveiliging. Dit initiatief beoogt bij te dragen tot de aanpak van de volgende problemen en onderliggende oorzaken:

Probleem 1: Er is onvoldoende strategische en duurzame coördinatie en samenwerking tussen de industrieën, de onderzoeksgemeenschappen die actief zijn op het gebied van cyberbeveiliging en de regeringen om de economie, maatschappij en democratie te beschermen met geavanceerde Europese cyberbeveiligingsoplossingen.

Probleem 2: Er wordt op onvoldoende grote schaal geïnvesteerd en er is beperkte toegang tot expertise, vaardigheden en faciliteiten voor cyberbeveiliging in heel Europa.

Probleem 3: Slechts een beperkt aantal Europese onderzoeks- en innovatieresultaten op het gebied van cyberveiligheid hebben zich vertaald in commercieel interessante oplossingen en zijn op grote schaal ingezet in de hele economie.

Deze problemen hebben een aantal onderliggende oorzaken, waaronder onvoldoende vertrouwen tussen de verschillende spelers op de cyberbeveiligingsmarkt, de inherente beperkingen van de bestaande mechanismen voor samenwerking en de bundeling van fondsen, het ontbreken van een kader voor gezamenlijke aanbestedingen voor dure cyberbeveiligingsinfrastructuur en cyberbeveiligingsproducten en -oplossingen, en het ongebruikte potentieel van push- en pullmechanismen op de markt.

Wat moet met dit initiatief worden bereikt?

Het initiatief moet ervoor zorgen dat de EU de essentiële (technologische en industriële) capaciteit behoudt en ontwikkelt om autonoom haar digitale economie, maatschappij en democratie te beveiligen, en dat de lidstaten profiteren van de meest geavanceerde cyberbeveiligingsoplossingen en cyberdefensiecapaciteit. Doel van het initiatief is ook het mondiale concurrentievermogen van de EU te vergroten en ervoor te zorgen dat de Europese ondernemingen en industrieën in verschillende sectoren toegang hebben tot de capaciteiten en middelen om van cyberbeveiliging een concurrentievoordeel te maken. Dit doel moet worden bereikt door doeltreffende mechanismen te ontwikkelen voor langdurige strategische samenwerking tussen alle relevante actoren (overheidsinstanties, industrieën, de onderzoeksgemeenschap uit zowel de civiele als militaire sector), door kennis en middelen te bundelen om geavanceerde capaciteiten en infrastructuur te kunnen aanbieden, door de ruime aanwending van Europese cyberbeveiligingsproducten en -oplossingen in de hele economie en de publieke sector aan te moedigen, door startende, kleine en middelgrote cyberbeveiligingsbedrijven te ondersteunen en door bij te dragen aan het dichten van de kloof inzake cyberbeveiligingsvaardigheden.

Wat is de meerwaarde van maatregelen op EU-niveau?

Ten opzichte van de huidige inspanningen op nationaal niveau zou het initiatief een toegevoegde waarde vormen omdat het helpt met de oprichting van een EU-breed ecosysteem voor cyberbeveiliging waarin industrie en onderzoek onderling met elkaar worden verbonden. Het moet de samenwerking tussen belanghebbenden aanmoedigen (onder meer tussen de civiele en militaire cyberbeveiligingssectoren) zodat optimaal wordt gebruikgemaakt van de bestaande middelen en deskundigheid op het gebied van cyberbeveiliging in heel Europa. Het moet de EU en de lidstaten ook helpen om proactief, strategisch en vanuit een langetermijnperspectief een industriebeleid voor cyberbeveiliging uit te stippelen en daarbij verder te gaan dan alleen onderzoek en ontwikkeling. Deze aanpak moet niet alleen helpen bij de zoektocht naar baanbrekende oplossingen voor de uitdagingen waarmee de particuliere en de openbare sector kampen, maar ook de effectieve aanwending van deze oplossingen ondersteunen. De betrokken industriële gemeenschappen, onderzoeksgemeenschappen en overheidsinstanties zullen ook toegang kunnen krijgen tot belangrijke capaciteiten, zoals test- en experimenteerfaciliteiten, die door een tekort aan financiële en personele middelen vaak niet binnen het bereik

van afzonderlijke lidstaten liggen. Het initiatief zal er ook toe bijdragen dat de vaardighedenkloof wordt gedicht en, door de grootste talenten toegang te geven tot grootschalige Europese projecten en hen op die manier interessante professionele uitdagingen te bieden, zal het voorkomen dat er een braindrain plaatsvindt. Al het bovenstaande wordt ook als noodzakelijk gezien als de EU wereldwijd als een leider op het gebied van cyberbeveiliging wil worden gezien.

