AANBEVELINGEN

AANBEVELING (EU) 2017/1584 VAN DE COMMISSIE

van 13 september 2017

inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Overwegende hetgeen volgt:

(1) Nu de onderlinge verbondenheid en afhankelijkheid van onze burgers en bedrijven, over sectoren en grenzen heen, groter is dan ooit tevoren, zijn het gebruik en de afhankelijkheid van informatie- en communicatietechnologieën fundamentele aspecten geworden van alle sectoren van de economische activiteit. De lidstaten en instellingen van de EU moeten goed voorbereid zijn op een cyberincident dat organisaties in meer dan één lidstaat of zelfs de hele Unie treft en dat de interne markt en, meer in het algemeen, de netwerk- en informatiesystemen waar de economie, democratie en samenleving van de Unie van afhankelijk zijn, ernstig kan verstoren.

(2) Een cyberincident kan worden beschouwd als een crisis op het niveau van de Unie wanneer de verstoring die door het incident wordt veroorzaakt te groot is om door een getroffen lidstaat alleen te worden verholpen of wanneer de technische of politieke gevolgen voor twee of meer lidstaten zo wijdverspreid zijn dat tijdige coördinatie en respons op het politieke niveau van de Unie vereist zijn.

(3) Cyberincidenten kunnen een ruimere crisis veroorzaken en gevolgen hebben voor activiteitensectoren die verder reiken dan netwerk- en informatiesystemen en communicatienetwerken; elke respons moet gebaseerd zijn op zowel cybergebonden als niet-cybergebonden risicobeperkende activiteiten.

(4) Cyberincidenten zijn onvoorspelbaar en ontstaan en verspreiden zich vaak op zeer korte tijd; de getroffen entiteiten en degenen die verantwoordelijk zijn om op het incident te reageren en de gevolgen ervan te beperken, moeten hun respons dus snel coördineren. Bovendien blijven cyberincidenten vaak niet beperkt tot één bepaald geografisch gebied; ze kunnen zich gelijktijdig voordoen of razendsnel verspreiden over meerdere landen.

(5) Een effectieve respons op grootschalige incidenten en crises op het gebied van cyberbeveiliging op het niveau van de EU vereist snelle en effectieve samenwerking tussen alle relevante belanghebbenden, en is afhankelijk van de paraatheid en capaciteiten van individuele lidstaten en van gecoördineerde gezamenlijke actie met de steun van de Unie. Het bestaan van vooraf vastgelegde en, in de mate van het mogelijke, goed ingeoefende samenwerkingsprocedures en -mechanismen, met duidelijk vastgestelde rollen en verantwoordelijkheden voor de belangrijkste actoren op nationaal en EU-niveau, is van essentieel belang om tijdig en effectief te kunnen reageren op incidenten.

(6) In zijn conclusies ([1]) inzake de bescherming van kritieke informatie-infrastructuur van 27 mei 2011 heeft de Raad de EU-lidstaten verzocht „de samenwerking tussen de lidstaten te intensiveren en op basis van de nationale crisisbeheersingservaringen en -resultaten en in samenwerking met het Enisa te helpen bij de ontwikkeling van Europese samenwerkingsmechanismen bij cyberincidenten, die zullen worden uitgetest in het kader van de volgende CyberEurope-oefening in 2012".

(7) In haar mededeling uit 2016 „Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche" ([2]) moedigt de Commissie de lidstaten aan de NIB-samenwerkingsmechanismen ([3]) maximaal te benutten en tevens de grensoverschrijdende samenwerking inzake

([1]) Conclusies van de Raad inzake de bescherming van kritieke informatie-infrastructuur „Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid", document 10299/11, Brussel, 27 mei 2011.
([2]) COM(2016) 410 final van 5 juli 2016.
([3]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

de paraatheid voor een grootschalig cyberincident te versterken. Zij voegde eraan toe dat een gecoördineerde aanpak van de crisissamenwerking tussen de verschillende elementen van het cyber-ecosysteem die paraatheid zou vergroten en dat een dergelijke „blauwdruk" ook de synergieën en samenhang met bestaande mechanismen voor crisismanagement zou waarborgen.

(8) In de conclusies van de Raad ([1]) over de bovenvermelde mededeling hebben de lidstaten de Commissie verzocht een dergelijke blauwdruk in te dienen, zodat de betrokken instanties en andere belanghebbenden deze kunnen bestuderen. De NIB-richtlijn voorziet echter niet in een samenwerkingskader op het niveau van de Unie in het geval van grootschalige cyberincidenten en -crises.

(9) De Commissie heeft tijdens twee afzonderlijke workshops, die op 5 april en 4 juli 2017 plaatsvonden in Brussel, overleg gepleegd met vertegenwoordigers van de lidstaten die afkomstig waren uit Computer Security Incident Response Teams (CSIRT's), de bij de NIB-richtlijn opgerichte samenwerkingsgroep en de Horizontale Groep cybervraagstukken van de Raad, en met vertegenwoordigers van de Europese Dienst voor extern optreden (EDEO), Enisa, Europol/EC3 en het Algemeen Secretariaat van de Raad.

(10) De in de bijlage bij deze aanbeveling gevoegde blauwdruk voor een gecoördineerde respons op grootschalige cyberincidenten en -crises op het niveau van de Unie is het resultaat van het bovenvermelde overleg en vormt een aanvulling op de mededeling „Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche".

(11) In de blauwdruk worden de doelstellingen en samenwerkingsvormen tussen de lidstaten en de EU-instellingen, -organen, -bureaus en -agentschappen (hierna „de EU-instellingen" genoemd) beschreven in reactie op grootschalige cyberincidenten en -crises, en wordt uiteengezet hoe bestaande crisisbeheersingsmechanismen optimaal gebruik kunnen maken van bestaande cyberbeveiligingsentiteiten op EU-niveau.

(12) Wanneer in de zin van overweging 2 op een cybercrisis wordt gereageerd, dan is de coördinatie van de respons in de Raad, op het politieke niveau van de Unie, gebaseerd op de geïntegreerde regeling politieke crisisrespons (IPCR) ([2]); de Commissie maakt gebruik van Argus ([3]), het proces voor sectoroverschrijdende coördinatie op hoog niveau. Als de crisis een belangrijke externe dimensie heeft of raakt aan het gemeenschappelijk Europees veiligheids- en defensiebeleid, dan wordt het Crisisresponsmechanisme (CRM) ([3]) van de Europese Dienst voor extern optreden (EDEO) geactiveerd.

(13) Op bepaalde gebieden voorzien sectorale crisisbeheersingsmechanismen op EU-niveau in samenwerking in het geval van cyberincidenten of -crises. Wat bijvoorbeeld het Europese wereldwijde satellietnavigatiesysteem (GNSS) betreft, is in Besluit 2014/496/GBVB van de Raad ([4]) reeds vastgesteld welke rol de Raad, de hoge vertegenwoordiger, de Commissie het Europees GNSS-agentschap en de lidstaten spelen in de keten van operationele verantwoordelijkheden die is opgezet om te reageren op een bedreiging voor de Unie, de lidstaten of het GNSS; dit heeft ook betrekking op cyberaanvallen. Deze aanbeveling laat dergelijke mechanismen dan ook onverlet.

(14) Het is in de eerste plaats de verantwoordelijkheid van de lidstaten om te reageren als zij getroffen worden door grootschalige cyberincidenten of -crises. Er is echter ook een belangrijke rol weggelegd voor de Commissie, de hoge vertegenwoordiger en de andere instellingen of diensten van de EU, die voortvloeit uit de Uniewetgeving of uit het feit dat cyberincidenten en -crises gevolgen kunnen hebben voor alle deelgebieden van de economische activiteit in de interne markt, voor de beveiliging en de internationale betrekkingen van de Unie en voor de instellingen zelf.

(15) De belangrijkste actoren die op het niveau van de Unie betrokken zijn bij een respons op cybercrises zijn onder meer de recentelijk opgerichte structuren en mechanismen van de NIB-richtlijn, namelijk het netwerk van Computer Security Incident Response Teams (CSIRT), en de relevante agentschappen en organen, namelijk het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), het Europees Centrum voor de bestrijding van cybercriminaliteit, dat deel uitmaakt van Europol (Europol/EC3), het Centrum van de Europese Unie voor de analyse van inlichtingen (Intcen), de afdeling Militaire Inlichtingen van de EU (EUMS INT) en het Situatiecentrum (SitRoom), die samen de gezamenlijke capaciteit op het gebied van inlichtingenanalyse vormen, de EU-Fusiecel (die deel uitmaakt van Intcen), het computercrisisteam voor de EU-instellingen en agentschappen (CERT-EU) en het Coördinatiecentrum voor respons in noodsituaties van de Europese Commissie.

(16) Het CSIRT-netwerk, dat in het kader van de NIB-richtlijn is opgezet, zorgt voor technische samenwerking tussen de lidstaten bij een respons op cyberincidenten. Enisa is het secretariaat van het netwerk en ondersteunt actief de

([1]) Document 14540/16 van 15 november 2016.
([2]) Zie voor nadere informatie punt 3.1 van het aanhangsel inzake crisisbeheersing, samenwerkingsmechanismen en actoren op het niveau van de EU.
([3]) Ibidem.
([4]) Besluit 2014/496/GBVB van de Raad van 22 juli 2014 over aspecten van de stationering, de exploitatie en het gebruik van het Europese wereldwijde satellietnavigatiesysteem, die betrekking hebben op de veiligheid van de Europese Unie, en tot intrekking van Gemeenschappelijk Optreden 2004/552/GBVB (PB L 219 van 25.7.2014, blz. 53).

samenwerking tussen de CSIRT's. De nationale CSIRT's en het CERT-EU werken samen en wisselen op vrijwillige basis informatie uit, indien nodig ook in reactie op cyberincidenten die één of meer lidstaten treffen. Op verzoek van de vertegenwoordiger van het CSIRT van een lidstaat kunnen zij, indien mogelijk, overleggen en een gecoördineerde respons bepalen op een incident dat binnen de jurisdictie van die lidstaat heeft plaatsgevonden. De relevante procedures zijn uiteengezet in de standaardwerkwijzen van het CSIRT-netwerk ([1]).

(17) Het CSIRT-netwerk is ook belast met het bespreken, onderzoeken en vaststellen van verdere vormen van operationele samenwerking, onder meer ook met betrekking tot categorieën risico's en incidenten, vroegtijdige waarschuwingen, wederzijdse bijstand, beginselen en voorwaarden voor coördinatie, wanneer lidstaten reageren op grensoverschrijdende risico's en incidenten.

(18) De bij artikel 11 van de NIB-richtlijn opgerichte samenwerkingsgroep is belast met het verlenen van strategische aansturing voor de activiteiten van het CSIRT-netwerk en het bespreken van de capaciteiten en paraatheid van de lidstaten en, op vrijwillige basis, het evalueren van nationale strategieën voor de beveiliging van netwerk- en informatiesystemen en de effectiviteit van CSIRT's, en het identificeren van beste praktijken.

(19) Binnen de samenwerkingsgroep bestaat een specifieke actielijn voor de opstelling van richtsnoeren voor de melding van incidenten, overeenkomstig artikel 14, lid 7, van de NIB-richtlijn, waarin bepaald wordt in welke omstandigheden verleners van essentiële diensten incidenten moeten melden overeenkomstig artikel 14, lid 3, en in welk formaat en volgens welke procedure deze meldingen moeten worden gedaan ([2]).

