Raad van de
Europese Unie

Brussel, 9 juni 2017
(OR. en)

9986/17

GENVAL 63
CYBER 92

NOTA

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
Betreft:	Zevende wederzijdse evaluatie De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit – Ontwerp-eindverslag

Overeenkomstig artikel 2 van Gemeenschappelijk Optreden 97/827/JBZ van 5 december 1997[1] heeft de Groep algemene aangelegenheden, waaronder evaluatie (GENVAL) op 3 oktober 2013 besloten de zevende wederzijdse evaluatie te wijden aan de praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit.

Voor de delegaties gaat hierbij het ontwerp van eindverslag over de zevende wederzijdse evaluatie. Dit document omvat de conclusies en de aanbevelingen van de eerder opgestelde landspecifieke rapporten.

[1] Gemeenschappelijk Optreden 97/827/JBZ van 5 december 1997 vastgesteld door de Raad op grond van artikel K.3 van het Verdrag betreffende de Europese Unie tot instelling van een mechanisme voor evaluatie van de uitvoering en toepassing op nationaal niveau van de internationale verbintenissen inzake de bestrijding van de georganiseerde criminaliteit (PB L 344 van 15.12.1997).

Het door het secretariaat-generaal van de Raad opgestelde ontwerp van eindverslag zal op 13 juni 2017 worden voorgelegd aan de Groep GENVAL, met het oog op een eerste gedachtewisseling.

De delegaties zal worden verzocht **uiterlijk op 3 juli 2017** schriftelijke opmerkingen over het ontwerp van eindverslag in te dienen bij het secretariaat-generaal van de Raad (secretariat.mutual-evaluation@consilium.europa.eu en giovanna.giglio@consilium.europa.eu).

De definitieve versie van het rapport zal aan het Coreper en de Raad worden voorgelegd ter informatie over de resultaten van de evaluatie. Er wordt aan herinnerd dat de Raad, indien hij dat nodig acht, overeenkomstig de in artikel 8, lid 3, van Gemeenschappelijk Optreden 97/827/JBZ neergelegde procedure aanbevelingen tot de betrokken lidstaat kan richten en hem kan verzoeken mee te delen welke vorderingen binnen de door de Raad vastgestelde termijn zijn gemaakt.

Overeenkomstig artikel 8, lid 4, van bovengenoemd gemeenschappelijk optreden dient het eindverslag tevens ter informatie aan het Europees Parlement te worden toegezonden.

Eindverslag over de zevende wederzijdse evaluatie inzake "De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit"

INHOUDSOPGAVE

I - INLEIDING

In overeenstemming met Gemeenschappelijk Optreden 97/827/JHA van 5 december 1997 tot instelling van een mechanisme voor evaluatie van de uitvoering en toepassing op nationaal niveau van de internationale verbintenissen inzake de bestrijding van de georganiseerde criminaliteit, wordt in dit rapport gepoogd de bevindingen en aanbevelingen van de zevende ronde van wederzijdse evaluaties samen te vatten en er conclusies uit te trekken.

Overeenkomstig artikel 2 van bovengenoemd gemeenschappelijk optreden heeft de Groep algemene aangelegenheden, waaronder evaluatie (GENVAL) op 3 oktober 2013 besloten de zevende wederzijdse evaluatie te wijden aan de praktische uitvoering en toepassing van de Europese beleidsmaatregelen inzake preventie en bestrijding van cybercriminaliteit.

De keuze van cybercriminaliteit als thema voor de zevende wederzijdse evaluatie is door de lidstaten gunstig onthaald. Omdat onder "cybercriminaliteit" een breed spectrum aan misdrijven valt, werd overeengekomen dat bij de evaluatie het accent zal liggen op misdrijven die volgens de lidstaten speciale aandacht behoeven. Daartoe bestrijkt de evaluatie hoofdzakelijk drie specifieke gebieden: cyberaanvallen, online seksueel misbruik van kinderen/kinderpornografie en online kaartfraude, en moet zij uitgebreid ingaan op de juridische en operationele aspecten van het tegengaan van cybercriminaliteit, op grensoverschrijdende samenwerking en op samenwerking met ter zake deskundige EU-instanties. Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie[2] (omzettingsdatum 18 december 2013) en Richtlijn 2013/40/EU over aanvallen op informatiesystemen[3] (omzettingsdatum 4 september 2015), zijn in dit verband met name van belang.

[2] PB L 335 van 17.12.2011, blz. 1.
[3] PB L 218 van 14.8.2013, blz. 8.

De vragenlijst voor de zevende wederzijdse evaluatie is door GENVAL op 27 november 2013 en 22 januari 2014 besproken en vervolgens via een stilzwijgende procedure goedgekeurd op 31 januari 2014. GENVAL heeft de volgorde van de bezoeken, behoudens bepaalde aanpassingen, en de samenstelling van de evaluatieteams met betrekking tot de waarnemers op 1 april 2014 goedgekeurd.

Overeenkomstig artikel 3 van Gemeenschappelijk Optreden 97/827/JHA hebben de lidstaten deskundigen met uitgebreide praktische kennis op dit gebied aangesteld, na een schriftelijk verzoek aan de delegaties door het hoofd van de eenheid DG D 2B van het secretariaat-generaal van de Raad op 28 januari 2014. Per missie hebben drie nationale deskundigen aan de evaluatie deelgenomen. Andere deskundigen, van de Commissie, Eurojust, Europol en Enisa, hebben aan sommige evaluatiemissies deelgenomen als waarnemers. Het secretariaat-generaal van de Raad heeft de missies gecoördineerd en heeft er met één of twee personeelsleden per evaluatie aan deelgenomen; voorts heeft het secretariaat-generaal het proces voorbereid en de deskundigen ondersteund.

De eerste evaluatiemissie vond plaats in Frankrijk van 28 tot en met 31 oktober 2014.
De laatste evaluatiemissie vond plaats in Zweden van 27 tot en met 30 september 2016.
Na elke evaluatiemissie is een gedetailleerd rapport over de betrokken lidstaat opgesteld.
De evaluatierapporten zijn vervolgens in de Groep GENVAL besproken en aangenomen[4].
De meeste rapporten zijn beschikbaar op de website van de Raad en voor het publiek toegankelijk.

[4] Frankrijk (7588/2/15 REV 1 DCL 1); Nederland (7587/15 DCL 1); VK (10952/2/15 REV 2 DCL 1); Roemenië (13022/1/15 REV 1 DCL 1); Slowakije (9761/1/15 REV 1 DCL 1); Estland (10953/15 DCL 1); Slovenië (14586/1/16 REV 1 DCL 1); Italië (9955/1/16 REV 1 DCL 1); Spanje (6289/1/16 REV 1 DCL 1); Bulgarije (5156/1/16 REV 1 DCL 1); Litouwen (6520/1/16 REV 1 DCL 1); Malta (7696/1/16 REV 1 DCL 1); Griekenland (14584/1/16 REV 1 DCL 1); Kroatië (5250/1/17 REV 1 DCL 1); Portugal (10905/1/16 REV 1 DCL 1); Cyprus (9892/1/16 REV 1 DCL 1); Polen (14585/1/16 REV 1 DCL 1); Tsjechische Republiek (13203/1/16 REV 1 DCL 1); Hongarije (14583/1/16 REV 1 DCL 1); Letland (5387/1/17 REV 1 DCL 1); Denemarken (13204/1/16 REV 1 DCL 1 + COR 1); België (8212/1/17 REV 1); Oostenrijk (8185/1/17 REV 1); Duitsland (7159/1/17 REV 1 DCL 1); Luxemburg (7162/1/17 REV 1 DCL 1); Ierland (7160/1/17 REV 1 DCL 1); Finland (8178/17); Zweden (8188/17 REV 1).

Dit document geeft de conclusies en de aanbevelingen weer van de eerder opgestelde landspecifieke rapporten[5]. Er zij echter opgemerkt dat gezien het langdurige karakter van de evaluatie, de landenrapporten niet altijd de huidige stand van zaken weergeven.

[5] De landenrapporten zijn onmiddellijk na de bezoeken aan de lidstaten opgesteld. De kans bestaat dat nieuwe ontwikkelingen, zoals de voltooiing van de uitvoering van wetgeving, achteraf hebben plaatsgevonden en niet in de landenrapporten zijn opgenomen.
Die ontwikkelingen dienen in de follow-up, die 18 maanden na de goedkeuring van de evaluatierapporten moet worden opgesteld, te worden meegenomen. Bij de bespreking van het verslag in de Groep GENVAL hebben de lidstaten vaak (toekomstige) maatregelen aangekondigd ter uitvoering van de aanbevelingen in hun individuele verslag.

II - SAMENVATTING

- Als gevolg van het frequentere internetgebruik is cybercriminaliteit een steeds toenemend misdaadfenomeen, en er ontstaan nieuwe trends, werkwijzen en criminaliteitsvormen, zowel cybergerelateerde inbreuken, waarvan de juridische definitie stelt dat zij een aspect van cybercriminaliteit omvatten, als gedigitaliseerde strafbare feiten, zijnde gewone inbreuken zijn waarvoor informatietechnologie is gebruikt. Vooruitgang boeken in de strijd tegen cyber-criminaliteit vereist derhalve in alle landen een hoog niveau van politieke wil, financiële inspanningen en een belangrijke investering in personele en technische middelen.

- Uit de evaluatie is gebleken dat alle lidstaten de strijd tegen cybercriminaliteit ernstig nemen, en dat zij daartoe over structuren, middelen en maatregelen beschikken. De graad van inzet en efficiëntie verschilt echter per lidstaat, en in sommige gevallen is er ruimte voor verbetering met betrekking tot bepaalde aspecten van de algehele aanpak ter bestrijding van cybercriminaliteit. Tegelijkertijd is tijdens de zevende evaluatie een aantal gemeenschappelijke problemen en uitdagingen geconstateerd, die als volgt kunnen worden samengevat.