B. Oplossingen

Welke wetgevende en niet-wetgevende beleidsmaatregelen zijn overwogen? Heeft een bepaalde optie de voorkeur? Waarom?

Er werden verschillende beleidsopties, zowel wetgevende als niet-wetgevende, bekeken. De volgende opties zijn meegenomen voor een diepgaande beoordeling:

1. **Het basisscenario** – de gezamenlijke optie – gaat uit van de voortzetting van de huidige aanpak om de industriële en technologische capaciteiten op het gebied van cyberbeveiliging in de EU verder op te bouwen door middel van onderzoek en innovatie en daarmee verband houdende samenwerkingsmechanismen in het kader van het programma Horizon Europa.
2. **Optie 1:** Een kennisnetwerk voor cyberbeveiliging met een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging met een mandaat om maatregelen te nemen ter ondersteuning van industriële technologieën, alsook op het gebied van onderzoek en innovatie.
3. **Optie 2:** Een kennisnetwerk voor cyberbeveiliging met een Europees onderzoeks- en kenniscentrum voor cyberbeveiliging dat enkel gericht is op onderzoek en innovatie.

De opties die in een vroeg stadium werden verworpen, waren 1) helemaal geen actie, 2) enkel een netwerk van bestaande kenniscentra, 3) een bestaand agentschap gebruiken (Enisa, REA of INEA).

Gezien de algemene verbintenis die de Commissie reeds is aangegaan voor dit initiatief en gezien de belangrijke rol die moet worden gespeeld door de lidstaten, ligt het belangrijkste onderscheid tussen de twee diepgaand onderzochte opties in hun reikwijdte, die tot uitdrukking komt in hun rechtsgrondslag: indien een entiteit uitsluitend zou worden gebaseerd op artikel 187 VWEU (optie 2), zou het initiatief beperkt blijven tot het gebied van onderzoek en innovatie, en zou er doorgaans van een financiële bijdrage van particuliere spelers worden uitgegaan. Indien een entiteit echter een dubbele rechtsgrondslag zou hebben – de artikelen 187 en 173 VWEU (optie 1) – zou dit zorgen voor een breder mandaat met onder meer steun voor aanwending, industriële ondersteuning en de creatie van sterkere synergieën met cyberdefensie. Hierbij zou ook een prominentere rol zijn weggelegd voor de lidstaten – zowel wat hun rol in het bestuur als hun rol als potentiële inkopers van cyberbeveiligingstechnologie betreft.

Uit de analyse bleek dat optie 1 het best geschikt is om de doelstellingen van het initiatief te verwezenlijken, waarbij optimale economische, maatschappelijke en milieueffecten worden bereikt en de belangen van de Unie het best worden gewaarborgd. De belangrijkste argumenten vóór deze optie zijn de flexibiliteit, waardoor verschillende modellen van samenwerking met de gemeenschap mogelijk zijn en waardoor het netwerk van kenniscentra het gebruik van bestaande kennis en middelen kan optimaliseren; de mogelijkheid om structuur aan te brengen in de samenwerkingsverbanden van publieke en private belanghebbenden uit alle relevante sectoren, met inbegrip van defensie; de mogelijkheid om een echt industriebeleid op het gebied van cyberbeveiliging uit te werken door ondersteuning te bieden aan activiteiten die niet alleen verband houden met onderzoek en ontwikkeling, maar ook met marktintroductie. Tot slot kan optie 1 de samenhang vergroten door te fungeren als een uitvoeringsmechanisme voor financiering in verband met cyberbeveiliging uit de programma's Digitaal Europa en Horizon Europa, en door een sterkere synergie te creëren tussen de civiele en militaire cyberbeveiligingsdimensies met betrekking tot het Europees Defensiefonds.

Wie steunt welke optie?