(20) Bewustzijn en begrip van de realtimesituatie, risicogedrag en bedreigingen, die zijn opgedaan dankzij rapportering, beoordelingen, studie, onderzoek en analyse, zijn van essentieel belang om goed onderbouwde besluiten te nemen. Voor een effectieve gecoördineerde respons is het van essentieel belang dat alle relevante belanghebbenden over dit „situatiebewustzijn" beschikken. Situatiebewustzijn heeft zowel betrekking op de oorzaken als de gevolgen van het incident. Algemeen wordt erkend dat dit afhankelijk is van de uitwisseling van informatie tussen relevante partijen in een geschikt formaat en op een voldoende veilige wijze, waarbij gebruik wordt gemaakt van een gemeenschappelijke classificatie om het incident te beschrijven.

(21) Een respons op cyberincidenten kan vele vormen aannemen, van het identificeren van technische maatregelen waarbij twee of meer entiteiten samen de technische oorzaken van het incident onderzoeken (bijv. de analyse van malware) of het identificeren van manieren waarop organisaties kunnen nagaan of ze zijn getroffen (bijv. Indicators of Compromise), tot operationele besluiten over de toepassing van dergelijke maatregelen en, op politiek niveau, besluiten over het gebruik van andere instrumenten, zoals het kader voor een gezamenlijke respons op kwaadwillige cyberactiviteiten ([3]) of het operationeel EU-protocol voor de bestrijding van hybride bedreigingen ([4]), al naargelang het incident.

(22) Het vertrouwen van Europese burgers en bedrijven in digitale diensten is van essentieel belang voor een bloeiende digitale interne markt. Daarom speelt crisiscommunicatie een bijzonder belangrijke rol in het beperken van de negatieve gevolgen van cyberincidenten en -crises. Ook in de context van het kader voor een gezamenlijk diplomatiek antwoord kan gebruik worden gemaakt van communicatie, als middel om het gedrag van (potentiële) daders die actief zijn vanuit derde landen te beïnvloeden. De politieke respons is alleen doeltreffend wanneer de publieke communicatie om de negatieve gevolgen van cyberincidenten en -crises te beperken en de publieke communicatie om daders te beïnvloeden, op elkaar worden afgestemd.

(23) De gevolgen van grootschalige cyberincidenten of -crises kunnen ook op doeltreffende wijze worden beperkt door het publiek te informeren over de wijze waarop zij op het niveau van een individuele gebruiker of een organisatie de gevolgen van een incident kunnen beperken (bijv. door een patch te installeren of aanvullende maatregelen te nemen om de dreiging af te wenden).

(24) Via de digitaleddiensteninfrastructuur op het gebied van cyberbeveiliging van de Connecting Europe Facility (CEF) ontwikkelt de Commissie een centraal dienstenplatform, een samenwerkingsmechanisme met de naam MeliCERTes, voor de CSIRT's van deelnemende lidstaten, zodat zij hun paraatheid, samenwerking en respons op ontluikende cyberdreigingen en -incidenten kunnen verbeteren. Via vergelijkende uitnodigingen tot het indienen van voorstellen voor de toekenning van subsidies in het kader van de CEF verleent de Commissie ook medefinanciering aan CSIRT's in de lidstaten, teneinde hun operationele capaciteiten op nationaal niveau te verbeteren.

([1]) In ontwikkeling; deze zullen naar verwachting tegen eind 2017 worden aangenomen.
([2]) Het is de bedoeling deze richtsnoeren tegen eind 2017 te voltooien.
([3]) Ontwerpconclusies van de Raad over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten („Instrumentarium voor cyberdiplomatie"), Doc. 9916/17.
([4]) Gezamenlijk werkdocument van de diensten van de EU „Operationeel EU-protocol voor de bestrijding van hybride bedreigingen", EU-draaiboek, SWD(2016) 227 final van 5 juli 2016.

(25) Cyberbeveiligingsoefeningen op EU-niveau zijn essentieel om de samenwerking tussen de lidstaten en de private sector te bevorderen en te verbeteren. Om dit doel te bereiken, organiseert Enisa sinds 2010 regelmatig pan-Europese oefeningen met betrekking tot cyberincidenten („Cyber Europe").

(26) In de conclusies van de Raad ([1]) over de uitvoering van de gezamenlijke verklaring van de voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de secretaris-generaal van de Noord-Atlantische Verdragsorganisatie wordt een oproep gedaan om de samenwerking in cyberoefeningen te versterken via wederzijdse deelname van het personeel aan de respectieve oefeningen, met name Cyber Coalition en Cyber Europe.

(27) Het voortdurend evoluerende dreigingslandschap en recente cyberincidenten zijn een indicatie van de alsmaar toenemende risico's waarmee de Unie wordt geconfronteerd; de lidstaten moeten dan ook onverwijld gevolg geven aan deze aanbeveling, uiterlijk tegen eind 2018,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

1. De lidstaten en de EU-instellingen moeten een EU-kader voor respons op cybercrises vaststellen, waarin de in de blauwdruk gepresenteerde doelstellingen en samenwerkingsvoorwaarden worden opgenomen volgens de daarin beschreven leidende beginselen.

2. Het EU-kader voor respons op cybercrises moet met name de relevante actoren, EU-instellingen en instanties van de lidstaten identificeren, op alle nodige niveaus — technisch, operationeel, strategisch/politiek — en indien nodig standaardwerkwijzen opstellen voor hun onderlinge samenwerking in het kader van de EU-mechanismen voor crisisbeheersing. Daarbij moet de nadruk worden gelegd op het uitwisselen van informatie zonder onnodige vertraging en de respons en de coördinatie van de respons tijdens grootschalige cyberincidenten en -crises.

3. Om dit doel te bereiken, moeten de bevoegde autoriteiten van de lidstaten samen voortwerken aan specificaties voor informatie-uitwisseling en samenwerkingsprotocollen. De samenwerkingsgroep moet de ervaringen op deze gebieden uitwisselen met de relevante EU-instellingen.

4. De lidstaten moeten ervoor zorgen dat hun nationale mechanismen voor crisisbeheersing voorzien in een passende respons op cyberincidenten en in de nodige procedures voor samenwerking op EU-niveau in de context van het EU-kader.

5. Wat de bestaande crisisbeheersingsmechanismen van de EU betreft, moeten de lidstaten, overeenkomstig de blauwdruk, samen met de diensten van de Commissie en de EDEO praktische uitvoeringsrichtsnoeren opstellen voor de integratie van hun nationale crisisbeheersings- en cyberbeveiligingsentiteiten en -procedures in de bestaande crisisbeheersingsmechanismen van de EU, namelijk de IPCR en het CRM van de EDEO. De lidstaten moeten met name zorgen voor passende structuren die efficiënte informatiestromen mogelijk maken tussen hun nationale crisisbeheersingsautoriteiten en hun vertegenwoordigers op EU-niveau in de context van de EU-crisismechanismen.

6. De lidstaten moeten ten volle gebruikmaken van de mogelijkheden die worden geboden door het programma van de Connecting Europe Facility (CEF) voor digitaledienstеninfrastructuur op het gebied van cyberbeveiliging, en moeten met de Commissie samenwerken om te garanderen dat het centraal dienstenplatform, een samenwerkingsmechanisme dat momenteel in ontwikkeling is, over de nodige functies beschikt en voldoet aan hun eisen op het gebied van samenwerking, ook tijdens cybercrises.

7. Met de bijstand van Enisa en voortbouwend op eerdere werkzaamheden op dit gebied, moeten de lidstaten samen een gemeenschappelijke classificatie opstellen en vaststellen, alsook een model voor situatieverslagen waarin de technische oorzaken en gevolgen van cyberincidenten worden beschreven, zodat zij hun technische en operationele samenwerking tijdens crises verder kunnen verbeteren. Wat dit betreft, dienen de lidstaten rekening te houden met de werkzaamheden die binnen de samenwerkingsgroep lopende zijn met betrekking tot richtsnoeren voor de melding van incidenten, en met name de aspecten die verband houden met het formaat van nationale meldingen.

8. De procedures die in het kader worden uiteengezet, moeten worden getest en indien nodig herzien op basis van de lessen die zijn getrokken uit de deelname van lidstaten aan cyberoefeningen op het niveau van de regio's, de lidstaten, de Unie en de NAVO en uit cyberdiplomatie. Ze moeten met name worden getest in het kader van de CyberEurope-oefeningen die door Enisa worden georganiseerd. De eerste gelegenheid om dit te doen is CyberEurope 2018.

([1]) Document ST 15283/16 van 6 december 2016.

9. De lidstaten en de EU-instellingen moeten regelmatig hun respons op grootschalige cyberincidenten en crises op nationaal en Europees niveau oefenen, met inbegrip van hun politieke respons, indien nodig, en in samenwerking met entiteiten uit de privésector, voor zover van toepassing.

Gedaan te Brussel, 13 september 2017

Voor de Commissie
Mariya GABRIEL
Lid van de Commissie

BIJLAGE

Blauwdruk voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberincidenten en -crises

INLEIDING

Deze blauwdruk is van toepassing op cyberincidenten die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen of die zodanig verstrekkende en significante technische of politieke gevolgen hebben voor twee of meer lidstaten of EU-instellingen dat tijdige coördinatie en respons op het politieke niveau van de Unie vereist zijn.

Dergelijke grootschalige cyberincidenten worden als een „cybercrisis" beschouwd.

In het geval de hele EU wordt getroffen door een cybercrisis, zorgt de Raad voor politieke coördinatie op het niveau van de Unie; de Raad maakt daarvoor gebruik van de regeling geïntegreerde politieke crisisrespons (IPCR).

Binnen de Commissie vindt de coördinatie plaats overeenkomstig het systeem voor snelle waarschuwing Argus.

Als de crisis een belangrijke externe dimensie heeft of raakt aan het gemeenschappelijk Europees veiligheids- en defensiebeleid, dan wordt het Crisisresponsmechanisme van de Europese Dienst voor extern optreden (EDEO) geactiveerd.

In de blauwdruk wordt beschreven hoe deze gevestigde crisisbeheersingsmechanismen volledig gebruik moeten maken van bestaande cyberbeveiligingsentiteiten op EU-niveau en van samenwerkingsmechanismen tussen de lidstaten.

De blauwdruk houdt daarbij rekening met een reeks leidende beginselen (evenredigheid, subsidiariteit, complementariteit en vertrouwelijkheid van informatie) en beschrijft de kerndoelstellingen van de samenwerking (effectieve respons, gedeeld situatiebewustzijn, publieke communicatieberichten) op drie niveaus (strategisch/politiek, operationeel en technisch), de betrokken mechanismen en actoren, en de activiteiten die nodig zijn om te voldoen aan deze kerndoelstellingen.

De blauwdruk heeft geen betrekking op de volledige cyclus van crisisbeheersing (preventie/risicobeperking, paraatheid, respons, herstel), maar is gefocust op respons. Desondanks komen ook bepaalde andere activiteiten aan bod, met name activiteiten die verband houden met het bereiken van een gedeeld situatiebewustzijn.

Het is tevens van belang erop te wijzen dat cyberincidenten aan de basis kunnen liggen of deel kunnen uitmaken van een ruimere crisis, die ook gevolgen heeft voor andere sectoren. Aangezien cybercrises meestal ook gevolgen hebben voor de fysieke wereld, moet een passende respons gebaseerd zijn op zowel cybergebonden als niet-cybergebonden risicobeperkende activiteiten. De respons op een cybercrisis moet worden gecoördineerd met andere crisisbeheersingsmechanismen op EU-, nationaal of sectoraal niveau.

Ten slotte is de blauwdruk geen vervanging voor bestaande mechanismen, regelingen of instrumenten die specifiek zijn voor een bepaalde sector of beleidsdomein, zoals de regeling die is opgezet in het kader van het Europees wereldwijd satellietnavigatiesysteem (GNSS) ([1]). De blauwdruk laat deze regelingen onverlet.