- Op het tijdstip van de evaluatie beschikte de meerderheid van de lidstaten over een nationale strategie voor cyberbeveiliging, die een kader biedt voor het vastleggen van de nationale prioriteiten en het invoeren van de belangrijkste coördinatiestructuren op strategisch en operationeel niveau ter bestrijding van cybercriminaliteit en met het oog op cyberveerkracht; een aantal lidstaten was daar nog mee bezig. Sommige lidstaten hadden ook een actieplan aangenomen voor de uitvoering van de nationale strategie voor cyberbeveiliging.

- Op het tijdstip van de evaluatie hadden de meeste lidstaten het in 2001 door de Raad van Europa aangenomen Verdrag van Boedapest inzake cybercriminaliteit, en het aanvullende protocol daarbij, betreffende de strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen, ondertekend en geratificeerd. De lidstaten die dat nog niet hadden gedaan, werd verzocht deze instrumenten te ondertekenen en te ratificeren.

- Een van de belangrijkste geconstateerde tekortkomingen betreft het verzamelen van afzonderlijke statistieken over cybercriminaliteit en cyberbeveiliging, aangezien de reeds beschikbare statistieken in de meeste lidstaten ontoereikend, gefragmenteerd en onvergelijkbaar zijn. Er zijn betrouwbare statistieken nodig om cybercriminaliteit te overzien, te monitoren, en de trends en ontwikkelingen erin te analyseren, teneinde passende maatregelen te nemen en de doeltreffendheid van het rechtssysteem voor de bestrijding van deze vorm van criminaliteit te beoordelen. De lidstaten werd daarom aanbevolen specifieke en alomvattende statistieken te verzamelen voor cybercriminaliteit in de verschillende fasen van de procedure, op basis van een gestandaardiseerde aanpak.

- Gezien de snelle ontwikkeling van de informatietechnologie, met steeds geavanceerdere methoden, en de complexiteit van cybercriminaliteit, is het belangrijk dat de beroeps-beoefenaars in deze sector een hoge graad van specialisatie hebben. Volgens de bevindingen van de evaluatie is het niveau van specialisatie in het algemeen voldoende of toereikend voor de rechtshandhavingsautoriteiten, terwijl er ruimte voor verbetering is wat betreft de rechterlijke macht, gelet op het feit dat cybercriminaliteit in verschillende lidstaten door openbare ministeries en strafrechtbanken wordt behandeld. De lidstaten is daarom aanbevolen het niveau van specialisatie van hun gerechtelijk personeel dat zich met gevallen van cybercriminaliteit bezighoudt, te verhogen.

- Om dezelfde redenen is uit de evaluatie het belang gebleken van regelmatige en voortdurende gespecialiseerde opleiding inzake cybercriminaliteit, zowel voor de rechtshandhavings-instanties als voor de rechterlijke macht, onder meer door optimaal gebruik te maken van de opleidingsmogelijkheden die worden geboden door EU-instanties zoals EC3/Europol, ECTEG, Eurojust, OLAF en Cepol.

- In de evaluatie is benadrukt dat nauwe en doeltreffende interinstitutionele coördinatie en samenwerking op basis van een door meerdere instanties gedragen benadering op strategisch en operationeel niveau tussen alle relevante publieke en particuliere belanghebbenden die betrokken zijn bij cybercriminaliteit en cyberbeveiliging, een belangrijk element is voor een efficiënte bestrijding van cybercriminaliteit en om ervoor te zorgen dat het nationaal cyberbeveiligings-systeem voldoende weerbaar is tegen cyberbedreigingen. In sommige lidstaten is een dergelijke samenwerking echter nog onvoldoende ontwikkeld of kan zij verder worden verbeterd.

- Met het oog daarop zijn de lidstaten ook aangemoedigd om de oprichting te overwegen van een centrale instantie/entiteit waarin zowel de publieke als de particuliere sector is vertegenwoordigd, om de activiteiten op dit gebied te coördineren.

- Nauwe samenwerking tussen de publieke en de particuliere sector - financiële instellingen en banken, telecombedrijven, internetproviders, ngo's, de academische wereld, het bedrijfsleven, beroepsverenigingen, enz. - is in dit verband essentieel, aangezien hun deskundigheid van grote toegevoegde waarde is voor het welslagen van onderzoeken en acties om cyberincidenten op te lossen. De meest geavanceerde vormen van samenwerking met de particuliere sector zijn geïnstitutionaliseerd door de oprichting van passende instellingen/werkgroepen. De beoordelaars hebben publiek-private partnerschappen aangemerkt als een belangrijk instrument voor een goede samenwerking tussen de rechtshandhavingsautoriteiten en de particuliere sector.

- Sommige lidstaten hebben rechtstreeks contact met in het buitenland gevestigde internet-providers, met name in de V.S., maar de samenwerking met dergelijke bedrijven is vrij problematisch omdat zij niet op elk verzoek antwoorden of omdat zij een verzoek om wederzijdse rechtshulp/een rogatoire commissie of een gerechtelijk bevel nodig hebben om de gevraagde informatie te verstrekken; uit de evaluatie is derhalve duidelijk gebleken dat de EU en haar lidstaten moeten nadenken over hoe ze die samenwerking kunnen verbeteren.

- Het toenemende gebruik van encryptie met geavanceerdere technieken wordt in alle lidstaten een steeds groter probleem, aangezien dit de toegang tot relevante informatie betreffende internet- of cybercriminaliteit bemoeilijkt of geheel verhindert. Decryptie is slechts mogelijk aan de hand van gespecialiseerde hardware en software die grote capaciteit vereisen, en uit de evaluatie is gebleken dat er slechts beperkt succes wordt geboekt bij het aanpakken van encryptie, vooral in meer complexe gevallen. Veel lidstaten maken gebruik van het decryptieplatform van Europol, het EU-cybercrimecentrum (EC-3). Volgens de bevindingen van de evaluatie kunnen de problemen die encryptie stelt gedeeltelijk worden verholpen met meer onderzoek en ontwikkeling en het ontwikkelen van nieuwe methoden, en met goede samenwerking tussen de verschillende betrokken instanties. De lidstaten en de EU-instellingen kregen tevens de aanbeveling om het opstellen van een decryptiebevel te overwegen.

- De aard van elektronisch bewijsmateriaal, en het gemak waarmee het kan worden gemanipuleerd of vervalst, kunnen problemen met betrekking tot de ontvankelijkheid ervan scheppen, die zich niet bij andere types bewijsmateriaal voordoen. Daarom zijn er in sommige lidstaten specifieke voorschriften betreffende het verzamelen van elektronisch bewijsmateriaal, opdat dit in de rechtbank ontvankelijk is. Uit de evaluatie is echter gebleken dat het procedurele recht in de meeste lidstaten technologieneutraal is, wat betekent dat er algemene regels en beginselen worden toegepast op het verzamelen van bewijsmateriaal en dat het procedure-systeem geen specifieke formele regels bevat inzake de ontvankelijkheid en de beoordeling van elektronisch bewijsmateriaal.

- In bepaalde lidstaten maakt de nationale wetgeving het mogelijk gegevens van abonnees rechtstreeks van buitenlandse providers te verkrijgen, terwijl in andere lidstaten de procedures voor wederzijdse rechtshulp moeten worden gevolgd, die sneller en doeltreffender zouden moeten zijn. De lidstaten is verzocht ervoor te zorgen dat hun nationale wetgeving voldoende flexibel is om de ontvankelijkheid van elektronisch bewijsmateriaal te faciliteren, ook wanneer het van een ander land is verkregen.

- Uit de evaluatie is gebleken dat in de "cloud" gepleegde cybermisdrijven in het algemeen moeilijk te onderzoeken en te vervolgen zijn, omdat het voor de rechtshandhavingsinstanties lastig is om de informatie in de "cloud" op te sporen en er toegang toe te krijgen. Afhankelijk van het type cybercriminaliteit kunnen er jurisdicties van verschillende staten, ook buiten de EU, bij betrokken zijn. Er kunnen zich derhalve rechtsbevoegdheidsgeschillen voordoen waarvoor om de bijstand van Eurojust en het EJN kan worden verzocht. Uit de evaluatie bleek dat het belangrijk is deze uitdagingen op EU-niveau aan te pakken.

- De evaluatie heeft de zorgen van de lidstaten bevestigd met betrekking tot de afwezigheid van een gemeenschappelijk juridisch kader inzake gegevensbewaring op EU-niveau. Dit heeft gevolgen voor de doeltreffendheid van strafrechtelijke onderzoeken en vervolgingen, met name wat betreft de betrouwbaarheid en de ontvankelijkheid in de rechtbank van bewijsmateriaal dat is gebaseerd op het verzamelen van gegevens over elektronische communicatie, alsmede voor grensoverschrijdende justitiële samenwerking. Momenteel is een gemeenschappelijk reflectieproces aan de gang waarbij de EU-instellingen en de lidstaten zijn betrokken, teneinde de kwestie van gegevensbewaring aan te pakken om juridische en praktische oplossingen te vinden voor de problemen die voortvloeien uit de jurisprudentie van het Hof van Justitie van de Europese Unie.

- Online seksueel misbruik van kinderen, in zijn verschillende gedaanten, is de voorbije jaren sterk gestegen. Om dergelijke vormen van criminaliteit doeltreffend te bestrijden wordt in de lidstaten in uiteenlopende mate uitvoering gegeven aan een breed scala van zowel preventieve maatregelen (onder andere opleidings- en voorlichtingscampagnes die gericht zijn op bewustmaking) als dwangmaatregelen (blokkering van de toegang of verwijdering van illegale inhoud), waarbij zowel de publieke als de particuliere sector is betrokken. Uit de evaluatie is gebleken dat slechts enkele lidstaten over een specifieke nationale databank beschikken voor slachtofferidentificatie ter bestrijding van seksueel misbruik van kinderen; de andere lidstaten, die alleen gebruik maken van de internationale databank van Interpol betreffende seksuele uitbuiting van kinderen (ICSE-DB), is aangeraden een dergelijke nationale databank te ontwikkelen. Verschillende lidstaten beschikken over maatregelen ter voorkoming van herhaald slachtofferschap, in sommige gevallen onder meer om slachtoffers en getuigen van seksueel misbruik van kinderen te beschermen tijdens strafrechtelijke procedures. Goede samenwerking tussen alle betrokken partijen, namelijk de rechtshandhavingsinstanties, de telefonische meldpunten, ngo's en internetproviders, wordt beschouwd als een essentieel element om deze vormen van criminaliteit aan te pakken.