Uit de raadpleging en het verzamelde bewijsmateriaal is duidelijk gebleken dat de industrie- en onderzoeksgemeenschappen vragende partij zijn voor een mechanisme waarmee de EU een coherent industriebeleid op het gebied van cyberbeveiliging kan voeren dat verder gaat dan onderzoek en ontwikkeling alleen en dat van Europa een wereldleider op het gebied van cyberveiligheid kan maken. Tegelijkertijd hebben de belanghebbenden benadrukt dat het, wil men succesvol zijn, belangrijk is om het kenniscentrum een duidelijk

omschreven rol te geven bij de ondersteuning en bevordering van de inspanningen van het netwerk en de betrokken gemeenschappen en om voor het netwerk een inclusieve, op samenwerking gebaseerde aanpak te hanteren zodat er geen nieuwe silo's ontstaan. De structuur moet ook flexibel zijn zodat deze gemakkelijk kan worden aangepast aan de snel veranderende wereld van de cyberbeveiliging. De lidstaten hebben benadrukt dat het netwerk van kenniscentra voor cyberbeveiliging inclusief moet zijn ten aanzien van alle lidstaten en hun bestaande excellentie- en kenniscentra, en dat er bijzondere aandacht dient te worden besteed aan complementariteit. De lidstaten benadrukten met name het belang van de coördinerende rol van het kenniscentrum ter ondersteuning van het netwerk. Daarom moet elk initiatief van de Commissie het juiste evenwicht vinden tussen de governance- en uitvoeringsstructuren én dit evenwicht weerspiegelen om een doeltreffende coördinatie op Europees niveau te garanderen, rekening houdend met de ontwikkelingen op nationaal niveau.

C. Effecten van de voorkeursoptie

Wat zijn de voordelen van de voorkeursoptie (indien van toepassing, anders van de belangrijkste opties)?

De voorkeursoptie biedt overheden en industrieën in de lidstaten de mogelijkheid beter beveiligde producten en oplossingen te gebruiken en aan te bieden, zodat ze cyberdreigingen beter kunnen vermijden en afwenden. Dit is met name van belang voor de beveiliging van de toegang tot essentiële diensten (zoals vervoers-, gezondheids-, bancaire en financiële diensten). Deze optie zou ook een positieve invloed hebben op het concurrentievermogen van de EU en van kleine en middelgrote ondernemingen. De bedoeling is namelijk een mechanisme te creëren waarmee de industriële cyberbeveiligingscapaciteiten van de lidstaten en de Unie kunnen worden uitgebouwd en waarmee wetenschappelijk toponderzoek kan worden omgezet in commercieel interessante oplossingen die in de hele economie kunnen worden aangewend. Dankzij deze optie kunnen middelen worden gebundeld om te investeren in de nodige capaciteiten op het niveau van de lidstaten en om gedeelde Europese activa te ontwikkelen en schaalvoordelen te realiseren. Dit zal er waarschijnlijk toe leiden dat kleine en middelgrote ondernemingen, de industrie en onderzoekers meer toegang krijgen tot dergelijke faciliteiten, wat de innovatie ten goede komt en de ontwikkelingsprocessen verkort. Bedrijven aan de vraagzijde zullen hun kosten zien dalen en het zal hen helpen om van cyberbeveiliging een concurrentievoordeel te maken. De voorkeursoptie maakt het mogelijk om marktkansen voor producten voor tweeërlei gebruik te grijpen, waarbij militaire en civiele gemeenschappen samenwerken aan gemeenschappelijke uitdagingen. Deze optie zou waarschijnlijk ook een meerwaarde bieden voor nationale inspanningen om de vaardighedenkloof inzake cyberbeveiliging te dichten. Op het niveau van de EU zou dit ook voor meer samenhang en synergie tussen de verschillende financieringsmechanismen zorgen.

De ontwikkeling van specifieke cyberbeveiligingsoplossingen voor sectoren met een potentieel enorme impact op het milieu (bijv. kerncentrales) zou indirect positieve gevolgen hebben voor het milieu als deze sectoren worden geholpen om de potentieel verwoestende gevolgen van cyberaanvallen op dit type infrastructuur te vermijden.