Leidende beginselen

Bij het streven naar de doelstellingen, het identificeren van de nodige activiteiten en het toewijzen van rollen en verantwoordelijkheden aan actoren of mechanismen, zijn de onderstaande leidende beginselen gevolgd; deze moeten ook in acht worden genomen wanneer toekomstige uitvoeringsrichtsnoeren worden opgesteld.

Evenredigheid: De meeste cyberincidenten die gevolgen hebben voor lidstaten zijn veel minder erg dan een nationale „crisis", laat staan een Europese. Het netwerk van Computer Security Incident Response Teams (CSIRT's), dat is opgericht bij de NIB-richtlijn ([2]), vormt de basis voor de samenwerking tussen lidstaten bij de respons op dergelijke incidenten. De nationale CSIRT's werken samen en wisselen op vrijwillige basis informatie uit, indien nodig ook in reactie op cyberincidenten die één of meer lidstaten treffen, overeenkomstig de standaardwerkwijzen van het CSIRT-netwerk. De blauwdruk moet daarom ten volle gebruikmaken van deze standaardwerkwijzen, en alle aanvullende taken die specifieke zijn voor cybercrises moeten in die werkwijzen tot uiting komen.

([1]) Besluit 2014/496/GBVB.
([2]) Richtlijn (EU) 2016/1148.

Subsidiariteit: Het subsidiariteitsbeginsel is van primordiaal belang. Het is in de eerste plaats de verantwoordelijkheid van de lidstaten om te reageren als zij getroffen worden door grootschalige cyberincidenten of -crises. Er is echter ook een belangrijke rol weggelegd voor de Commissie, de Europese Dienst voor extern optreden en de andere instellingen, bureaus, agentschappen en organen van de EU. Deze rol is duidelijk uiteengezet in de IPCR, maar vloeit ook voort uit de Uniewetgeving of simpelweg uit het feit dat cyberincidenten en -crises gevolgen kunnen hebben voor alle deelgebieden van de economische activiteit in de interne markt, voor de beveiliging en de internationale betrekkingen van de Unie en voor de instellingen zelf.

Complementariteit: De blauwdruk houdt volledig rekening met de bestaande crisisbeheersingsmechanismen, namelijk de regeling geïntegreerde politieke crisisrespons (IPCR), Argus en het Crisisresponsmechanisme van de EDEO; ook de recentelijk opgerichte structuren en mechanismen van de NIB-richtlijn, namelijk het CSIRT-netwerk, en de relevante EU-agentschappen en -organen, namelijk het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (het Enisa), het Europees Centrum voor de bestrijding van cybercriminaliteit, dat deel uitmaakt van Europol (Europol/EC3), het Centrum van de Europese Unie voor de analyse van inlichtingen (Intcen), de afdeling militaire inlichtingen van de EU (EUMS INT) en het Situatiecentrum (SitRoom), die samen de gezamenlijke capaciteit op het gebied van inlichtingenanalyse vormen, de EU-Fusiecel (die deel uitmaakt van Intcen) en het computercrisisteam voor de EU-instellingen en -agentschappen (CERT-EU) worden in de blauwdruk geïntegreerd. Daarbij moet de blauwdruk ervoor zorgen dat hun interactie en samenwerking zo complementair mogelijk is en zo weinig mogelijk overlappingen creëert.

Vertrouwelijke informatie: Alle informatie-uitwisseling in het kader van de blauwdruk moet voldoen aan de toepasselijke regels inzake beveiliging ([1]) en bescherming van persoonsgegevens en aan het verkeerslichtprotocol ([2]). Voor de uitwisseling van gerubriceerde informatie, ongeacht de toegepaste rubriceringsregeling, worden de beschikbare officieel erkende instrumenten gebruikt ([3]). De verwerking van persoonsgegevens moet voldoen aan de toepasselijke EU-regels, met name de algemene verordening gegevensbescherming ([4]), de e-privacyrichtlijn ([5]) en de verordening ([6])„betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door instellingen, organen, bureaus en agentschappen van de Unie en betreffende het vrije verkeer van die gegevens".

Kerndoelstellingen

De samenwerking in het kader van de blauwdruk volgt de bovenvermelde aanpak op drie niveaus: politiek, operationeel en technisch. Op elk niveau kan de samenwerking bestaan uit de uitwisseling van informatie en gezamenlijke acties om de onderstaande kerndoelstellingen te verwezenlijken.

— Een effectieve respons mogelijk maken. De respons kan vele vormen aannemen, van het identificeren van technische maatregelen waarbij twee of meer entiteiten samen de technische oorzaken van het incident onderzoeken (bijv. de analyse van malware) of het identificeren van manieren waarop organisaties kunnen nagaan of ze zijn getroffen (bijv. Indicators of Compromise), tot operationele besluiten over de toepassing van dergelijke technische maatregelen en, op politiek niveau, besluiten over de inzet van andere instrumenten, zoals de diplomatieke EU-respons op kwaadwillige cyberactiviteiten („instrumentarium voor cyberdiplomatie") of het operationeel EU-protocol voor de bestrijding van hybride bedreigingen, al naargelang het incident.

— Situatiebewustzijn delen. Het is van essentieel belang voor een gecoördineerde respons dat alle relevante belanghebbenden op de drie niveaus (technisch, operationeel, politiek) de gebeurtenissen die zich voordoen voldoende begrijpen. Situatiebewustzijn kan zowel betrekking hebben op de technologische aspecten van de oorzaken als op de gevolgen en oorsprong van het incident. Aangezien cyberincidenten gevolgen kunnen hebben voor tal van sectoren (financiën, energie, vervoer, gezondheidszorg enz.) is het van primordiaal belang dat de passende informatie, in het geschikte formaat, alle relevante belanghebbenden tijdig bereikt.

([1]) Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie (PB L 72 van 17.3.2015, blz. 41) en Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53). Besluit van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 19 april 2013 betreffende de beveiligingsvoorschriften voor de Europese Dienst voor extern optreden (PB C 190 van 29.6.2013, blz. 1). Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 274 van 15.10.2013, blz. 1).

([2]) https://www.first.org/tlp/

([3]) In juni 2016 waren hiervoor onder meer de transmissiekanalen CIMS (Classified Information Management System), ACID (encryptiealgoritme), RUE (beveiligd systeem voor de opstelling, uitwisseling en opslag van RESTREINT UE/EU RESTRICTED-documenten) en SOLAN beschikbaar. Andere instrumenten om gerubriceerde informatie te verzenden, zijn PGP of S/MIME.

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

([5]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([6]) Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1) — wordt momenteel herzien.

— Overeenstemming bereiken over belangrijke publieke communicatieberichten ([1]). Crisiscommunicatie speelt een belangrijke rol bij het beperken van de negatieve gevolgen van cyberincidenten en -crises, maar kan ook worden gebruikt om het gedrag van (potentiële) daders te beïnvloeden. Het gedrag van daders kan ook worden beïnvloed door in de berichtgeving duidelijk te wijzen op de waarschijnlijke diplomatieke gevolgen. De politieke respons zal alleen doeltreffend zijn wanneer de publieke communicatie om de negatieve gevolgen van cyberincidenten en -crises te beperken en de publieke communicatie om daders te beïnvloeden, op elkaar worden afgestemd. De verspreiding van praktische informatie over manieren waarop het publiek de gevolgen van een incident kan beperken (bijv. door een patch te installeren of aanvullende maatregelen te nemen om de dreiging af te wenden), is van zeer groot belang voor de cyberbeveiliging.

SAMENWERKING TUSSEN LIDSTATEN ONDERLING EN TUSSEN LIDSTATEN EN EU-ACTOREN OP TECHNISCH, OPERATIONEEL EN STRATEGISCH/POLITIEK NIVEAU

Een effectieve respons op grootschalige cyberincidenten of -crises op EU-niveau hangt af van effectieve technische, operationele en strategisch/politieke samenwerking.

Op elk niveau moeten de betrokken actoren specifieke activiteiten uitvoeren met betrekking tot de drie kerndoelstellingen:

— Gecoördineerde respons

— Gedeeld situatiebewustzijn

— Publieke communicatie

Tijdens het incident of de crisis zullen lagere samenwerkingsniveaus de hogere niveaus waarschuwen, informeren en ondersteunen; de hogere niveaus zullen de lagere niveaus aansturen ([2]) en besluiten nemen, in voorkomend geval.

Samenwerking op technisch niveau

Toepassingsgebied van de activiteiten:

— Aanpak van incidenten ([3]) tijdens een cybercrisis.

— Monitoring van en toezicht op incidenten, met inbegrip van permanente analyse van dreigingen en risico's.

Mogelijke actoren

In de blauwdruk is bepaald dat het CSIRT-netwerk, dat wordt voorgezeten door het EU-voorzitterschap en gebruik maakt van het secretariaat van het Enisa, op technisch niveau het centrale mechanisme is voor samenwerking.

— Lidstaten

  — De bij de NIB-richtlijn opgerichte bevoegde autoriteiten en centrale contactpunten

  — CSIRT's

— Organen/Bureaus/Agentschappen van de EU

  — Enisa

  — Europol/EC3

  — CERT-EU

([1]) Het is belangrijk erop te wijzen dat publieke communicatie zowel communicatie over het incident aan het brede publiek kan betekenen, als communicatie van meer technische of operationele informatie aan kritieke sectoren en/of getroffenen. Het is mogelijk dat hiervoor vertrouwelijke kanalen en specifieke technische instrumenten/platformen moeten worden gebruikt. Elke lidstaat heeft hoe dan ook zelf het recht en de verantwoordelijkheid om te communiceren met operatoren en het bredere publiek. Overeenkomstig het eerder uiteengezette subsidiariteitsbeginsel dragen de lidstaten en de nationale CSIRT's derhalve de eindverantwoordelijkheid voor de informatie die op hun grondgebied en onder hun doelgroep wordt verspreid.

([2]) „Toestemming om te handelen" — tijdens een cybercrisis zijn korte responstijden van essentieel belang om passende risicobeperkende maatregelen vast te stellen. Om deze korte responstijden te garanderen, kan een lidstaat vrijwillig een „toestemming om te handelen" geven aan een andere lidstaat; dit bekent dat die andere lidstaat onmiddellijk mag ingrijpen, zonder de hogere niveaus of EU-instellingen te hoeven raadplegen en alle normaal vereiste officiële kanalen te doorlopen, als dit niet vereist is voor een bepaald incident (een CSIRT hoeft bijvoorbeeld geen hogere niveaus te raadplegen om waardevolle informatie door te sturen naar een CSIRT in een andere lidstaat).

([3]) „Aanpak van incidenten": alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en respons op een incident.

— Europese Commissie

  — Het ERCC (een dienst binnen DG ECHO die 24/7 operationeel is) en de aangewezen leidende dienst (DG CNECT of DG HOME, al naargelang de specifieke aard van het incident), het secretariaat-generaal (Argus-secretariaat), DG HR (directoraat Beveiliging), DG DIGIT (IT-beveiliging).

  — Voor andere EU-agentschappen ([1]), het respectieve bevoegde DG in de Commissie of de EDEO (eerste aanspreekpunt).

— EDEO

  — SIAC (gezamenlijke capaciteit op het gebied van inlichtingenanalyse: EU Intcen en EUMS INT)

  — EU-situatiecentrum en de aangewezen geografische of thematische dienst

  — EU-Fusiecel voor analyse van hybride bedreigingen (onderdeel van Intcen — cyberbeveiliging in een hybride context)

Gedeeld situatiebewustzijn:

— In het kader van de regelmatige samenwerking op technisch niveau ter ondersteuning van het situatiebewustzijn van de Unie, moet het Enisa regelmatig het EU Cybersecurity Technical Situation Report over incidenten en bedreigingen opstellen, op basis van publiek beschikbare informatie en eigen analyses en verslagen die het ontvangt van de CSIRT's van de lidstaten (op vrijwillige basis) of de bij de NIB-richtlijn opgerichte centrale contactpunten, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol en CERT-EU, en, voor zover passend, het EU-centrum voor inlichtingen (Intcen) van de Europese Dienst voor extern optreden (EDEO). Dit verslag moet ter beschikking worden gesteld van de relevante instanties van de Raad, de Commissie, de HV/VV en het CSIRT-netwerk.