- Wat betreft cyberbeveiliging spelen de door de meeste lidstaten reeds ingestelde nationale CERT's een cruciale rol in het monitoren van en reageren op cyberincidenten. Voorts werd het de lidstaten aanbevolen in hun nationale recht een verplichting op te nemen voor de particuliere sector om onverwijld bij de rechtshandhavingsautoriteiten melding te maken van cyberaanvallen die aanzienlijke gevolgen hebben voor de continuïteit van essentiële diensten. Beide kwesties zijn opgenomen in de NIS-Richtlijn en zullen uiterlijk op 9 mei 2018 moeten zijn omgezet.

- Aangezien cybercriminaliteit en cybergerelateerde misdrijven en het onderzoek ernaar vaak meerdere lidstaten betreffen, is samenwerking en het delen van informatie met EU-instanties - Europol/EC3, Eurojust, het EJN en Enisa - prioritair. Om dezelfde reden werd een intensiever gebruik van de gezamenlijke onderzoeksteams (GOT's) aanbevolen, als een doeltreffend instrument voor grensoverschrijdende onderzoeken.

- Het internet kent geen grenzen, en daarom is een soepele en goed functionerende internationale samenwerking essentieel om cybercriminaliteit op een doeltreffende manier aan te pakken. De evaluatie heeft echter aangetoond dat procedures voor wederzijdse rechtshulp traag, tijdrovend en ondoeltreffend zijn, met negatieve gevolgen voor de onderzoeken, aangezien digitaal bewijsmateriaal vluchtig is en snel moeten worden behandeld. Er is bijgevolg behoefte aan een snellere afhandeling van verzoeken om wederzijdse rechtshulp in onderzoeken naar cybercriminaliteit. Voorts zijn de lidstaten aangemoedigd frequenter gebruik te maken van de instrumenten van Eurojust, het EJN, en Europol, en om informele contacten aan te knopen met de bevoegde buitenlandse instanties teneinde een snellere reactie te krijgen op verzoeken om wederzijdse rechtshulp.

III - NATIONALE STRATEGIE VOOR CYBERBEVEILIGING

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Het Enisa heeft in 2012 een praktische gids uitgewerkt voor de ontwikkeling en uitvoering van de nationale strategieën voor cyberbeveiliging. Volgens die gids is een nationale strategie voor cyberbeveiliging een instrument om de beveiliging en de veerkracht van nationale infrastructuren en diensten te versterken.

- In het algemeen bestaat de doelstelling van een nationale strategie voor cyberbeveiliging erin een kader te bieden ter bepaling van de nationale prioriteiten en tot instelling van de belangrijkste coördinatiestructuren op strategisch en operationeel niveau, teneinde cybercriminaliteit te bestrijden en te zorgen voor cyberveerkracht.

- Een alomvattende nationale strategie voor cyberbeveiliging dient gericht te zijn en specifieke en meetbare doelstellingen te bevatten, alsook een duidelijke afbakening van de verantwoordelijkheden, zodat de taken van de verschillende betrokkenen kunnen worden gecoördineerd en een kostenraming kan worden gemaakt van de acties die moeten worden ondernomen.

- Op het tijdstip van de evaluatie had de meerderheid van de lidstaten een nationale strategie voor cyberbeveiliging aangenomen, en sommige van hen ook een actieplan voor de tenuitvoerlegging ervan, terwijl enkele lidstaten daarmee bezig waren.

- Nadat een nationale strategie voor cyberbeveiliging en, in voorkomend geval, een actieplan is ontwikkeld, is het van belang voor een behoorlijke follow-up te zorgen en nauwlettend toe te zien op de uitvoering van de nationale strategie.

- Door de snelle ontwikkeling van zowel informatietechnologie (IT) als van nieuwe soorten cybergerelateerde inbreuken is er ook behoefte aan een voortdurende actualisering van de geldende maatregelen en beschikbare middelen om cybercriminaliteit op een doeltreffende manier te bestrijden, en derhalve aan een tijdige herziening, wanneer nodig, van de nationale strategie voor cyberbeveiliging.

- De instelling van één orgaan met coördinatiefuncties voor de uitvoering van de nationale strategie voor cyberbeveiliging, zoals sommige lidstaten hebben, kan als een goede praktijk worden beschouwd die door andere lidstaten moet worden gevolgd.

- In de nieuw vastgestelde Richtlijn 2016/1148/EU (NIS-richtlijn) is bepaald dat een nationale strategie voor de beveiliging van netwerk- en informatiesystemen moet worden aangenomen teneinde de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen vast te leggen met het oog op een hoog niveau van beveiliging van netwerk- en informatiesystemen (artikel 7).

AANBEVELINGEN

- ***De lidstaten die nog geen nationale strategie voor cyberbeveiliging hebben aangenomen worden aangemoedigd dit zo snel mogelijk te doen en ook de aanneming van een actieplan te overwegen; de lidstaten die een dergelijke strategie wel hebben aangenomen dienen te zorgen voor de goede uitvoering ervan en daartoe eventueel één orgaan/entiteit te belasten met coördinerende taken.***

- ***De lidstaten dienen steeds wanneer nodig hun nationale strategie voor cyberbeveiliging te actualiseren, in overeenstemming met de desbetreffende ontwikkelingen op IT-gebied en de trends op het gebied van cybercriminaliteit.***

IV - VERDRAG VAN BOEDAPEST

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Het in 2001 door de Raad van Europa aangenomen Verdrag van Boedapest inzake cybercriminaliteit is het eerste internationale verdrag over via het internet en andere computernetwerken gepleegde misdrijven, en betreft met name inbreuken op auteursrechten, computergerelateerde fraude, kinderpornografie, haatmisdrijven, en schendingen van netwerkbeveiliging. Het omvat ook een reeks bevoegdheden en procedures zoals het doorzoeken van computernetwerken en legale interceptie.

- Het belangrijkste doel ervan is een gemeenschappelijk strafrechtelijk beleid om de samenleving tegen cybercriminaliteit te beschermen, vooral door passende wetgeving vast te stellen en internationale samenwerking te bevorderen.

- Met name de artikelen 16, 17, 29 en 30 van het Verdrag regelen de spoedbewaring van opgeslagen computergegevens en verkeersgegevens en de gedeeltelijke verstrekking van verkeersgegevens, terwijl bij artikel 35 het internationale 24/7-netwerk voor noodsituaties wordt ingesteld, waarmee gegevens kunnen worden bevroren en digitaal bewijsmateriaal zodoende kan worden bewaard. Dat laatste is een belangrijk instrument aangezien het een snelle mogelijkheid tot bewaring van digitaal bewijsmateriaal schept, vóór het toezenden van een verzoek om wederzijdse rechtshulp.

- Het Verdrag van Boedapest wordt aangevuld door een aanvullend protocol betreffende de strafbaarstelling van handelingen van racistische en xenofobische aard verricht via computersystemen en, wat betreft de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, door het Verdrag van Lanzarote.
- Op het tijdstip van de evaluatie hadden de meeste lidstaten deze instrumenten ondertekend en geratificeerd; een aantal lidstaten had dat nog niet gedaan. In de conclusies van de Raad van 9 juni 2016 over het verbeteren van de strafrechtspleging in de cyberruimte, wordt de lidstaten opnieuw verzocht om het Verdrag inzake cybercriminaliteit van 23 november 2001 te ratificeren en uit te voeren.

AANBEVELINGEN

- ***De lidstaten die dat nog niet hebben gedaan, worden verzocht het in 2001 door de Raad van Europa aangenomen Verdrag van Boedapest inzake cybercriminaliteit en het aanvullende protocol erbij te ondertekenen en te ratificeren, en deze instrumenten volledig ten uitvoer te leggen.***

V - STATISTIEKEN

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Uit de analyse van de EU-wetgeving blijkt een duidelijke behoefte aan het verzamelen van statistieken op het gebied van cybercriminaliteit. Overeenkomstig artikel 14, lid 1, van Richtlijn 2013/40/EU over aanvallen op informatiesystemen, zorgen de lidstaten voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

- Overeenkomstig artikel 14, lid 2, van dezelfde richtlijn, vermelden de in lid 1 bedoelde statistieken ten minste de beschikbare gegevens over het aantal in de artikelen 3 tot en met 7 bedoelde strafbare feiten die door de lidstaten zijn geregistreerd en het aantal personen dat is vervolgd en veroordeeld in verband met de in de artikelen 3 tot en met 7 bedoelde strafbare feiten.

- Voorts worden de lidstaten uit hoofde van overweging 44 van Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie aangemoedigd mechanismen voor gegevensverzameling tot stand te brengen of contactpunten te creëren, op nationaal of lokaal niveau en in samenwerking met het maatschappelijk middenveld, voor de observatie en evaluatie van het verschijnsel van seksueel misbruik en seksuele uitbuiting van kinderen.

- Voorts vloeit de behoefte om statistieken te verzamelen op nationaal niveau in beginsel voort uit de nationale wet- of regelgeving van de lidstaten.

- Statistieken over cybercriminaliteit zijn bijzonder belangrijk. Enerzijds maken zij het mogelijk de omvang van de nieuwe opkomende trends van deze groeiende vorm van criminaliteit in detail te analyseren en er inzicht in te krijgen, zodat een overzicht kan worden verkregen en de ontwikkelingen kunnen worden gemonitord, met het oog op passende maatregelen; anderzijds maken zij een oordeel mogelijk over de doeltreffendheid van het rechtssysteem en de toereikendheid van wetgeving bij het bestrijden van cybercriminaliteit en het beschermen van de particuliere belangen van de burger-slachtoffers.