Wat zijn de kosten van de voorkeursoptie (indien van toepassing, anders die van de belangrijkste opties)?

De kosten van de voorkeursoptie houden voornamelijk verband met de kosten van de werking van het kenniscentrum en de nationale coördinatiecentra. De kosten van de uitvoering van verschillende financieringsprogramma's (Digitaal Europa en Horizon Europa) worden onderworpen aan afzonderlijke effectbeoordelingen.

Wat zijn de gevolgen voor bedrijven, kleine, middelgrote en micro-ondernemingen?

Europese bedrijven, aan zowel de vraag- als aanbodzijde van de cyberbeveiligingsmarkt, met inbegrip van kleine, middelgrote en micro-ondernemingen die actief zijn op het gebied van cyberbeveiliging, zullen bij de belanghebbende partijen horen die de grootste impact ondervinden. De oprichting van het kenniscentrum en het netwerk brengt voor deze partijen geen wettelijke verplichtingen met zich mee, en toch zullen ze bij het ontwerp van nieuwe producten meer kosten kunnen besparen en zullen ze gemakkelijker toegang krijgen tot de gemeenschap van investeerders en de nodige financiering kunnen aantrekken voor commercieel interessante oplossingen. Nog belangrijker voor kleine, middelgrote en micro-ondernemingen is de toegang tot door de overheid gefinancierde test- en experimenteerfaciliteiten, aangezien deze ondernemingen over onvoldoende middelen beschikken om zelf de nodige infrastructuur aan te kopen of om deze buiten hun markt (en vaak buiten

de EU) te gaan zoeken. Gehoopt wordt ook dat dit initiatief Europese kleine, middelgrote en micro-ondernemingen die actief zijn op het gebied van cyberbeveiliging, zal toelaten nieuwe markten aan te boren. Bovendien zal het gekozen mechanisme zorgen voor coördinatie tussen de onderzoekswereld en de industrie en dus het onderzoek rechtstreeks op concrete industriële behoeften afstemmen. De terbeschikkingstelling van geavanceerde knowhow en instrumenten op het gebied van cyberbeveiliging zal de marktdeelnemers indirect helpen om de NIS-richtlijn na te leven.

Zijn er significante gevolgen voor de nationale begrotingen en overheden?

Het initiatief zal de lidstaten in staat stellen om investeringen in noodzakelijke cyberbeveiligingsinfrastructuur op nationaal en Europees niveau te coördineren. Dankzij het mechanisme kunnen middelen worden gebundeld voor instrumenten en infrastructuren die anders duurder of zelfs onbetaalbaar zouden zijn voor afzonderlijke lidstaten. Deze benadering zou leiden tot schaalvoordelen en rationalisering. De financiële bijdrage van de lidstaten aan het kenniscentrum en aan relevante maatregelen moet in verhouding staan tot de bijdrage van de Unie.

Zijn er nog andere significante gevolgen?

Ja, het initiatief heeft een duidelijk positief effect, omdat het de lidstaten waarschijnlijk veel meer capaciteiten zou geven om hun economieën autonoom te beveiligen, hun kritieke sectoren te beschermen, het concurrentievermogen van de Europese cyberbeveiligingsbedrijven en -industrieën in verschillende sectoren te versterken, zodat deze hun huidige activa naar behoren kunnen beveiligen, veilige innovatieve producten kunnen ontwerpen, en tegelijk hun O&O-uitgaven voor beveiliging kunnen verlagen. Hierdoor zou de EU uiteindelijk een leidende rol kunnen spelen op het vlak van digitale en cyberbeveiligingstechnologieën van de volgende generatie.

D. Evaluatie

Wanneer wordt dit beleid geëvalueerd?

In het rechtsinstrument wordt een expliciete bepaling opgenomen om toe te zien op de essentiële prestatie-indicatoren (KPI's), alsook een clausule inzake toetsing en evaluatie op grond waarvan de Europese Commissie een tussentijdse evaluatie zal uitvoeren om de gevolgen van het instrument en de toegevoegde waarde ervan te meten. De Europese Commissie zal daarna verslag uitbrengen bij het Europees Parlement en de Raad. Na deze evaluatie kan de Commissie voorstellen om het mandaat van het kenniscentrum en het netwerk te herzien en om het uit te breiden.