— In het geval van ernstige cyberincidenten stelt de voorzitter van het CSIRT-netwerk, met de hulp van het Enisa, een EU Cybersecurity Incident Situation Report ([2]) op dat wordt ingediend bij het voorzitterschap, de Commissie en de HV/VV via het roterende voorzitterschap van CSIRT.

— *Alle andere EU-agentschappen* brengen verslag uit aan hun bevoegde DG, dat op zijn beurt verslag uitbrengt aan de leidende dienst van de Commissie.

— *CERT-EU* stelt technische verslagen op voor het CSIRT-netwerk, de EU-instellingen en agentschappen (voor zover van toepassing) en Argus (indien geactiveerd).

— *Europol/EC3* ([3]) *en CERT-EU* stellen een deskundige forensische analyse van technische artefacten en andere technische informatie op voor het CSIRT-netwerk.

— EDEO SIAC: de EU-Fusiecel voor analyse van hybride bedreigingen brengt namens Intcen verslag uit aan de relevante diensten van de EDEO.

Respons:

— *Het CSIRT-netwerk* wisselt technische bijzonderheden en analyses van het incident uit, zoals IP-adressen, Indicators of Compromise ([4]) enz. Dergelijke informatie moet onverwijld aan het Enisa worden bezorgd, uiterlijk 24 uur nadat het incident werd vastgesteld.

— Overeenkomstig de standaardwerkwijzen van het CSIRT-netwerk, moeten de leden van het netwerk samen inspanningen leveren om de beschikbare technische artefacten en andere technische informatie over het incident te analyseren, teneinde de oorzaak ervan vast te stellen en mogelijke technische risicobeperkende maatregelen te nemen.

— Het Enisa maakt gebruik van zijn deskundigheid om te helpen bij de technische activiteiten van de CSIRT's, overeenkomstig zijn mandaat ([5]).

([1]) Afhankelijk van de aard van het incident en de gevolgen voor verschillende activiteitensectoren (financiën, vervoer, energie, gezondheidszorg enz.), worden de relevante EU-agentschappen of -organen bij de activiteiten betrokken.

([2]) Het EU Cybersecurity Incident Situation Report is een bundeling van nationale verslagen die door de nationale CSIRT's worden ingediend. Het formaat van het verslag moet worden vastgesteld in de standaardwerkwijzen van het CSIRT-netwerk

([3]) Overeenkomstig de voorwaarden en procedures die zijn uiteengezet in het juridisch kader van het EC3.

([4]) Indicator of Compromise (IOC) — in forensisch computeronderzoek is dit een artefact dat is waargenomen op een netwerk of in een besturingssysteem en dat hoogstwaarschijnlijk wijst op een inbraak in het computersysteem. Typische voorbeelden van IOC's zijn virushandtekeningen en IP-adressen, MD5-hashes, malwarebestanden of URL's of domeinnamen van botnet-servers.

([5]) Voorstel voor een verordening betreffende inzake Enisa, het EU-agentschap voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van informatie- en communicatietechnologie voor cyberbeveiliging („de cyberbeveiligingsverordening"), 13 september 2017.

— De CSIRT's van de lidstaten coördineren hun technische respons, met de hulp van het Enisa en de Commissie.

— EDEO SIAC: De EU-Fusiecel start namens het Intcen de procedure voor het verzamelen van eerste aanwijzingen.

Publieke mededelingen:

— De CSIRT's stellen technische adviezen ([1]) en kwetsbaarheidswaarschuwingen ([2]) op en verspreiden deze onder hun respectieve gemeenschappen en de bevolking nadat de toestemmingsprocedures die in elk geval van toepassing zijn, zijn doorlopen.

— Het Enisa faciliteert de opstelling en verspreiding van gemeenschappelijke berichten van het CSIRT-netwerk.

— Het Enisa coördineert zijn publieke communicatieactiviteiten met het CSIRT-netwerk en de dienst van de woordvoerder van de Commissie.

— Het Enisa en EC3 coördineren hun publieke communicatieactiviteiten op basis van het gedeelde situatiebewustzijn dat is overeengekomen tussen de lidstaten. Ze coördineren beide hun publieke communicatieactiviteiten met de dienst van de woordvoerder van de Commissie.

— Als de crisis een externe dimensie heeft of raakt aan het gemeenschappelijk Europees veiligheids- en defensiebeleid, dan moet de publieke communicatie worden gecoördineerd met de EDEO en de dienst van de woordvoerder van de HV/VV.

Samenwerking op operationeel niveau

Toepassingsgebied van de activiteiten:

— Besluitvorming op politiek niveau voorbereiden

— Het beheer van de cybercrisis coördineren (in voorkomend geval)

— De gevolgen en effecten op EU-niveau beoordelen en mogelijke risicobeperkende maatregelen voorstellen

Mogelijke actoren

— Lidstaten

  — De bij de NIB-richtlijn opgerichte bevoegde autoriteiten en centrale contactpunten

  — CSIRT's, cyberbeveiligingsagentschappen

  — Andere nationale sectorale instanties (in het geval van incidenten of crises die gevolgen hebben voor meerdere sectoren)

— Organen/Bureaus/Agentschappen van de EU

  — Enisa

  — Europol/EC3

  — CERT-EU

— Europese Commissie

  — de (Adjunct) Secretaris-generaal SG (Argus-proces)

  — DG CNECT/HOME

  — De veiligheidsautoriteit van de Commissie

  — Andere DG's (in het geval van incidenten of crises die gevolgen hebben voor meerdere sectoren)

([1]) Technisch advies met betrekking tot de oorzaken van het incident en mogelijke risicobeperkende maatregelen.
([2]) Informatie over de technische kwetsbaarheid die wordt misbruikt om IT-systemen negatief te beïnvloeden.

— EDEO

  — de (Adjunct) secretaris-generaal voor crisisbeheersing en SIAC (EU Intcen en EUMS INT)

  — EU-Fusiecel voor analyse van hybride bedreigingen

— Raad

  — het voorzitterschap (horizontale werkgroep van het voorzitterschap inzake cyberbedreigingen of Coreper ([1])) ondersteund door het SGR, of PVC ([2]) en — indien geactiveerd — met de steun van de IPCR;

Situatiebewustzijn:

— De opstelling van politiek-strategische verslagen ondersteunen (bijv. het ISAA in het geval van de activering van de IPCR);

— De *Horizontale Groep cybervraagstukken* bereidt de vergadering van het Coreper of het PVC voor, al naargelang van toepassing.

— Indien de IPCR wordt geactiveerd,

  — kan het voorzitterschap rondetafelvergaderingen organiseren om zijn voorbereidingen voor het Coreper of PVC te ondersteunen, waarbij relevante belanghebbenden in de lidstaten, de instellingen, de agentschappen en derde partijen zoals niet-EU-landen en internationale organisaties kunnen worden betrokken. Crisisvergaderingen worden georganiseerd om knelpunten op te sporen en voorstellen voor acties met betrekking tot horizontale aangelegenheden op te stellen.

  — De *leidende dienst van de Commissie of de EDEO*, als leidende dienst van ISAA, stelt het ISAA-verslag op, met bijdragen van het Enisa, het CSIRT-netwerk, Europol/EC3, EUMS INT, Intcen en alle andere relevante actoren. In het ISAA-verslag wordt op basis van correlaties van technische incidenten en crisisbeoordelingen (dreigingsanalyse, risicobeoordeling, niet-technische gevolgen en effecten, niet-cybergebonden aspecten van het incident of de crisis enz.) een EU-brede beoordeling gemaakt die specifiek is afgestemd op de behoeften van het operationele en politieke niveau.

— Indien Argus wordt geactiveerd,

  — dragen CERT-EU en EC3 ([3]) rechtstreeks bij tot de uitwisseling van informatie binnen de Commissie.

— Indien het Crisisresponsmechanisme van de EDEO wordt geactiveerd,

  — zal het SIAC intensiever informatie verzamelen, de informatie uit alle bronnen bundelen en een analyse en beoordeling van het incident opstellen.

Respons (op verzoek van het politieke niveau):

— grensoverschrijdende samenwerking met het centrale contactpunt en de nationale bevoegde autoriteiten (NIB-richtlijn) om de gevolgen en effecten te beperken.

— Alle technische beperkende maatregelen activeren en de technische capaciteiten coördineren die nodig zijn om de gevolgen van gerichte aanvallen op informatiesystemen te stoppen of in te perken.

— Samenwerking en, indien zo besloten, coördinatie van technische capaciteiten om tot een gezamenlijke of op samenwerking gebaseerde respons te komen, overeenkomstig de ***standaardwerkwijzen van het CSIRT-netwerk***.

— De behoefte aan samenwerking met relevante derde partijen beoordelen.

— (indien geactiveerd) Besluitvorming volgens het Argus-proces.

— (indien geactiveerd) Besluiten voorbereiden en coördineren volgens de IPCR.

— (indien geactiveerd) De besluitvorming van de EDEO ondersteunen via het Crisisresponsmechanisme van de EDEO, ook wat betreft de contacten met derde landen en internationale organisaties, en alle maatregelen die gericht zijn op de bescherming van missies en activiteiten van het gemeenschappelijk Europees veiligheids- en defensiebeleid en de EU-delegaties.

([1]) Het Comité van permanente vertegenwoordigers (Coreper, artikel 240 van het Verdrag betreffende de werking van de Europese Unie — VWEU) is verantwoordelijk voor de voorbereiding van de werkzaamheden van de Raad van de Europese Unie.

([2]) Het Politiek en Veiligheidscomité is een comité van de Raad van de Europese Unie dat actief is op het gebied van het buitenlands- en veiligheidsbeleid, zoals vermeld in artikel 38 van het Verdrag betreffende de Europese Unie.

([3]) Overeenkomstig de voorwaarden en procedures die zijn uiteengezet in het juridisch kader van EC3.

Publieke mededelingen:

— Overeenstemming bereiken over publieke communicatie met betrekking tot het incident.

— Als de crisis een externe dimensie heeft of raakt aan het gemeenschappelijk Europees veiligheids- en defensiebeleid, dan moet de publieke communicatie worden gecoördineerd met de EDEO en de dienst van de woordvoerder van de HV/VV.

Samenwerking op strategisch/politiek niveau

Mogelijke actoren

— Voor lidstaten: de ministers die bevoegd zijn voor cyberbeveiliging

— Voor de Europese Raad: de voorzitter

— Voor de Raad: het roterende voorzitterschap

— Met betrekking tot maatregelen uit het instrumentarium voor cyberdiplomatie: het PVC en de Horizontale Groep

— Voor de Europese Commissie: de voorzitter of de afgevaardigde vicevoorzitter/commissaris.

— De hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid/vicevoorzitter van de Commissie

Toepassingsgebied van de activiteiten: Strategisch en politiek beheer van zowel de cybergebonden als niet-cybergebonden aspecten van de crisis, met inbegrip van maatregelen in het kader van een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten.

Gedeeld situatiebewustzijn:

— Nagaan welk effect de door de crisis veroorzaakte verstoringen hebben op de werking van de Unie.

Respons:

— Aanvullende crisisbeheersingsmechanismen/-instrumenten activeren, al naargelang van de aard en gevolgen van het incident. Het kan bijvoorbeeld gaan om het mechanisme voor civiele bescherming.