- Voorts vergemakkelijkt het verzamelen van statistische gegevens het werk van de EU-instellingen (de Commissie) en -instanties (Europol, Eurojust of Enisa) die betrokken zijn bij de strijd tegen cybercriminaliteit. Zij maken een vollediger beeld mogelijk van de problematiek van cybercriminaliteit en netwerk- en informatiebeveiliging op het niveau van de EU en dragen zo bij tot het formuleren van een doeltreffender antwoord.

- De statistieken zijn ook belangrijk voor een realistisch beeld van de frequentie van cybercriminaliteit, namelijk omdat de slachtoffers - zowel individuen als banken of bedrijven - dergelijke inbreuken, waaronder ernstige, onvoldoende melden aan de rechtshandhavingsinstanties.

- Alomvattende statistieken dienen alle gebieden te bestrijken die belangrijk worden geacht voor dit soort criminaliteit, in alle fasen van de procedure: onderzoek, vervolging, proces, het specifieke criminele feit en de specifieke onderzoeksmaatregel, het aantal gemelde strafbare feiten, het aantal uitgevoerde onderzoeken en besluiten om bepaalde types cybercriminaliteit niet te onderzoeken, het aantal slachtoffers en klachten van slachtoffers, het aantal vervolgde en veroordeelde personen voor verschillende soorten cyber-criminaliteit, het aantal grensoverschrijdende gevallen, het resultaat van de verzoeken om wederzijdse rechtshulp en de duur van de procedure.

- Een van de voornaamste tekortkomingen die in de zevende evaluatie zijn geconstateerd in de meerderheid van de lidstaten, betreft evenwel de mate waarin afzonderlijke statistieken worden verzameld over cybercriminaliteit, gedigitaliseerde misdrijven (gewone inbreuken die zijn gepleegd met gebruikmaking van informatie- en communicatietechnologie) en cyberbeveiligingsincidenten. De beschikbare statistieken zijn in de meeste lidstaten ontoereikend, gefragmenteerd en niet vergelijkbaar.

- Voorts beschikken vele lidstaten niet over een gemeenschappelijke definitie van cybercriminaliteit en gedigitaliseerde criminaliteit voor statistische doeleinden. In vele lidstaten is het onmogelijk om het aandeel van cybercriminaliteit in de totale criminaliteit te bepalen, en andere lidstaten die specifieke statistieken over cybercriminaliteit bijhouden, genereren die in de vorm van een enkel cijfer; het is derhalve niet mogelijk de feiten in categorieën te verdelen en een onderscheid te maken tussen gevallen van cybercriminaliteit in de strikte zin van het woord, en gedigitaliseerde strafbare feiten. Niet alle lidstaten stellen geregelde statistische rapporten op inzake cybercriminaliteit.

- In de meeste lidstaten zijn de gerechtelijke statistieken gescheiden van die van de rechtshandhavingsautoriteiten. Aangezien statistische systemen vaak aanzienlijk verschillen tussen bevoegde instanties, en elke autoriteit zijn gegevens uit verschillende bronnen en met verschillende methoden verzamelt, en ze beheert met verschillende criteria en/of gebruikmakend van verschillende databanken die niet interoperabel zijn, kan cyber-criminaliteit niet met één enkel statistisch systeem worden gevolgd.

- In vele lidstaten zijn de cybercriminaliteitscijfers die in de verschillende systemen worden ingevoerd erg laag. In deze gevallen kunnen er vragen rijzen over de efficiëntie van de opsporing, de vervolging en bestraffing van cybercriminaliteit en over de juistheid van de statistische gegevens.

- Het delen van statistieken tussen rechtshandhavingsinstanties en gerechtelijke instanties zou van grote waarde kunnen zijn voor een follow-upmechanisme en voor de prioritering van de doelstellingen in de strijd tegen dit fenomeen. Vaak is er echter geen of onvoldoende uitwisseling van statistische gegevens tussen de verschillende nationale instanties die betrokken zijn bij het aanpakken van cybercriminaliteit.

AANBEVELINGEN

- ***De lidstaten die kampen met problemen in verband met het ontbreken van een gemeenschappelijke definitie of een gemeenschappelijke opvatting van cybercriminaliteit worden aangemoedigd een consistente nationale definitie (of opvatting) van cyber-criminaliteit te ontwikkelen, die door alle betrokkenen dient te worden gehanteerd in de strijd tegen cybercriminaliteit en met het oog op het verzamelen van statistieken.***

- ***De lidstaten dienen specifieke statistieken voor cybercriminaliteit te verzamelen, waarmee zij zowel de algemene cijfers over cybercriminaliteit als het aandeel van cyber-criminaliteit in de totale criminaliteit kunnen bepalen.***

- ***De lidstaten dienen een gestandaardiseerde benadering te ontwikkelen voor het verzamelen van alomvattende statistieken in de verschillende fasen van het proces, uitgesplitst naar specifieke gebieden van cybercriminaliteit, bij voorkeur die welke op EU-niveau zijn bepaald, namelijk online seksueel misbruik van kinderen, online kaartfraude, en cyberaanvallen.***

- ***De lidstaten dienen oplossingen te overwegen die de interoperabiliteit tussen de verschillende databanken met cijfers inzake cybercriminaliteit mogelijk maken, teneinde snel werk te maken van vergelijking tussen zaken, strafrechtelijke identificatie en kwantificering van zaken.***

VI - STRUCTUREN - DE RECHTERLIJKE MACHT

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- De structuur en de organisatie van de rechterlijke macht variëren in de verschillende lidstaten, onder andere wat betreft de bevoegdheidstoewijzing voor het aanpakken van cybercriminaliteit.

- Door de snelle ontwikkeling van ICT en de complexiteit en de steeds grotere geavanceerdheid van cybercriminaliteit, hangt het succes van onderzoeken, vervolgingen en veroordelingen in zaken van cybercriminaliteit in grote mate af van de vakkundigheid en de ervaring van de autoriteiten die belast zijn met het onderzoek en het proces. Een degelijk niveau van begrip en kennis, en van gerichte specialisatie van het gerechtelijk apparaat is derhalve van cruciaal belang.

- Uit de wederzijdse evaluatie blijkt echter dat de mate van specialisatie van openbaar aanklagers en rechters die zich met cybercriminaliteit en daarmee samenhangende misdrijven bezighouden, niet altijd toereikend is.

- In een groot aantal lidstaten wordt cybercriminaliteit behandeld door het openbaar ministerie/parketten-generaal en in geen enkele lidstaat zijn er gespecialiseerde rechtbanken of rechters aangesteld om gevallen van cybercriminaliteit te onderzoeken of te berechten. Sommige lidstaten hebben daarentegen gespecialiseerde aanklagers of gespecialiseerde structuren binnen het Openbaar Ministerie die zich met cybermisdrijven bezighouden.

- In een paar lidstaten zijn er parketten/afdelingen die bevoegd zijn voor misdrijven die door georganiseerde criminele groeperingen zijn gepleegd of door hen zijn opgedragen, of voor economische misdrijven en corruptie, waaronder cybermisdrijven.

- Volgens de interne organisatie van de rechterlijke macht, op grond van de specialisaties van de openbaar aanklagers of de concentratie van rechterlijke functies met betrekking tot cybermisdrijven, ligt in een paar lidstaten de feitelijke verantwoordelijkheid voor de behandeling van dat soort misdrijven gewoonlijk bij gespecialiseerde openbaar aanklagers en rechters, die zijn opgeleid of ervaring hebben op het gebied van cybercriminaliteit en daardoor in de praktijk een hoge graad van specialisatie hebben bereikt, die hen in staat stelt hun collega's bij te staan.

- In sommige lidstaten zijn er nationale netwerken van cyberaanklagers die gespecialiseerd zijn in cybercriminaliteit, wat als goede praktijk kan worden beschouwd, omdat daardoor kennis en ervaring kan worden uitgewisseld en de verspreiding van beste praktijken onder rechtsbeoefenaars wordt vergemakkelijkt.

- De beoordelaars hadden de lidstaten aanbevolen om, met de hulp van Eurojust, de oprichting te bevorderen van een Europees netwerk van rechters dat gespecialiseerd is in de bestrijding van cybercriminaliteit, met het oog op het verbeteren en vergemakkelijken van justitiële samenwerking op dit gebied. Ondertussen is deze doelstelling verwezenlijkt door het naar aanleiding van de conclusies van de Raad in juni 2016 opgezette Europees justitieel netwerk cybercriminaliteit (EJCN), dat al in werking is getreden.

AANBEVELINGEN

- ***De lidstaten dienen de specialisatiegraad van hun gerechtelijk apparaat te verhogen, met het oog op het doeltreffend vervolgen en sanctioneren van cybergerelateerde en gedigitaliseerde misdrijven. Daartoe dienen zij bij voorkeur gespecialiseerde bureaus of inwendige structuren/eenheden en/of gespecialiseerde aanklagers en rechters aan te stellen met een goed begrip en een goede kennis van cybercriminaliteit, om dergelijke zaken te behandelen.***

- ***De lidstaten dienen op nationaal niveau netwerken op te zetten van in cybercriminaliteit gespecialiseerde aanklagers en rechters, als bijkomend instrument om de bestrijding van dit soort criminaliteit doeltreffender te maken.***

VII - STRUCTUREN - RECHTSHANDHAVINGSINSTANTIES

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- De structuur en de organisatie van de rechtshandhavingsinstanties variëren aanzienlijk in de verschillende lidstaten, onder andere op het vlak van de bevoegdheidstoewijzing inzake cybercriminaliteit. In sommige lidstaten werken gespecialiseerde eenheden op basis van een tweeledige aanpak met een strategische planning en operationele activiteiten, terwijl in andere lidstaten deze functies apart door verschillende autoriteiten en instanties worden vervuld.

- Een doeltreffende organisatie, internationale integratie en vakbekwaamheid van de bij cybercriminaliteit betrokken rechtshandhavingsinstanties zijn belangrijk om deze misdrijven doeltreffend aan te pakken. Een hoog niveau van kennis en specialisatie van de rechtshandhavingsinstanties is om dezelfde redenen als voor de rechterlijke macht essentieel om deze complexe en geavanceerde vorm van criminaliteit doeltreffend te bestrijden.