— Maatregelen nemen in het kader van een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten.

— Noodsteun ter beschikking stellen van getroffen lidstaten, bijvoorbeeld door het cyberbeveiligingsnoodfonds te activeren ([1]), zodra dit is opgericht.

— Samenwerking en coördinatie met internationale organisaties, indien van toepassing, zoals de Verenigde Naties (VN), de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en met name de NAVO.

— Gevolgen voor de nationale veiligheid en defensie analyseren.

Publieke communicatie:

Beslissen over een gemeenschappelijke communicatiestrategie voor het publiek.

GECOÖRDINEERDE RESPONS MET DE LIDSTATEN OP EU-NIVEAU IN HET KADER VAN DE IPCR

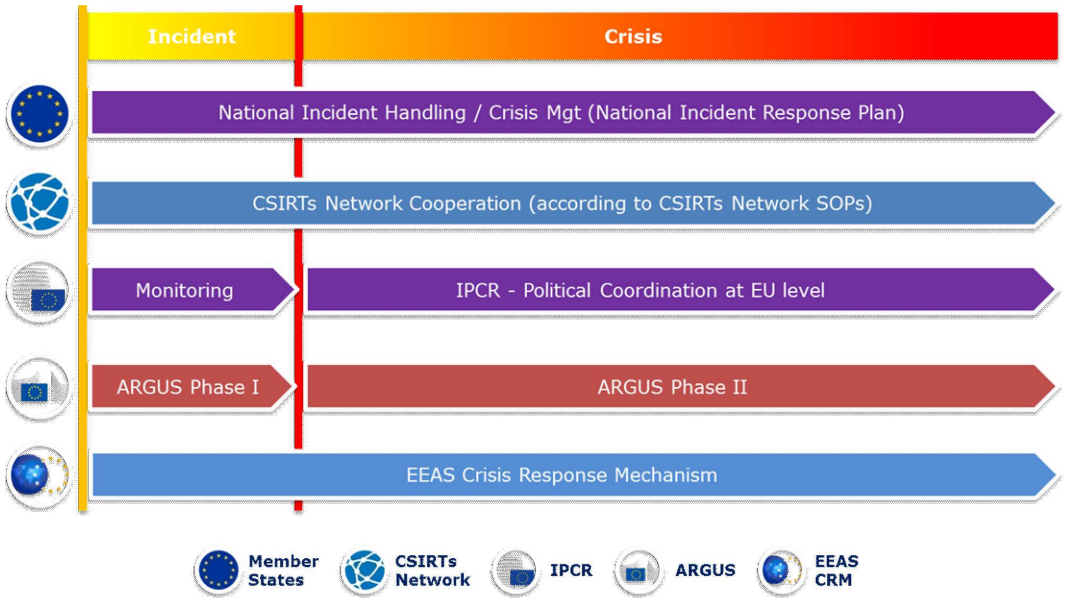
Overeenkomstig het beginsel van complementariteit op EU-niveau, wordt in dit deel dieper ingegaan op de kerndoelstellingen en de verantwoordelijkheden en activiteiten van de autoriteiten van de lidstaten, het CSIRT-netwerk, het Enisa, CERT-EU, Europol/EC3, Intcen, de EU-Fusiecel voor analyse van hybride bedreigingen en de Horizontale Groep cybervraagstukken van de Raad binnen het IPCR-proces. De actoren worden geacht te handelen overeenkomstig vastgestelde procedures op EU- of nationaal niveau.

Het is van essentieel belang erop te wijzen dat, zoals aangegeven in figuur 1, de activiteiten op nationaal niveau en de samenwerking in het CSIRT-netwerk (indien nodig), ongeacht de activering van de EU-crisisbeheersingsmechanismen, tijdens elk incident of elke crisis worden uitgevoerd volgens de beginselen van subsidiariteit en evenredigheid.

([1]) Het cyberbeveiligingsnoodfonds is een actie die wordt voorgesteld in de gezamenlijke mededeling „Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU”, JOIN(2017) 450/1.

Figuur 1

Respons op EU-niveau op een cyberincident/-crisis



Alle hierna beschreven activiteiten moeten worden uitgevoerd overeenkomstig de standaardwerkwijzen/regels van de betrokken samenwerkingsmechanismen, en in overeenstemming met de gevestigde mandaten en bevoegdheden van de afzonderlijke actoren en instellingen. Het is mogelijk dat deze procedures/regels op sommige punten moeten worden aangevuld/gewijzigd om tot de best mogelijke samenwerking te komen en effectief te kunnen reageren op grootschalige cyberincidenten en -crises.

Het is mogelijk dat niet alle hierna gepresenteerde actoren actie moeten ondernemen tijdens een specifiek incident. Niettemin moeten de blauwdruk en de relevante standaardwerkwijzen van de samenwerkingsmechanismen erop voorzien zijn dat dit wel het geval is.

Aangezien niet alle cyberincidenten of -crises dezelfde impact hebben op de samenleving, moeten de sectorale actoren op alle niveaus zeer flexibel inzetbaar zijn en is de respons afhankelijk van zowel cybergebonden als niet-cybergebonden risicobeperkende maatregelen.

Beheer van cybercrises — Cyberbeveiliging integreren in het IPCR-proces

De IPCR-regelingen, die worden beschreven in de IPCR-standaardwerkwijzen, volgen de hierna beschreven stappen ([1]) (of sommige stappen al dan niet nodig zijn, hangt af van de situatie).

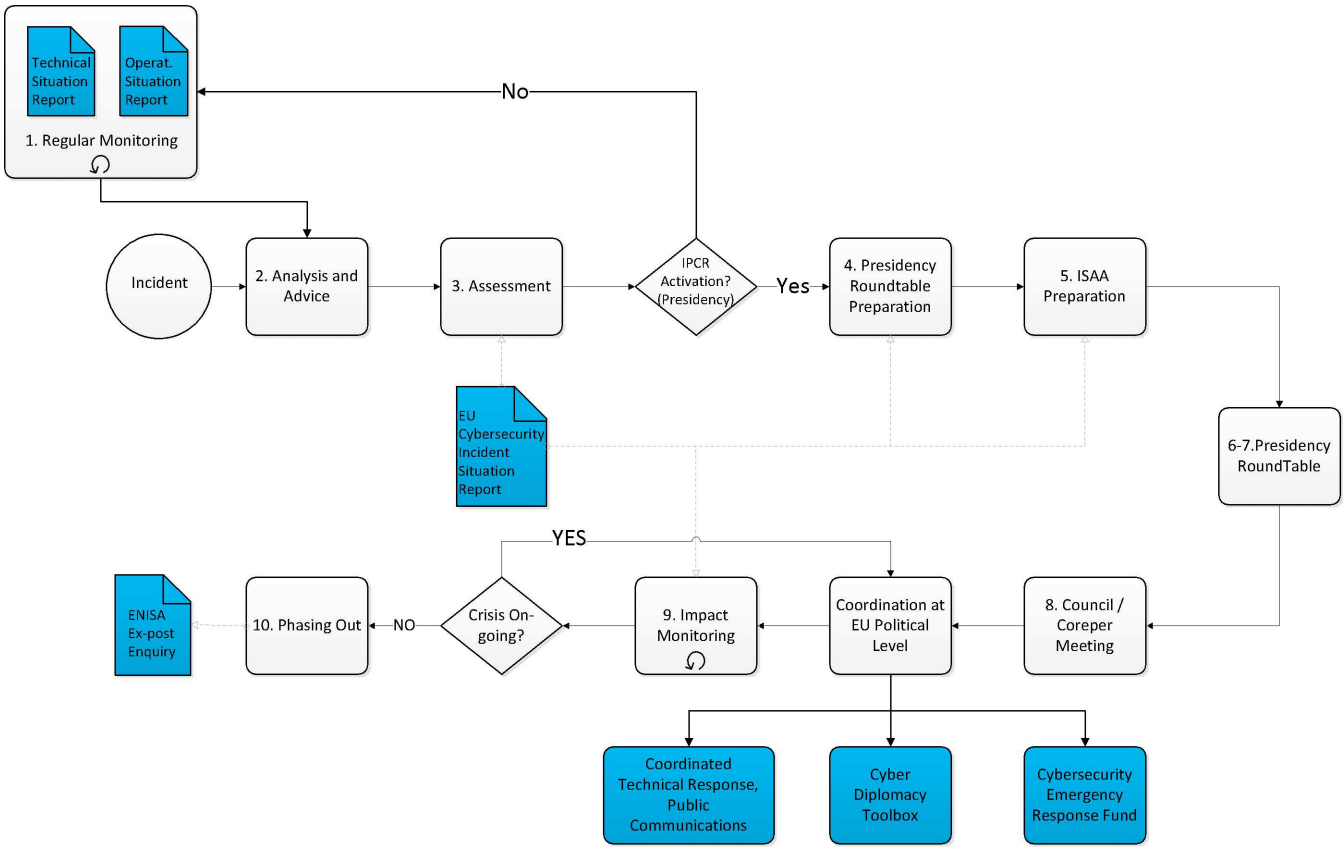
In elke stap worden specifieke activiteiten en actoren op het gebied van cyberveiligheid vermeld. Voor het gemak van de lezer wordt in elke stap de tekst van de IPCR-standaardwerkwijzen getoond, gevolgd door de activiteiten die specifiek zijn voor de blauwdruk. Deze stapsgewijze benadering maakt het ook mogelijk om duidelijk bestaande **hiaten** op te sporen in de noodzakelijke capaciteiten en procedures, die een effectieve respons op cybercrises verhinderen.

Figuur 2 (zie hieronder) ([2]) is een grafische voorstelling van het IPCR-proces, waarbij nieuwe elementen zijn aangegeven in het blauw.

([1]) Uit document 12607/15 „IPCR-standaardwerkwijzen", overeengekomen door de Groep vrienden van het voorzitterschap, waarvan het Coreper in oktober 2015 nota heeft genomen.
([2]) Zie het aanhangsel voor een grotere versie van de figuur.

Figuur 2

Elementen van de IPCR die specifiek zijn voor cyberbeveiliging



Noot: Gezien de aard van hybride bedreigingen op cybergebied, die ontworpen zijn om onder de drempel van een herkenbare crisis te blijven, moet de EU preventieve en paraatheidsmaatregelen nemen. De EU-Fusiecel voor analyse van hybride bedreigingen krijgt de opdracht om snel relevante incidenten te analyseren en de passende coördinatiestructuren op de hoogte te brengen. De regelmatige rapportering van de Fusiecel kan informatie helpen verschaffen voor de sectorale beleidsvorming, teneinde de paraatheid te verbeteren.

— **Stap 1 — Regelmatige sectorale monitoring en waarschuwing**: de bestaande, regelmatige sectorale situatieverslagen en waarschuwingen geven het voorzitterschap van de Raad indicaties over een ontwikkelende crisis en de mogelijke evolutie ervan.

— **Vastgestelde hiaten**: Er zijn momenteel geen regelmatige en gecoördineerde situatieverslagen en waarschuwingen met betrekking tot cyberincidenten (en dreigingen) op EU-niveau.

— **Blauwdruk: Monitoring/rapportering van de situatie op het gebied van cyberbeveiliging in de EU**

— **Het Enisa stelt regelmatig een technisch situatieverslag op over cyberincidenten en -dreigingen in de EU**, op basis van publiek beschikbare informatie en eigen analyses en verslagen die het ontvangt van de CSIRT's van de lidstaten (op vrijwillige basis) of de bij de NIB-richtlijn opgerichte centrale contactpunten, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol, CERT-EU en het EU-centrum voor inlichtingen (Intcen) van de Europese dienst voor extern optreden (EDEO). Dit verslag moet ter beschikking worden gesteld van de relevante instanties van de Raad, de Commissie en het CSIRT-netwerk.