- Over het algemeen bleek uit de wederzijdse evaluatie dat de mate van specialisatie van de rechtshandhavingsinstanties weliswaar hoger is dan in de rechterlijke macht, maar in veel gevallen vatbaar is voor verbetering.

- In de meeste lidstaten zijn er gespecialiseerde centrale structuren voor cybercriminaliteit of eenheden binnen het ministerie van Binnenlandse Zaken en/of de politie, die belast zijn met het voorkomen en bestrijden van cybercriminaliteit op nationaal niveau en zodoende met een hoge specialisatiegraad op dit gebied zorgen voor de coördinatie van het onderzoek naar cybercriminaliteit in het land. Dit bevordert ook de communicatie tussen de politie en de openbaar aanklagers. In verschillende lidstaten zijn er ook gedecentraliseerde, gespecialiseerde eenheden op lokaal en regionaal niveau die zich specifiek bezighouden met het onderzoek naar cybercriminaliteit.

- Sommige lidstaten hebben het advies gekregen werk te maken van de reorganisatie van de politie en het nodige te doen om het personeelsbestand uit te breiden, politiemensen een doeltreffendere en intensievere opleiding te geven, en voldoende technisch materiaal in de strijd tegen cybercriminaliteit aan te bieden. Voorts moeten de apparatuur en de middelen van de rechtshandhavingsinstanties continu geactualiseerd worden als antwoord op de constante ontwikkeling en diversificatie van de modus operandi van cybercriminaliteit.

- De belangrijkste obstakels voor het succesvol onderzoek naar cybercriminaliteit zijn onder andere de snelle ontwikkeling van de technologie, het toenemend professionalisme en het stijgend niveau van expertise van cybercriminelen, het feit dat cybercriminaliteit zich gemakkelijk kan uitstrekken tot de jurisdictie van verschillende landen, de moeilijke toegang tot digitaal bewijsmateriaal met betrekking tot cybercriminaliteit en de uitdagingen in verband met het gebruik van encryptie, Tor en anonimisering.

- Momenteel bestaat in geen enkele lidstaat een nationaal netwerk van politiefunctionarissen die gespecialiseerd zijn in cybercriminaliteit.

AANBEVELINGEN

- ***De lidstaten dienen ervoor te zorgen dat de specialisatiegraad van rechtshandhavingsinstanties die zich met het onderzoek naar cybercriminaliteit bezighouden, behouden blijft en, zo nodig, wordt verhoogd. De lidstaten die zulks nog niet hebben gedaan, dienen te overwegen om gespecialiseerde eenheden binnen de rechtshandhavingsinstanties op te richten om cybercriminaliteit ook op regionaal/lokaal niveau doeltreffender te bestrijden.***

- ***De lidstaten dienen te overwegen om op nationaal niveau een netwerk van in cybercriminaliteit gespecialiseerde politiefunctionarissen op te zetten, dat ook kan bijdragen tot de instandhouding van een communicatiekanaal tussen de publieke en de particuliere sector en de politie.***

- ***De lidstaten dienen te overwegen het niet-technisch politiepersoneel in de gewestelijke of regionale structuren te versterken en te zorgen voor voldoende technische apparatuur om in hun behoeften te voorzien.***

VIII - SAMENWERKING EN COÖRDINATIE OP NATIONAAL NIVEAU

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Aangezien cybercriminaliteit grensoverschrijdend is en de verantwoordelijkheid voor de beveiliging van de cyberspace op nationaal vlak over het algemeen gedeeld wordt door verschillende actoren met verschillende verantwoordelijkheden en capaciteiten, zowel publieke als particuliere, militaire en civiele, collectieve en individuele, is een multi-disciplinaire benadering van essentieel belang voor het doeltreffend voorkomen en bestrijden van cybercriminaliteit en het waarborgen van cyberveerkracht.

- In deze context is nauwe en doeltreffende interinstitutionele coördinatie en samenwerking tussen de verschillende overheidsinstanties en -organen op operationeel en strategisch niveau, en tussen centrale en lokale/regionale overheden, van essentieel belang voor het coördineren van initiatieven en het versterken van gegevensuitwisseling, technische ondersteuning en onderzoekstechnieken.

- Een nauwe samenwerking bij het bestrijden van cybercriminaliteit is niet alleen nodig tussen de politie en het Openbaar Ministerie, maar ook met de nationale inlichtingen-diensten om technische ondersteuning te krijgen (onderscheppingen, expertise, enzovoort), en met de inlichtingendiensten bij strafrechtelijke onderzoeken en vervolgingen, in het bijzonder voor het verkrijgen en verwerken van digitaal bewijsmateriaal.

- Samenwerking tussen de publieke en de particuliere sector is ook cruciaal voor het succesvol onderzoeken, vervolgen en veroordelen van cybercriminaliteit en gedigitaliseerde misdrijven en voor de respons op cyberdreigingen en -aanvallen (voor meer bijzonderheden, zie volgende hoofdstuk).

- In combinatie met het regelgevingskader voor samenwerking tussen instanties, indien dat is gedefinieerd, bepalen de nationale cyberbeveiligingsstrategie en, indien dat bestaat, het actieplan voor de uitvoering ervan, het algemene kader voor de coördinatie en samenwerking tussen alle openbare instellingen en overheden met verantwoordelijkheid op het gebied van cyberbeveiliging, en met de particuliere sector, met het oog op de afbakening van taken en verantwoordelijkheden.

- De correcte uitvoering van de nationale cyberbeveiligingsstrategie is derhalve van essentieel belang voor het creëren van synergie en het maximaliseren van de paraatheid en het reactievermogen bij de bestrijding van cybercriminaliteit en de versterking van de cyberbeveiliging.

- Uit de evaluaties blijkt dat de vormen, modaliteiten en niveaus van samenwerking en coördinatie tussen de belanghebbenden die betrokken zijn bij de bestrijding van cybercriminaliteit en bij de zorg voor cyberbeveiliging, in de verschillende lidstaten variëren, waarbij sommige meer geavanceerde en doeltreffende vormen van interactie hebben ontwikkeld dan andere, die in individuele verslagen als goede praktijk zijn aangemerkt.

- De beste manier om te garanderen dat het systeem goed werkt, is een gestructureerd mechanisme, met name wanneer de coördinatiefuncties bij kwesties inzake cyber-beveiliging en beleidsmaatregelen tegen cybercriminaliteit, aan een enkele institutionele autoriteit (d.w.z. ministeries of instanties in hun organisatiestructuur) of een ad-hocorgaan of -entiteit, zijn toegewezen. Sommige lidstaten beschikken reeds over een dergelijke instelling/instantie, die een institutioneel kader voor samenwerking biedt, waarin zowel publieke als particuliere belanghebbenden die betrokken zijn bij de bestrijding van cybercriminaliteit en bij cyberbeveiliging, vertegenwoordigd zijn, en ten tijde van de evaluatie overwogen andere lidstaten er een in te stellen.

- In een aantal lidstaten is er geen rechtskader voor de samenwerking tussen instanties in cybercriminaliteitszaken, en de autoriteiten die betrokken zijn bij het onderzoeken en vervolgen van cybercriminaliteit werken op informele wijze samen, aangezien zij hun tegenhangers bij de andere autoriteiten kennen en daarom gemakkelijk met elkaar in contact treden; dit werkt goed en is bevorderlijk voor contact en dialoog zonder onnodige bureaucratische vertragingen.

- Sommige lidstaten waar tekortkomingen zijn geconstateerd in de context van de wederzijdse evaluatie leveren inspanningen om bestaande structuren en processen van samenwerking en coördinatie te versterken, met het oog op het doeltreffender voorkomen en bestrijden van cybercriminaliteit.

AANBEVELINGEN

- ***De lidstaten dienen prioriteit te geven aan de institutionele coördinatie en samenwerking tussen alle belanghebbenden die betrokken zijn bij de voorkoming en bestrijding van cybercriminaliteit en bij cyberbeveiliging, op basis van een multidisciplinaire aanpak, met het oog op het tot stand brengen van synergie en het maximaliseren van paraatheid en reactievermogen.***

- ***De lidstaten worden met name aangemoedigd een gestructureerd samenwerkingskader op te zetten of te versterken, en mogelijk een centrale instantie/entiteit op te richten waarin zowel publieke als particuliere belanghebbenden die betrokken zijn bij de bestrijding van cybercriminaliteit en bij cyberbeveiliging, vertegenwoordigd zijn, met coördinerende functies en beslissingsbevoegdheden.***

IX - SAMENWERKING TUSSEN DE PUBLIEKE EN DE PARTICULIERE SECTOR

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Een nauwe samenwerking tussen de publieke en de particuliere sector is van fundamenteel belang, aangezien het bestrijden van cybercriminaliteit zeer complex is, wat betekent dat rechtshandhavingsinstanties deze criminaliteit niet met succes kunnen bestrijden zonder de medewerking van de particuliere sector (financiële / bankinstellingen, telecommunicatie-bedrijven, internetproviders, niet-gouvernementele organisaties, universiteiten, het bedrijfsleven, beroepsverenigingen, enzovoort).

- Een dergelijke samenwerking kan beide sectoren ten goede komen, aangezien hierdoor een breed scala van entiteiten samenwerkt en een synergie tussen hen tot stand wordt gebracht, wat bijdraagt tot een hoger niveau van cyberbeveiliging.

- De bijdrage van particuliere belanghebbenden wat betreft expertise, technische ondersteuning en informatieuitwisseling inzake cyberdreigingen en ontwikkelingen op het vlak van cyberbeveiliging, heeft een grote toegevoegde waarde voor het succes van onderzoeken en maatregelen om cyberincidenten op te lossen. Het is ook nuttig om openbaar aanklagers bij de contacten met de particuliere sector te betrekken om er zeker van te zijn dat bewijsmateriaal overeenkomstig de huidige wetgeving is verzameld en ontvankelijk is in gerechtelijke procedures.

- Uit de evaluatie blijkt dat de mate van samenwerking tussen de publieke en de particuliere sector in de verschillende lidstaten varieert en dat deze over het algemeen uitgebreider en doeltreffender is wanneer zij meer gestructureerd is en er een klimaat van vertrouwen heerst. Voor sommige lidstaten zijn in de evaluatie goede praktijken aangemerkt, terwijl voor andere de noodzaak van een betere samenwerking is onderstreept.

- Om cybercriminaliteit te voorkomen en te bestrijden en cyberbeveiliging te garanderen, maken sommige lidstaten uitgebreid gebruik van publiek-private partnerschappen, wat in sommige gevallen in de nationale cyberbeveiligingsstrategie is voorzien, terwijl in andere het gebruik ervan tot specifieke gebieden beperkt blijft of nog niet ten uitvoer is gelegd. Het kan in verscheidene vormen worden vastgesteld, onder meer op basis van memoranda van overeenstemming of gelijksoortige formele overeenkomsten.

- In de resultaten van de evaluatie zijn publiek-private partnerschappen door de beoordelaars aangemerkt als belangrijk instrument voor een goede samenwerking tussen de rechtshandhavingsinstanties en de particuliere sector, met name internetproviders, en de financiële sector, met name banken, maar ook met ngo's, computercrisisteams en kritieke infrastructuur.

- Zoals in sommige individuele verslagen wordt vermeld, komt de regeling van het publiek-privaat partnerschap met een kader waarin plichten en regels zijn vastgelegd, de uitwisseling en het beheer van informatie ten goede, aangezien het informele processen mogelijk maakt, in plaats van meer traditionele methodes te gebruiken die zijn gebaseerd op de officiële uitwisseling van documentatie op officieel verzoek van de rechtshandhavingsinstanties.

- De meest geavanceerde vormen van samenwerking met de particuliere sector zijn aangetroffen in sommige lidstaten waar een dergelijke samenwerking geïnstitutionaliseerd is door de oprichting van toepasselijke instellingen/werkgroepen voor samenwerking tussen de particuliere sector en de overheid /rechtshandhavingsinstanties. Dit komt vaker voor wat betreft de samenwerking met de banksector (zie hieronder), maar, zoals aanbevolen in sommige individuele verslagen, is het nuttig om deze vorm van samenwerking uit te breiden naar andere gebieden en belanghebbenden in de particuliere sector.

- Niet alle lidstaten hebben echter een formeel kader ontwikkeld voor publiek-private partnerschappen, en in sommige lidstaten vinden samenwerking, overleg en uitwisseling van informatie over incidenten, trends en ontwikkelingen met de particuliere sector op informele wijze plaats, en niet op wettelijke of contractuele basis.

- Samenwerking met internetproviders (isp's) of cloud-providers en met aanbieders van elektronische communicatiediensten is bijzonder nuttig om van hun expertise te kunnen profiteren en om toegang te krijgen tot abonneegegevens in verband met cybercriminaliteit. Door risicobeoordelingen uit te voeren, geschikte veiligheidsmaatregelen te nemen en een gestructureerd veiligheidsbeleid te voeren, kunnen aanbieders van elektronische communicatienetwerken en -diensten niet alleen bepaalde soorten cybercriminaliteit voorkomen, maar de rechtshandhavingsinstanties ook bijstaan met substantieel bewijsmateriaal, op voorwaarde dat dit via de door de wet voorgeschreven procedures is verkregen.

- Volgens de evaluatie moeten er oplossingen worden gevonden voor een duidelijk en geschikt kader voor het regelen van de betrekkingen van de justitiële autoriteiten met internetproviders in de EU. Procedures waardoor autoriteiten binnen een redelijke termijn een antwoord op hun vragen krijgen en het opzetten van een systeem van sancties voor niet-naleving/niet-medewerken/tekortkoming (administratieve of procedurele boete) kunnen die samenwerking verbeteren.

- Sommige lidstaten hebben rechtstreeks contact met in het buitenland gevestigde internetproviders, vooral in de VS, maar de samenwerking met dat soort bedrijven is vrij problematisch, omdat zij niet op alle vragen antwoorden of vaak antwoorden dat zij de gevraagde informatie niet kunnen geven zonder wederzijdse rechtshulp/rogatoire commissie of gerechtelijk bevel. Deze situaties hebben grote gevolgen voor de onderzoeken en kunnen soms zelfs leiden tot afsluiting van een bepaalde zaak, aangezien door het gebrek aan informatie de identiteit van de overtreder, de tijd en de plaats van het misdrijf, en het instrument waarmee het misdrijf werd gepleegd, moeilijker vast te stellen is.

- Volgens de evaluatie kan een dialoog tussen de belangrijkste internetoperatoren, hostingbedrijven en internetproviders op EU- en internationaal niveau, hun samenwerking versterken in de context van gerechtelijke onderzoeken.

- Een doeltreffende samenwerking tussen de rechtshandhavingsinstanties enerzijds en de financiële instellingen en commerciële banken anderzijds, is ook van essentieel belang in de strijd tegen onlinekaartfraude en andere fraude met betrekking tot internetbankieren (en het gebruik van malware bij bankieren), met het oog op het vaststellen van dat soort fraude, het informeren van de particuliere sector over nieuwe tendensen en het bepalen van conservatoire maatregelen.

- In bepaalde lidstaten wordt een dergelijke samenwerking bevorderd door specifieke bankenverenigingen of interbancaire comités, die in het leven zijn geroepen om fraude bij betalingssystemen en betaalmiddelen te bestrijden, en regelmatig vergaderingen houden, waaraan de politie deelneemt. In één lidstaat werd de deelname van de politie aan het adviesorgaan van de nationale bankenvereniging door de beoordelaars als goede praktijk beschouwd.

- In andere lidstaten is de samenwerking tussen de rechtshandhavingsinstanties en de bank- en financiële instellingen minder gestructureerd en blijft zij beperkt tot contacten en/of vergaderingen met het oog op samenwerking en uitwisseling van informatie inzake met cybercriminaliteit verband houdende kwesties.

- In sommige lidstaten bestaat voor de particuliere sector een rapportageverplichting inzake cybercriminaliteit, terwijl in andere lidstaten die rapportage niet verplicht is of beperkt blijft tot specifieke takken van de particuliere sector of een bepaald soort cybermisdrijf.

- In bepaalde gevallen geschiedt de rapportage over cybercriminaliteit op vrijwillige basis.
  Uit de evaluaties blijkt echter dat in sommige lidstaten financiële en kredietinstellingen en internetproviders terughoudend staan tegenover het rapporteren en ondersteunen van een strafrechtelijke procedure om de strafrechtelijke aansprakelijkheid van de dader te bepalen. Zij zijn eerder geïnteresseerd om zo spoedig mogelijk de schade te herstellen die zou kunnen voortvloeien uit publicatie en berichtgeving in de media, die niet goed voor hun geloofwaardigheid en reputatie zijn.

- Wanneer de particuliere sector het slachtoffer of de benadeelde partij is, is volgens bepaalde individuele verslagen de samenwerking met rechtshandhavingsinstanties meestal goed, aangezien de sector zorgt voor de bewaring van het bewijsmateriaal, de interpretatie ervan, en de overhandiging ervan aan de rechtshandhavingsinstanties.

- De particuliere sector speelt ook een belangrijke rol bij de bescherming van kinderen en bij preventie en bewustmakingsactiviteiten in dat verband; particuliere verenigingen en ngo's die actief zijn op dit gebied en samenwerken met rechtshandhavingsinstanties die betrokken zijn bij de bestrijding van online seksuele uitbuiting, spelen een belangrijke rol door meldingen van misbruik te kanaliseren.

- Volgens de conclusies van de evaluatie zou een dialoog met de particuliere sector die verder gaat dan de verplichte rapportagevereisten in ieder geval tot betere resultaten leiden bij de bestrijding van cybercriminaliteit.

- Overheden moeten ook samenwerken, zoals in een aantal lidstaten het geval is, met universiteiten, onderwijsinstellingen, sociale diensten, het bedrijfsleven, beroepsverenigingen, media en andere organisaties om negatieve gevolgen van computercriminaliteit en cybercriminaliteit voor de informatiebeveiliging in het land te voorkomen en te neutraliseren. Met name is de samenwerking met universiteiten erg belangrijk voor bewustmaking, opleiding, en onderzoek en ontwikkeling (O & O).

AANBEVELINGEN

- ***De lidstaten dienen regelmatige samenwerking tussen de publieke en de particuliere sector in stand te houden en te vergroten (banken, telecommunicatiebedrijven en internetproviders), en ook aanklagers en mogelijk rechters daarbij te betrekken, teneinde methoden te bespreken die garanderen dat elektronisch bewijsmateriaal volgens de huidige wetgeving wordt verzameld, met het oog op de ontvankelijkheid in gerechtelijke procedures.***

- ***De lidstaten dienen gebruik te maken van gestructureerde publiek-private partnerschappen, om ervoor te zorgen dat er een duidelijk kader is voor de samenwerking tussen de publieke en de particuliere sector, met duidelijke regels en plichten.***

- ***De lidstaten dienen de particuliere sector aan te moedigen informatie met de overheidsdiensten te delen en, in voorkomend geval, in de nationale wetgeving een rapportageverplichting voor de particuliere sector inzake cybergerelateerde misdrijven op te nemen, die met name inhoudt dat de kredietinstellingen cyberaanvalincidenten die zowel op de kredietinstellingen als op hun klanten gericht zijn, onverwijld melden.***

- ***De Europese Unie en haar lidstaten dienen na te denken over hoe zij de samenwerking kunnen verbeteren tussen de rechtshandhavingsinstanties en internationale telecommunicatiebedrijven en internetproviders, met inbegrip van de mogelijkheid voor de EU om overeenkomsten te sluiten met grote buitenlandse particuliere ondernemingen om samenwerking in strafzaken te bevorderen.***

X - ONDERZOEKSTECHNIEKEN

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Gezien de brede waaier aan cybermisdrijven kan er geen sprake zijn van algemeen beproefde procedures of methodes voor het onderzoek van die misdrijven. Ieder onderzoek en elke aanpak hangt af van de specifieke omstandigheden, en de onderzoeksprocedures en -methodes moeten op de zaak in kwestie zijn toegesneden.