— De EU-Fusiecel voor analyse van hybride bedreigingen moet namens SIAC een **operationeel situatieverslag over cyberbeveiliging in de EU** opstellen. Dit verslag ondersteunt ook het kader voor een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten.

— Beide verslagen worden ter beschikking gesteld van de EU en de nationale belanghebbenden, om hun eigen situatiebewustzijn te verbeteren, informatie te verstrekken met het oog op besluitvorming en grensoverschrijdende regionale samenwerking te faciliteren.

Nadat een incident is vastgesteld

— **Stap 2 — Analyse en advies**: op basis van beschikbare monitoring en waarschuwingen houden de diensten van de Commissie, de EDEO en het SGR elkaar op de hoogte van mogelijke ontwikkelingen, teneinde klaar te zijn om het voorzitterschap te adviseren over te gaan tot een activering van de IPCR (volledig of in de modus informatie-uitwisseling);

— **Blauwdruk:**

— Voor de Commissie, DG CNECT, DG HOME, DG HR.DS en DG DIGIT, ondersteund door het Enisa, EC3 en CERT-EU.

— EDEO. Voortbouwend op het werk van SitRoom en inlichtingendiensten verschaft de EU-Fusiecel voor analyse van hybride bedreigingen situatiebewustzijn over werkelijke en potentiële hybride bedreigingen die gevolgen hebben voor de EU en haar partners, met inbegrip van cyberbedreigingen. Als uit de analyse en beoordeling van de EU-Fusiecel voor analyse van hybride bedreigingen blijkt dat er een mogelijke dreiging tegen een richtlijn, partnerland of organisatie bestaat, verstrekt Intcen (in de eerste plaats) informatie op operationeel niveau, volgens gevestigde procedures. Het operationeel niveau stelt dan aanbevelingen op voor het politiek-strategische niveau, met inbegrip van de mogelijke activering van crisisbeheersingsmaatregelen in monitoring-modus (bijv. het Crisisresponsmechanisme van de EDEO of de monitoringpagina van de IPCR).

— In het geval van ernstige cyberincidenten stelt de voorzitter van het CSIRT-netwerk, met de hulp van het Enisa, een EU Cybersecurity Incident Situation Report ([1]) op, dat wordt ingediend bij het voorzitterschap, de Commissie en de HV/VV via het roterende voorzitterschap van CSIRT.

— **Stap 3 — Beoordeling/Besluit over de activering van de IPCR**: het voorzitterschap beoordeelt de behoefte aan politieke coördinatie, informatie-uitwisseling of besluitvorming op EU-niveau. Daartoe kan het voorzitterschap een informele rondetafelvergadering beleggen. Het voorzitterschap gaat in de eerste plaats na op welke gebieden optreden van het Coreper of de Raad nodig is. Dit vormt de basis van de richtsnoeren voor de opstelling van geïntegreerde situatiekennis- en -analyseverslagen (ISAA). In het licht van de kenmerken van de crisis, de mogelijke gevolgen en de aanverwante politieke behoeften, beslist het voorzitterschap of het gepast is vergaderingen van de relevante groepen van de Raad en/of het Coreper en/of het PVC te beleggen.

— **Blauwdruk:**

— Deelnemers aan de rondetafel:

— De diensten van de Commissie en de EDEO adviseren het voorzitterschap over hun respectieve bevoegdheidsterreinen.

— De vertegenwoordigers van de lidstaten in de horizontale groep cybervraagstukken, ondersteund door deskundigen uit de hoofdsteden (CSIRT's, instanties die bevoegd zijn voor cyberbeveiliging, andere).

— Politieke/strategische richtsnoeren voor ISAA-verslagen op basis van het meest recente EU Cybersecurity Incident Situation Report en aanvullende informatie van deelnemers aan de rondetafel.

— Relevante groepen en comités:

— Horizontale groep cybervraagstukken.

De Commissie, de EDEO en het SGR kunnen, met volledige instemming van en in samenspraak met het voorzitterschap, ook besluiten de IPCR te activeren in de modus informatie-uitwisseling door een crisispagina te genereren, teneinde het pad te effenen voor een mogelijke volledige activering.

— **Stap 4 — Activering van de IPCR/Informatieverzameling en -uitwisseling**: na activering (volledig of in de modus informatie-uitwisseling) wordt een crisispagina gegenereerd op het IPCR-webplatform, teneinde specifieke informatie-uitwisselingen mogelijk te maken die gericht zijn op aspecten die zullen bijdragen tot ISAA, en voorbereidingen te treffen voor de besprekingen op politiek niveau. Wie de leiding heeft over ISAA (een van de diensten van de Commissie of de EDEO) hangt af van de omstandigheden van het geval.

— **Stap 5 — Opstelling van ISAA-verslagen**: de opstelling van ISAA-verslagen wordt geïnitieerd. De Commissie/de EDEO geven ISAA-verslagen uit, zoals uiteengezet in de ISAA-standaardwerkwijzen, en kunnen de informatie-uitwisseling verder bevorderen op het IPCR-webplatform, of specifieke verzoeken om informatie doen. De ISAA-

([1]) Het EU Cybersecurity Incident Situation Report is een bundeling van nationale verslagen die door de nationale CSIRT's worden ingediend. Het formaat van het verslag moet worden vastgesteld in de standaardwerkwijzen van het CSIRT-netwerk.

verslagen worden afgestemd op de behoeften van het politieke niveau (d.w.z. Coreper of de Raad), zoals gedefinieerd door het voorzitterschap en uiteengezet in zijn richtsnoeren, waardoor een strategisch overzicht en een geïnformeerd debat over de door het voorzitterschap vastgestelde agendapunten mogelijk wordt. Overeenkomstig de ISAA-standaardwerkwijzen, zal de aard van de cybercrisis bepalen of het ISAA-verslag wordt voorbereid door een van de diensten van de Commissie (DG CNECT, DG HOME) of door de EDEO.

Na de activering van de IPCR geeft het voorzitterschap de specifieke domeinen aan waaraan ISAA aandacht moet schenken om de politieke coördinatie en/of het besluitvormingsproces in de Raad te ondersteunen. Het voorzitterschap zal ook de timing van het verslag aangeven, na overleg met de diensten van de Commissie/de EDEO;

— **Blauwdruk:**

— Het ISAA-verslag bevat bijdragen van relevante diensten, zoals:

— Het CSIRT-netwerk, in de vorm van het EU Cybersecurity Incident Situation Report.

— EC3, SitRoom, de EU-Fusiecel voor analyse van hybride bedreigingen, CERT-EU. De EU-Fusiecel voor analyse van hybride bedreigingen levert bijdragen tot en ondersteunt de leidende ISAA-dienst en de IPCR-rondetafel, voor zover van toepassing.

— Sectorale agentschappen en organen van de EU, al naargelang de getroffen sectoren.

— Instanties van de lidstaten (andere dan de CSIRT's).

— Het verzamelen van ISAA-input ([1]):

— Commissie en EU-agentschappen: het IT-systeem Argus vormt het interne kernnetwerk voor ISAA. De EU-agentschappen sturen hun bijdragen naar hun bevoegde DG's, die op hun beurt de relevante informatie invoeren in Argus. De diensten van de Commissie en de Agentschappen verzamelen informatie uit bestaande sectorale netwerken van de lidstaten en internationale organisaties en uit andere relevante bronnen.

— Voor de EDEO: het EU-situatiecentrum, ondersteund door de andere relevante afdelingen van de EDEO, vormt het interne kernnetwerk en het centrale contactpunt voor ISAA. De EDEO verzamelt informatie van derde landen en relevante internationale organisaties.

— **Stap 6 — Voorbereiding van de informele rondetafel van het voorzitterschap**: het voorzitterschap, bijgestaan door het secretariaat-generaal van de Raad, zal de timing, agenda, deelnemers en de verwachte resultaten (mogelijke concrete resultaten) van de informele rondetafelvergadering van het voorzitterschap bepalen. Het SGR geeft relevante informatie namens het voorzitterschap door op het IPCR-webplatform en stelt met name de notulen van de vergadering op.

— **Stap 7 — Rondetafel van het voorzitterschap/voorbereidende maatregelen voor politieke coördinatie/besluitvorming van de EU**: het voorzitterschap zal een informele rondetafel bijeenroepen om de situatie te beoordelen en om de punten die onder de aandacht van het Coreper of de Raad moeten worden gebracht, voor te bereiden en te beoordelen. De informele rondetafel van het voorzitterschap is ook het forum waarop alle voorstellen voor actie die bij het Coreper/de Raad zijn ingediend, worden beoordeeld en besproken.

— **Blauwdruk:**

— De Horizontale Groep cybervraagstukken bereidt het Coreper of het PVC voor.

— **Stap 8 — Politieke coördinatie en besluitvorming in het Coreper/de Raad**: de resultaten van de vergaderingen van het Coreper/de Raad hebben betrekking op de coördinatie van de respons op alle niveaus, besluiten over buitengewone maatregelen, politieke verklaringen enz. Deze besluiten vormen ook geactualiseerde politieke/strategische richtsnoeren voor de verdere opstelling van ISAA-verslagen.

— **Blauwdruk:**

— Het politieke besluit om de respons op de cybercrisis te coördineren, wordt ten uitvoer gelegd via de activiteiten (uitgevoerd door de overeenkomstige actoren) die zijn beschreven onder **Respons** en **Publieke communicatie** van het bovenstaande punt 1 „Samenwerking op strategisch/politiek, operationeel en technisch niveau".

— Voor de opstelling van ISAA-verslagen zijn de activiteiten noodzakelijk die in punt 1 zijn beschreven onder de noemer **situatiebewustzijn**, op technisch, operationeel en politiek/strategisch niveau.

([1]) ISAA-standaardwerkwijzen.

— **Stap 9 — Monitoring van de gevolgen**: de leidende ISAA-dienst zal, met de steun van ISAA-medewerkers, informatie verstrekken over de evolutie van de crisis en de gevolgen van de genomen politieke beslissingen. Deze feedback ondersteunt een proces in ontwikkeling; het voorzitterschap baseert zich op deze feedback bij zijn besluit of de betrokkenheid van het politieke niveau van de EU moet worden voortgezet of de IPCR moet worden teruggeschroefd.

— **Stap 10 — Uitfasering**: volgens hetzelfde proces als dat voor de activering kan het voorzitterschap een informele rondetafel bijeenroepen om te beoordelen of de IPCR actief moet blijven of niet. Het voorzitterschap kan beslissen de activering te stoppen of terug te schroeven.

— **Blauwdruk:**

— Het Enisa kan worden verzocht om bij te dragen tot een ex-post technisch onderzoek van het incident of dit onderzoek zelf uit te voeren, overeenkomstig zijn mandaat.

AANHANGSEL

1. CRISISBEHEERSING, SAMENWERKINGSMECHANISMEN EN ACTOREN OP HET NIVEAU VAN DE EU

Crisisbeheersingsmechanismen

Regeling geïntegreerde politieke crisisrespons (IPCR): de regeling geïntegreerde politieke crisisrespons (IPCR), die op 25 juni 2013 door de Raad is aangenomen ([1]), is ontworpen om op het politieke niveau van de EU een tijdige coördinatie en respons op een grote crisis te faciliteren. De IPCR ondersteunt ook de coördinatie op politiek niveau van de respons op de activering van de solidariteitsclausule (artikel 222 VWEU), zoals gedefinieerd in het op 24 juni 2014 vastgestelde Besluit 2014/415/EU van de Raad inzake de regeling voor de toepassing van de solidariteitsclausule door de Unie. Het activeringsproces en de acties die vervolgens moeten worden ondernomen, zijn uiteengezet in de IPCR-standaardwerkwijzen ([2]).