- Vooral op het gebied van cybercriminaliteit veranderen de modus operandi, de software en de instrumenten die worden gebruikt voortdurend en snel. De onderzoeksmaatregelen moeten daarom voortdurend geactualiseerd worden (bijv. met speciale onderzoeks-software), overeenkomstig de ontwikkelingen op het gebied van cybercriminaliteit.

- Naast de gewone onderzoekstechnieken worden ook speciale technieken gebruikt voor het onderzoek van gevallen van cybercriminaliteit. Er zijn een aantal mogelijkheden: de meest gebruikte speciale onderzoekstechnieken, die bijzonder doeltreffende werkinstrumenten zijn bij gevallen van seksuele uitbuiting van kinderen, zijn het onderscheppen van communicatie, het bewaren van gegevens en het undercoveronderzoek.

- Dit laatste, dat vooral nuttig is als het onderzoek niet kan worden uitgevoerd met technische middelen, gebeurt door undercoveragenten in te zetten om onderzoek te doen op fora en panels. Dit soort onderzoeken hebben echter het meeste kans op goede resultaten als zij op lange termijn worden verricht.

- Andere speciale onderzoekstechnieken zijn gebaseerd op nieuwe technische mogelijkheden bij de bestrijding van onlinecomputercriminaliteit, zoals onlinemonitoring, of andere technieken zoals hardwaretoegangsblokkeringen en speciale bitkopieerapparaten, onderzoek en inbeslagneming op afstand (bijv. in het geval van rechtshandhavingsinstanties die online een verdachte computer hacken in plaats van hem fysiek in handen te krijgen), IP-tracking (bijv. Skype en andere berichtendiensten), open source zoekacties op het internet, back-ups van gegevens van gegevensdragers en van het internet (websites, logbestanden). Er worden ook speciale technieken gebruikt voor mobiele apparatuur (bijv. UFED).

- De nationale wetgeving van de lidstaten voorziet echter niet altijd in het gebruik van speciale onderzoekstechnieken. In sommige lidstaten is hiervoor een gerechtelijk bevel nodig.

AANBEVELINGEN

- ***De lidstaten die dat nog niet hebben gedaan, worden aangemoedigd in hun nationale wetgeving het gebruik van speciale onderzoekstechnieken mogelijk te maken ter vergemakkelijking van het onderzoek in zaken van cybercriminaliteit.***

XI - ENCRYPTIE

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- De toenemende beschikbaarheid en benutting van beveiligde en betrouwbare encryptietechnologieën waarborgt de beveiliging, veilige transmissie en vertrouwelijkheid van computergegevens, en bijgevolg de bescherming van de persoonlijke levenssfeer van de burgers en de doeltreffende gegevensbescherming in cyberspace.

- Dat er bij zowel de bewaring van gegevens als de communicatie via internet evenwel in toenemende mate gebruik wordt gemaakt van encryptie via steeds verfijndere technieken, maakt het almaar moeilijker de encryptie ongedaan te maken, en dat leidt in alle lidstaten steeds vaker tot problemen.

- Criminelen versleutelen gegevens vaak met opzet om het illegale materiaal in hun bezit te beschermen, wat zowel de strijd tegen als de preventie van cybercriminaliteit bemoeilijkt. Aangezien encryptie in veel toepassingen de norm is en in verband met een breed gamma van strafbare feiten wordt gebruikt, ondervinden de rechtshandhavingsinstanties vaak problemen met versleutelde gegevens.

- De encryptie maakt het moeilijk of geheel onmogelijk toegang te krijgen tot relevante informatie in verband met onlinecriminaliteit of cybercriminaliteit, met name voor het in kaart brengen van communicatie- of computergegevens die in het bezit zijn van verdachten of daders, niet louter in het kader van forensisch onderzoek, maar ook in alle andere soorten onderzoeken. Daarnaast is het als gevolg van de toepassing van eind-tot-eindencryptie door een toenemend aantal dienstverleners moeilijk materiaal te onderscheppen of te doorgronden.

- Voor versleutelde gegevens noch versleutelde communicatie bestaat er een standaardoplossing. Na onderzoek van een afzonderlijk geval kunnen er gerichte maatregelen, zoals bijzondere maatregelen inzake telecommunicatie-observatie of decryptiemaatregelen, in stelling worden gebracht.

- In dit verband is het opsporen met de noodzakelijke apparatuur van de versleutelde inhoud, die niet altijd als zodanig is aangegeven, en van de vorm van encryptie de voornaamste uitdaging. Het belangrijkste probleem is echter de decryptie zelf, dat slechts mogelijk is door het inzetten van gespecialiseerde hardware met een hoog vermogen en software die met grote investeringen en aanzienlijke kosten gepaard gaat.

- Bij de aanpak van deze problemen is het nodig vertrouwd te zijn met de huidige stand van de encryptietechnologie en onderzoek te doen naar de zwakke punten in algoritmen en toepassingen, onder meer om mogelijke fouten uit te buiten.

- Uit de evaluatie is gebleken dat er doorgaans in zekere mate succes wordt geboekt wanneer zeer eenvoudige encryptiemethoden zijn gebruikt en dat het mogelijk is encryptiemethoden op te sporen of de encryptie terug te draaien met passende software (zoals PRTK via het FTK-platform) die decryptie mogelijk maakt. Eenvoudige wachtwoorden kunnen met de juiste apparaten en instrumenten worden gekraakt.

- De onderzoeksinstanties kunnen er in aanzienlijke mate toe bijdragen dat wachtwoorden met succes worden gekraakt door informatie die relevant is voor het wachtwoord zelf (eventuele wachtwoordzinnen, fragmenten van een zin, karakterreeksen, lengte van het wachtwoord, enz.) en al het digitaal bewijsmateriaal (opslagapparaten) voor te leggen aan aan forensische computerdeskundigen. Dit is evenwel niet altijd doeltreffend.

- Volgens de bevindingen van de evaluatie is in bepaalde gevallen een ingewikkeldere encryptie van inhoud met succes ontcijferd wanneer er werd gewerkt met bruut geweld (d.w.z. alle mogelijke codes proberen) of woordenlijstaanvallen (d.w.z. woorden gebruiken die zijn bedacht voor het kraken van wachtwoorden) of de verdachte het wachtwoord of de zin die nodig was om de encryptie te omzeilen prijsgaf, ingeval hij aanvaardde mee te werken of te goeder trouw was.

- De betrokkenen zijn echter niet altijd bereid om mee te werken met de autoriteiten, en er bestaan geen middelen om betrokkenen daartoe te dwingen. Zoals in een apart verslag is aangegeven, zou de doeltreffendheid van onderzoeken kunnen worden verbeterd door een decryptiebevel in te voeren, dat ook op Europees niveau zou kunnen worden ontwikkeld.

- Algemeen gesproken blijkt uit de evaluatie evenwel dat er weinig succes wordt geboekt bij het aanpakken van de decryptiekwestie op alle gebieden, waaronder toegang, inhoudsgegevens en eind-tot-eindencryptie, aangezien de door criminelen gebruikte algoritmen en de toepassing ervan vaak technisch solide zijn.

- De voornaamste problemen die zich in verband met encryptie voordoen betreffen bestanden die met krachtige encryptie zijn beschermd (via AES-256 versleutelde archieven) en encryptie van de volledige schijf (via TrueCrypt, BitLocker, FileVault2, WinRar of PGP). In deze gevallen kan decryptie met bruut geweld of via woordenlijstaanvallen uitermate tijdrovend zijn (maanden, in sommige gevallen zelfs jaren), een grote hoeveelheid computervermogen vergen (gespecialiseerde commerciële software en netwerkclusterinfrastructuur) om de cryptografische bescherming te doorbreken in gevallen waarin de daders lange en ingewikkelde wachtwoorden gebruiken om de encryptiesleutel te vinden.

- Volgens de bevindingen van de evaluatie is het in veel gevallen bijgevolg niet mogelijk om het encryptieprobleem doeltreffend op te lossen en zijn decryptiepogingen niet altijd succesvol, met name indien het wachtwoord technisch geavanceerd is en niet binnen een redelijke termijn kan worden achterhaald; in bepaalde gevallen wordt het decryptieproces stopgezet.

- In sommige lidstaten wordt voor de decryptie samengewerkt met particuliere bedrijven, waarvan de deskundigheid nuttig blijkt, vooral wanneer de encryptiemethoden zeer geraffineerd zijn. In verscheidene lidstaten worden particuliere bedrijven daarentegen niet betrokken bij decryptie in het kader van strafonderzoeken; de decryptie is exclusief de taak van de nationale forensische instituten.

- De middelen en diensten van Europol, met name het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) bieden de mogelijkheid om voor geraffineerde decryptie gebruik te maken van het Europolplatform, en sommige lidstaten doen daar een beroep op.

- Volgens de bevindingen van de evaluatie kunnen de encryptieproblemen met het oog op meer succesvolle onderzoeken deels worden gecompenseerd door meer onderzoek en ontwikkeling en het ontwikkelen van nieuwe methoden, onder meer voor een intelligentere analyse van het patroon of de patronen in de creatie van wachtwoorden door verdachten en de dynamische aggregatie van computervermogen.

- Goede samenwerking tussen de verschillende betrokken instanties, met name de rechtshandhavingsinstanties, de instanties voor forensisch IT-onderzoek en de openbare aanklagers, is ook onmisbaar, onder meer omdat vanwege de eraan verbonden kosten niet elke afdeling of instantie zich de hardware en software voor het achterhalen van wachtwoorden kan veroorloven.

- Samenwerking tussen de lidstaten op het gebied van decryptie geschiedt door het delen van middelen en ervaring en het deelnemen aan gezamenlijke operaties. Indien het nodig is bewijsmateriaal ter decryptie naar andere autoriteiten door te zenden, is dit mogelijk via de kanalen van Europol en Interpol.