Argus: het crisiscoördinatiesysteem dat in 2005 door de Europese Commissie is opgericht om te zorgen voor specifieke coördinatie in het geval van een grote crisis die meerdere sectoren treft. Dit systeem wordt ondersteund door een algemeen systeem voor snelle waarschuwing (een IT-instrument) dat dezelfde naam draagt. Argus valt uiteen in twee fasen, waarbij fase II (in het geval van een grote crisis die meerdere sectoren treft) aanleiding geeft tot vergaderingen van het Crisiscoördinatiecomité (CCC), onder het gezag van de voorzitter van de Commissie of een commissaris aan wie de verantwoordelijkheid is overgedragen. Het CCC bestaat uit vertegenwoordigers van de relevante DG's van de Commissie, kabinetten en andere EU-diensten, die zorgen voor de aansturing en coördinatie van de respons van de Commissie op de crisis. Onder het voorzitterschap van de adjunct secretaris-generaal beoordeelt het CCC de situatie, weegt het de opties tegen elkaar af, neemt het praktische besluiten met betrekking tot de EU-instrumenten onder de bevoegdheid van de Commissie, en zorgt het ervoor dat deze besluiten ten uitvoer worden gelegd ([3]) ([4]).

Crisisresponsmechanisme van de EDEO: het Crisisresponsmechanisme van de EDEO is een gestructureerd systeem dat de EDEO in staat stelt te reageren op crises en noodgevallen van externe aard of met een belangrijke externe dimensie — met inbegrip van hybride bedreigingen — die gevolgen (kunnen) hebben voor de belangen van de EU of de lidstaten. Door te zorgen voor de deelname van relevante ambtenaren van de Commissie en het secretariaat van de Raad aan zijn vergaderingen, faciliteert het Crisisresponsmechanisme (CRM) synergieën tussen enerzijds de diplomatieke, beveiligings- en defensie-inspanningen, en anderzijds de door de Commissie beheerde financiële, handels- en samenwerkingsinstrumenten. De Crisiscel kan worden geactiveerd voor de duur van de crisis.

Samenwerkingsmechanismen

CSIRT-netwerk: het Computer Security Incident Response Team Network groepeert alle nationale en gouvernementele CSIRT's en CERT-EU. Het doel van dit netwerk is de uitwisseling van informatie over dreigingen en cyberincidenten tussen de CSIRT's mogelijk te maken en te verbeteren, en samen te werken bij de respons op cyberincidenten en -crises.

Horizontale Groep cybervraagstukken van de Raad: de horizontale groep werd opgericht om te zorgen voor strategische en horizontale coördinatie van cyberbeleidsthema's in de Raad, en kan zowel bij wetgevende als bij niet-wetgevende activiteiten worden betrokken.

Actoren

Enisa: het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging werd opgericht in 2004. Het Agentschap werkt nauw samen met de lidstaten en de privésector om advies te geven en oplossingen aan te reiken voor kwesties als de pan-Europese cyberbeveiligingsoefeningen, de ontwikkeling van nationale cyberbeveiligingsstrategieën, de samenwerking tussen CSIRT's en capaciteitsopbouw. Het Enisa werkt rechtstreeks samen met CSIRT's in de hele EU en is het secretariaat van het CSIRT-netwerk.

ERCC: het Coördinatiecentrum voor respons in noodsituaties van de Commissie (onder het directoraat-generaal voor Civiele Bescherming en Humanitaire Hulp — DG ECHO) ondersteunt en coördineert een breed gamma aan preventie-, paraatheids- en responsactiviteiten op 24/7-basis. Het centrum werd opgericht in 2013 en vormt het centrale knooppunt van de crisisrespons van de Commissie; het staat in verbinding met andere crisiscentra in de EU en is 24/7 actief als centraal IPCR-contactpunt.

([1]) Finale toetsing van de EU-regeling inzake coördinatie bij crisis- en noodsituaties (CCA): de EU-regeling geïntegreerde politieke-crisisbestrijding (IPCR), 10708/13, door de Raad aangenomen op 24 juni 2013.

([2]) 12607/15 „IPCR-standaardwerkwijzen", overeengekomen door de Groep vrienden van het voorzitterschap, waarvan het Coreper in oktober 2015 nota heeft genomen.

([3]) Bepalingen van de Commissie betreffende het algemeen systeem voor snelle waarschuwing „Argus", COM(2005) 662 def. van 23 december 2005.

([4]) Besluit 2006/25/EG, Euratom van de Commissie van 23 december 2005 tot wijziging van haar Reglement van orde (PB L 19 van 24.1.2006, blz. 20), betreffende instelling van het algemeen systeem voor snelle waarschuwing „Argus".

Europol/EC3: Het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) is in 2013 opgericht binnen Europol en ondersteunt de respons van de ordehandhavingsdiensten op cybercriminaliteit in de EU. EC3 verstrekt operationele en analytische ondersteuning voor de onderzoeken van lidstaten en doet dienst als centraal knooppunt voor criminele informatie en inlichtingen ter ondersteuning van activiteiten en onderzoeken van de lidstaten; het verschaft operationele analyse, coördinatie, deskundigheid en hooggespecialiseerde technische en digitale forensische ondersteuning.

CERT-EU: het Computer Emergency Response Team van de EU-instellingen, organen en agentschappen heeft als opdracht de bescherming van de EU-instellingen, organen en agentschappen tegen cyberdreigingen te verbeteren. Het is lid van het CSIRT-netwerk. CERT-EU heeft technische overeenkomsten gesloten over de uitwisseling van informatie over cyberdreigingen met NATO CIRC, bepaalde derde landen en grote commerciële spelers op het vlak van cyberbeveiliging.

De inlichtingengemeenschap van de EU bestaat uit het EU-Centrum voor de analyse van inlichtingen (**Intcen**) en het directoraat Inlichtingen van de Militaire Staf van de EU (EUMS INT), in het kader van de regeling voor de **gezamenlijke capaciteit op het gebied van inlichtingenanalyse** (SIAC). SIAC heeft als opdracht analyses van inlichtingen, vroegtijdige waarschuwingen en situatiebewustzijn te verstrekken aan de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de Europese Dienst voor extern optreden (EDEO). SIAC biedt zijn diensten aan aan de verschillende EU-besluitvormingsorganen op het gebied van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB), het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) en terrorismebestrijding, en aan de lidstaten. EU Intcen en EUMS INT zijn geen operationele agentschappen en beschikken niet over de capaciteiten om inlichtingen te verzamelen. Het operationele niveau van de inlichtingendiensten is de verantwoordelijkheid van de lidstaten. SIAC heeft alleen betrekking op strategische analyses.

EU-Fusiecel voor analyse van hybride bedreigingen: in de gezamenlijke mededeling inzake de bestrijding van hybride bedreigingen van april 2016 wordt de EU-Fusiecel voor analyse van hybride bedreigingen (EU HFC) aangewezen als het contactpunt voor alle bronnenanalyse over hybride bedreigingen in de EU: het mandaat van de EU-Fusiecel voor analyse van hybride bedreigingen is in december 2016 goedgekeurd door de Commissie via een dienstenoverkoepelende raadpleging. De EU-Fusiecel voor analyse van hybride bedreigingen is gevestigd in Intcen, maakt deel uit van SIAC en werkt dus samen met EUMS INT; er is een permanent militair lid toegewezen aan de EU-Fusiecel. „Hybride" verwijst naar het opzettelijk gebruik door staten of niet-overheidsactoren van een combinatie van meerdere geheime/open, militaire/civiele instrumenten en hefbomen, zoals cyberaanvallen, desinformatiecampagnes, spionage, economische druk, het gebruik van derde partijen om verantwoordelijkheid af te schuiven of andere subversieve activiteiten. De EU HFC maakt gebruik van een uitgebreid netwerk van contactpunten, zowel in de Commissie als de lidstaten, om te zorgen voor de geïntegreerde respons/overheidsbrede benadering die nodig is om het hoofd te bieden aan diverse uitdagingen.

EU-SitRoom: het EU-situatiecentrum maakt deel uit van het EU-Centrum voor de analyse van inlichtingen (EU Intcen) en verstrekt operationele capaciteit aan de EDEO om te zorgen voor een onmiddellijke en effectieve respons op crises. Het is een civiel-militair orgaan dat permanent stand-by is en 24/7 over de hele wereld monitoring en situatiebewustzijn verstrekt.

Relevante instrumenten

Kader voor een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten: het kader, waarover in juni 2017 overeenstemming is bereikt, maakt deel uit de EU-aanpak van cyberdiplomatie en draagt aldus bij tot de preventie van conflicten, de beperking van de risico's van cyberdreigingen en grotere stabiliteit in de internationale betrekkingen. Het kader maakt volledig gebruik van de maatregelen van het gemeenschappelijk buitenlands en veiligheidsbeleid, waaronder — indien nodig — restrictieve maatregelen. Het gebruik van de maatregelen van het kader moet zorgen voor samenwerking en inperking van dreigingen op zeer korte en langere termijn, en moet het gedrag van daders en potentiële daders op lange termijn beïnvloeden.

2. COÖRDINATIE VAN CYBERCRISES IN DE IPCR — HORIZONTALE COÖRDINATIELAAG EN POLITIEKE ESCALATIE

De IPCR kan worden gebruikt (en is gebruikt) om technische en operationele problemen op te lossen, maar altijd vanuit een politiek/strategische invalshoek.

Bij een escalerende crisis kan de IPCR worden aangepast aan de ernst van de crisis, door van „monitoring-modus" over te gaan naar „modus informatie-uitwisseling", het eerste niveau van de IPCR-activering, tot „volledige IPCR-activering".

De beslissing om over te gaan tot volledige activering wordt genomen door het roterende voorzitterschap van de Raad. De Commissie, de EDEO en het SGR kunnen de IPCR activeren in de modus informatie-uitwisseling. Monitoring en

informatie-uitwisseling leiden tot verschillende niveaus van informatie-uitwisseling, waarbij informatie-uitwisseling de vraag naar de opstelling van ISAA-verslagen activeert. De volledige activering voegt rondetafelvergaderingen toe aan het instrumentarium, waardoor het voorzitterschap aan tafel komt (meestal de voorzitter van Coreper II of een deskundige op het niveau van de permanente vertegenwoordigers, maar in uitzonderlijke gevallen zijn ook rondetafels op ministerniveau georganiseerd).

Actoren

Het roterende voorzitterschap (meestal de voorzitter van het Coreper) heeft de leiding

Voor de Europese Raad: het kabinet van de voorzitter

Voor de Europese Commissie: DSG/DG-niveau en/of deskundigen ter zake

Voor de EDEO, DSG/MD-niveau en/of deskundigen ter zake

Voor het SGR: het kabinet van het secretariaat-generaal, het IPCR-team en de bevoegde DG's

Toepassingsgebied van de activiteiten: Een gemeenschappelijk geïntegreerd beeld van de situatie scheppen, het bewustzijn van knelpunten of tekortkomingen op elk van de drie niveaus vergroten teneinde ze aan te pakken op politiek niveau, besluiten aan tafel stimuleren als deze binnen de bevoegdheid van de deelnemers vallen, of voorstellen voor actie opstellen die naar het Coreper II en de Raad gaan.

Gedeeld situatiebewustzijn:

(Niet actief): IPCR-monitoringpagina's kunnen worden gegenereerd om de ontwikkeling te volgen van situaties die kunnen escaleren tot een crisis met gevolgen voor de EU.

(IPCR in modus informatie-uitwisseling): Op basis van input van de diensten van de Commissie, de EDEO en de lidstaten (via de IPCR-vragenlijsten) stelt de leidende ISAA-dienst ISAA-verslagen op.

(Volledige activering van de IPCR): In aanvulling op de ISAA-verslagen brengen rondetafels verschillende actoren uit de lidstaten, de Commissie, de EDEO, de relevante agentschappen enz. bijeen om tekortkomingen en knelpunten te bespreken.

Samenwerking en respons:

Aanvullende crisisbeheersingsmechanismen/-instrumenten activeren/synchroniseren, al naargelang van de aard en gevolgen van het incident. Het kan bijvoorbeeld gaan om het mechanisme voor civiele bescherming, het kader voor een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten of het „gezamenlijk kader voor de bestrijding van hybride bedreigingen".

Crisiscommunicatie:

Het IPCR-netwerk van crisisvoorlichters kan worden geactiveerd door het voorzitterschap, in samenspraak met de relevante diensten in de Commissie, het SGR en de EDEO, teneinde de opstelling van gemeenschappelijke berichten te ondersteunen of overleg te plegen over de meeste effectieve communicatie-instrumenten.

3. BEHEER VAN CYBERCRISES IN ARGUS — INFORMATIE-UITWISSELING BINNEN DE EUROPESE COMMISSIE

Naar aanleiding van onverwachte crises die actie op Europees niveau vereisten (de terroristische aanslagen in Madrid in maart 2004, de tsunami in Zuidoost-Azië in december 2004 en de terroristische aanslagen in Londen in juli 2005), heeft de Commissie in 2005 het Argus-coördinatiesysteem opgericht, ondersteund door het gelijknamige systeem voor snelle waarschuwing ([1]) ([2]). Dit heeft tot doel te voorzien in een specifiek **crisiscoördinatieproces** in het geval van grote multisectorale crises, dat het mogelijk maakt crisisgerelateerde informatie in realtime uit te wisselen en snel besluiten te nemen.

Argus maakt een onderscheid tussen twee fasen, al naargelang de ernst van de gebeurtenis:

Fase I: wordt gebruikt voor de uitwisseling van informatie over een crisis van beperkte omvang

([1]) Commissie van de Europese Gemeenschappen, 23 december 2005, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Bepalingen van de Commissie betreffende het algemeen systeem voor snelle waarschuwing „Argus", COM(2005) 662 definitief.

([2]) Besluit 2006/25/EG, Euratom.

Voorbeelden van recentelijk gerapporteerde gebeurtenissen van fase I zijn de bosbranden in Portugal en Israël, de aanslag in Berlijn in 2016, de overstromingen in Albanië, orkaan Matthew in Haïti en de droogte in Bolivia. Elk DG kan een gebeurtenis van fase I openen als het van oordeel is dat een situatie op zijn bevoegdheidsdomein ernstig genoeg is om informatie uit te wisselen. DG CNECT of DG HOME kunnen bijvoorbeeld een gebeurtenis van fase I openen als zij van oordeel zijn dat een cybersituatie op hun respectieve bevoegdheidsdomein ernstig genoeg is om informatie uit te wisselen.

Fase II: wordt gebruikt voor grote crises die meerdere sectoren treffen of voor voorspelbare of nakende dreigingen voor de Unie.

Fase II brengt een specifiek coördinatieproces op gang, dat de Commissie in staat stelt besluiten te nemen en over te gaan tot een snelle, gecoördineerde en coherente respons op het hoogste niveau van haar bevoegdheidsdomein en in samenwerking met de andere instellingen. Fase II is bedoeld voor grote crises die meerdere sectoren treffen of voor voorspelbare of nakende dreigingen. Voorbeelden van echte gebeurtenissen van fase II zijn de migratie-/vluchtelingencrisis die sinds 2015 aan de gang is, de drievoudige ramp in Fukushima (2011) en de uitbarsting van de vulkaan *Eyjafjallajökull* in IJsland (2010).

Fase II wordt door de voorzitter geactiveerd, op eigen initiatief of op verzoek van een lid van de Commissie. De voorzitter kan de politieke verantwoordelijkheid voor de respons van de Commissie overdragen aan de commissaris van de dienst die het meest is betrokken bij de crisis, of kan de verantwoordelijkheid zelf opnemen.

In fase II vinden spoedvergaderingen van het Crisiscoördinatiecomité (CCC) plaats. Deze vergaderingen worden bijeengeroepen door de voorzitter of de commissaris aan wie de verantwoordelijkheid is overgedragen. De vergaderingen worden belegd door het SG via het IT-instrument van Argus. Het CCC is een specifieke operationele structuur voor crisisbeheer die wordt ingesteld om de respons van de Commissie op een crisis te leiden en te coördineren, en die is samengesteld uit vertegenwoordigers van de betrokken directoraten-generaal van de Commissie, kabinetten en andere EU-diensten. Onder het voorzitterschap van de adjunct secretaris-generaal **beoordeelt het CCC de situatie, weegt het de opties tegen elkaar af en neemt het besluiten, zorgt het ervoor dat de besluiten en acties ten uitvoer worden gelegd** en ziet het toe op de coherentie en consistentie van de respons. Het SG verleent steun aan het CCC.

4. CRISISRESPONSMECHANISME VAN DE EDEO

Het Crisisresponsmechanisme van de EDEO (CRM) wordt geactiveerd wanneer zich een ernstige situatie of noodgeval voordoet dat raakt aan de externe dimensie van de EU. Het CRM wordt geactiveerd door de adjunct secretaris-generaal voor crisisbeheersing, na overleg met de HV/VV of de secretaris-generaal. De HV/VV, het SG of een andere adjunct secretaris-generaal of MD kunnen de adjunct secretaris-generaal voor crisisbeheersing ook vragen om het crisisresponsmechanisme te activeren.

Het CRM draagt bij tot de coherentie van de EU-respons op crises, binnen de veiligheidsstrategie. Het CRM faciliteert met name synergieën tussen diplomatieke, beveiligings- en defensie-inspanningen aan de hand van financiële, handels- en samenwerkingsinstrumenten die door de Commissie worden beheerd.

Het CRM is gekoppeld aan het algemene systeem voor de respons op noodgevallen (Argus) en de regeling geïntegreerde politieke crisisrespons (IPCR), zodat synergieën kunnen worden benut in het geval van gelijktijdige activering. Het Situatiecentrum in de EDEO doet dienst als communicatieknooppunt tussen de EDEO en de systemen voor respons op noodgevallen in de Raad en de Commissie.

Wanneer het CRM wordt geactiveerd, wordt meestal eerst een **crisisvergadering** bijeengeroepen tussen de leidende managers van de EDEO, de Commissie en de Raad die getroffen zijn door de crisis in kwestie. In deze crisisvergadering worden de gevolgen van de crisis op korte termijn beoordeeld en kan worden besloten onmiddellijk actie te ondernemen, de Crisiscel te activeren of het Crisisplatform bijeen te roepen. Dit kan in willekeurige volgorde gebeuren.

De **Crisiscel** is een kleinschalige controlekamer waar vertegenwoordigers van de EDEO en de diensten van de Commissie en de Raad die betrokken zijn bij de respons op de crisis samenkomen om de situatie permanent te volgen, zodat steun kan worden verleend aan de besluitvormers in het EDEO-hoofdkwartier. Wanneer de Crisiscel wordt geactiveerd, is ze zeven dagen per week en 24 uur per dag operationeel.

Het **Crisisplatform** brengt relevante diensten van de EDEO, de Commissie en de Raad bijeen om de gevolgen van de crisis op middellange en lange termijn te beoordelen en overeenstemming te bereiken over de te nemen maatregelen. Het Crisisplatform wordt voorgezeten door de HV/VV of de secretaris-generaal, of door de adjunct secretaris-generaal voor crisisbeheersing. Het Crisisplatform beoordeelt de effectiviteit van EU-maatregelen in landen of regio's die door de crisis zijn getroffen, beslist over wijzigingen van de maatregelen of aanvullende maatregelen en bespreekt voorstellen voor maatregelen van de Raad. Het Crisisplatform is een ad-hocvergadering; het is dus niet permanent geactiveerd.

De **Taskforce** is samengesteld uit vertegenwoordigers van de diensten die betrokken zijn bij de respons en kan worden geactiveerd om de tenuitvoerlegging van de EU-respons te volgen en te faciliteren. Zij beoordeelt de gevolgen van het optreden van de EU, bereidt beleidsdocumenten en keuzenota's voor, draagt bij tot de voorbereiding van het politiek kader voor crisisaanpak (Political Framework for Crisis Approach, PFCA) en tot de Communicatiestrategie, en stelt andere regelingen vast die de tenuitvoerlegging van de EU-respons kunnen faciliteren.

5. REFERENTIEDOCUMENTEN

Hierna volgt een lijst referentiedocumenten waarmee rekening is gehouden bij de opstelling van de blauwdruk:

— The European Cyber Crises Cooperation Framework, Versie 1, 17 oktober 2012.

— Report on Cyber Crisis Cooperation and Management, Enisa, 2014.

— Actionable Information for Security Incident Response, Enisa, 2014.

— Common practices of EU-level crisis management and applicability to cyber crises, Enisa, 2015.

— Strategies for Incident Response and Cyber Crisis Cooperation, Enisa, 2016.

— EU Cyber Standard Operating Procedures, Enisa, 2016.

— A good practice guide of using taxonomies in incident prevention and detection, Enisa, 2017.

— Mededeling „Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche", COM(2016) 410 final, 5 juli 2016.

— Conclusies van de Raad over de versterking van het Europese cyberweerbaarheidssysteem en bevordering van een concurrerende en innovatieve cyberbeveiligingssector — Conclusies van de Raad (15 november 2016), 14540/16.

— Besluit 2014/415/EU van de Raad van 24 juni 2014 inzake de regeling voor de toepassing van de solidariteitsclausule door de Unie (PB L 192 van 1.7.2014, blz. 53).

— Finale toetsing van de EU-regeling inzake coördinatie bij crisis- en noodsituaties (CCA): de EU-regeling geïntegreerde politieke-crisisbestrijding (IPCR), 10708/13, 7 juni 2013.

— Integrated Situational Awareness and Analysis (ISAA) — Standard Operating Procedures, DS 1570/15, 22 oktober 2015.

— Bepalingen van de Commissie betreffende het algemeen systeem voor snelle waarschuwing „Argus", COM(2005) 662 definitief van 23 december 2005.

— Besluit 2006/25/EG, Euratom van de Commissie van 23 december 2005 tot wijziging van haar Reglement van orde (PB L 19 van 24.1.2006, blz. 20).

— Argus Modus Operandi, Europese Commissie, 23 oktober 2013.

— Ontwerpconclusies van de Raad over een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten („Instrumentarium voor cyberdiplomatie"), Doc. 9916/17.

— Operationeel EU-protocol voor de bestrijding van hybride bedreigingen, „EU-draaiboek", SWD(2016) 227.

— EEAS Crisis Response Mechanism, 8 november 2016 [Ares(2017)880661]. Gezamenlijk werkdocument van de diensten van de EU „operationeel EU-protocol voor de bestrijding van hybride bedreigingen", EU-draaiboek, SWD(2016) 227 final van 5 juli 2016.

— Gezamenlijke mededeling aan het Europees Parlement en de Raad: Gezamenlijk kader voor de bestrijding van hybride bedreigingen: een reactie van de Europese Unie, JOIN/2016/018 final, 6 april 2016.

— EEAS(2016) 1674 — Working Document of the European External Action Service — EU Hybrid Fusion Cell — Terms of Reference

6. ELEMENTEN VAN HET IPCR-PROCES DIE SPECIFIEK ZIJN VOOR CYBERBEVEILIGING