AANBEVELINGEN

- ***De lidstaten dienen te investeren in gespecialiseerde hardware en software met voldoende rekenvermogen en in goed opgeleid personeel om ook in complexe gevallen voor de decryptie van versleutelde bestanden en communicatie te zorgen.***

- ***De lidstaten dienen zorg te dragen voor samenwerking tussen alle relevante stakeholders, onder meer in voorkomend geval met particuliere ondernemingen, teneinde de decryptievaardigheid van de bevoegde instanties te verbeteren.***

- ***De lidstaten dienen meer aandacht te te besteden aan onderzoek en ontwikkeling teneinde nieuwe en efficiëntere decryptiemethoden te ontwikkelen, en gebruik te maken van de Europolfaciliteiten, met name het decryptieplatform van het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3), voor meer geraffineerde gevallen van encryptie.***

- ***De lidstaten en de EU-instellingen dienen ook te overwegen een decryptiebevel in te voeren.***

XII - ELEKTRONISCH BEWIJSMATERIAAL

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- In een significant aantal lidstaten bestaat in de nationale wetgeving geen definitie van het concept van elektronisch bewijs. De termen in het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van de Raad van Europa (hierna "het verdrag van Boedapest), en in Richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen dienen ter referentie.

- In de praktijk wordt onder elektronisch bewijsmateriaal doorgaans verstaan: informatie die wordt gegenereerd, opgeslagen of verzonden via elektronische apparatuur en aan de hand waarvan kan worden bepaald of er al dan niet sprake is van een strafbaar feit, welke persoon een dergelijk strafbaar feit heeft begaan en wat de noodzakelijke randvoorwaarden zijn voor de afwikkeling van een zaak.

- Het omvat, maar is niet beperkt tot, registratie-informatie, geschiedenis van het internetverkeer, inhoudsgegevens, afbeeldingen, IP-adressen, e-mails, elektronische documenten, digitale videobestanden, audiobestanden en afbeeldingen, databanken, spreadsheetgegevens, cookies, afdrukgegevens, elektronische boekhouding, gps-geolocatiegegevens, logbestanden van uitgevoerde bankverrichtingen, enz.

- Het verzamelen, analyseren en gebruiken van elektronisch bewijsmateriaal kan van belang zijn in strafprocedures, niet alleen in verband met strafbare feiten tegen en via computers, maar ook in verband met andere strafbare feiten waarbij elektronisch bewijsmateriaal betrokken kan zijn.

- De aard van elektronisch bewijsmateriaal en het gemak waarmee het kan worden gemanipuleerd of vervalst, kunnen problemen met betrekking tot de ontvankelijkheid ervan scheppen die zich niet voordoen bij andere types bewijsmateriaal; er kan bijvoorbeeld meer bewijsmateriaal worden geëist, zoals analyses met forensische instrumenten of deskundigenbewijs van forensische onderzoekers.

- Daarom bestaan er in sommige lidstaten met het oog op de ontvankelijkheid in rechtbanken specifieke voorschriften betreffende de vergaring van elektronisch bewijsmateriaal. Dit kan onder andere inhouden dat een deskundige met technische kennis de gegevens moet verzamelen zodat de integriteit van het elektronisch bewijsmateriaal wordt beschermd of de bewijsketen goed wordt gedocumenteerd wat betreft de manier waarop het bewijsmateriaal oorspronkelijk is verkregen, wie het heeft verwerkt en hoe het is verwerkt, wat onder meer de vraag impliceert of het in enige zin is veranderd.

- Sommige lidstaten volgen inzake het verzamelen van elektronisch bewijsmateriaal de beste praktijken op het gebied van digitaal forensisch onderzoek die zijn vastgelegd in het verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken of in internationale richtsnoeren zoals de ACPO-richtsnoeren, die ook gelden voor de opslag en overdracht van elektronisch bewijsmateriaal.

- Uit de evaluatie is echter gebleken dat het procedurele recht in de meeste lidstaten technologie-neutraal is, wat betekent dat er algemene regels en beginselen worden toegepast op het verzamelen van bewijsmateriaal en dat het proceduresysteem geen specifieke formele regels bevat inzake de ontvankelijkheid en de beoordeling van elektronisch bewijsmateriaal; elektronisch bewijsmateriaal is aan dezelfde voorwaarden onderworpen als ander bewijsmateriaal en wordt door rechters beoordeeld overeenkomstig de algemene strafprocedureregels.

- In het algemeen wordt elektronisch bewijsmateriaal dus ontvankelijk in strafprocedures indien het op rechtmatige wijze is verkregen en relevant is voor de rechtsgang. Dit geldt ook voor elektronisch bewijsmateriaal dat buiten de staat is verzameld via samenwerking met lidstaten of internationale wederzijdse rechtshulp.

- Het gebrek aan regelgeving inzake de methode voor het verzamelen en presenteren aan de rechtbank van elektronisch bewijsmateriaal zou, zoals in een afzonderlijk verslag is aangegeven, de doeltreffende vervolging van gevallen van cybercriminaliteit in beginsel niet mogen belemmeren, aangezien de ontvankelijkheid van elektronisch bewijsmateriaal valt onder de algemene regelgeving voor bewijsmateriaal.

- In een aantal lidstaten is elektronisch bewijs net zoals het meeste traditionele bewijsmateriaal ontvankelijk voor de rechter en wordt het door de rechter geëvalueerd op basis van het beginsel van de vrije waardering van het bewijs. Dit betekent dat alles wat in een zaak bewijswaarde heeft in beginsel mag worden voorgelegd aan een rechter, die per geval zal bepalen welke waarde aan elk bewijsstuk moet worden toegekend. Volgens de conclusies van de evaluatie kan dit als een goede praktijk worden beschouwd.

- Indien de regels voor de ontvankelijkheid van bewijsmateriaal daarentegen tamelijk streng zijn, kan dit leiden tot obstakels voor elektronisch bewijsmateriaal, vooral indien het in een ander land is verkregen, bijvoorbeeld via verzoeken om wederzijdse rechtshulp.

- De politie kan op de locatie van de huiszoeking opgeslagen gegevens raadplegen, alsook op afstand opgeslagen gegevens of gegevens die in het buitenland zijn opgeslagen, zulks overeenkomstig internationale overeenkomsten. Indien de verduidelijking van voor strafprocedures relevante feiten de veiligstelling vergt van opgeslagen gegevens die in strafdossiers moeten worden opgenomen, onder meer operationele gegevens die zijn opgeslagen door het computersysteem of op om het even welke gegevensdrager (bv. cd-, dvd-dragers, mobiele telefoons), worden de betrokken objecten doorgaans in beslag genomen overeenkomstig de toepasselijke regels inzake strafvordering van de lidstaten.

- Indien elektronisch bewijs zich op het internet bevindt of eigendom is van de aanbieders van elektronische diensten, is samenwerking met dienstverleners van de informatie-maatschappij of aanbieders van elektronische-communicatiediensten essentieel om de benodigde gegevens te verstrekken en maatregelen te nemen ter voorkoming van de vernietiging of wijziging van de gegevens.

- Het onbegrensde karakter van cyberspace stelt rechtshandhavings- en justitiële autoriteiten voor bijzondere uitdagingen. Elektronisch bewijsmateriaal, dat tegenwoordig cruciaal is voor onderzoeken en justitiële autoriteiten, kan van overal ter wereld in luttele seconden worden opgeslagen, gewijzigd en verwijderd.

- Bijgevolg kan elektronisch bewijsmateriaal ook binnen enkele seconden mondiaal worden verplaatst, verwijderd en beheerd of over verscheidene rechtsgebieden worden verspreid. Het is evenwel niet in alle lidstaten mogelijk rechtstreekse toegang te krijgen tot elektronisch bewijsmateriaal dat zich in een ander land of in de cloud bevindt, en er moeten wederzijdse-rechtshulpprocedures worden gevolgd.

- Volgens de conclusies van de evaluatie, moeten de huidige procedures voor wederzijdse rechtshulp met het oog op het aanpakken van deze problemen sneller en doeltreffender verlopen, en de onderzoekende autoriteiten moeten zeer snel in de mogelijkheid worden gesteld verzoeken te sturen naar veel verschillende landen.

- In bepaalde lidstaten is het bij nationaal recht toegestaan dat abonnee-informatie rechtstreeks van buitenlandse providers wordt verkregen, op voorwaarde dat zulks ook is toegestaan bij het recht van de staat van de hoofdzetel van de aanbieder. In één lidstaat wenste een aantal beroepsbeoefenaren een geharmoniseerd mechanisme voor de uitwisseling van abonneegegevens en nieuwe benaderingen op EU-niveau voor het bepalen van de rechtsmacht.

- Er bestaan tussen de lidstaten verschillen wat betreft de praktijken en formulieren voor het beschikbaar stellen van elektronisch bewijs dat in het onderzoek in het kader van een dossier is verkregen in een formaat dat nader onderzoek door de openbare aanklagers en rechters mogelijk maakt.

- De inbeslagname van computerhardware die elektronisch bewijsmateriaal bevat lijkt niet de te verkiezen optie, aangezien een slachtoffer van cybercriminaliteit het hinderlijk zou kunnen vinden om het in de loop van het onderzoek zonder zijn of haar digitale apparatuur te moeten stellen.

- Een andere optie voor het veiligstellen van digitaal materiaal zou kunnen zijn om opgeslagen gegevens te kopiëren naar (of er een afspiegeling van te maken op) een andere gegevensdrager (bv. dvd of een harde schijf) en in deze vorm ter beschikking te stellen, en/of om met name leesbare gegevens (bv. sms-berichten) of afbeeldingsbestanden af te drukken en tevens in papiervorm ter beschikking te stellen.

- Gewoonlijk wordt dezelfde procedure gevolgd voor elektronisch bewijsmateriaal dat in het buitenland is vergaard. Indien het land dat heeft geholpen met het verwerven van het bewijsmateriaal, echter bijzondere voorwaarden stelt, zullen de politie en de openbare aanklagers die voorwaarden in acht moeten nemen.

- Wanneer de openbare aanklager en de rechters die zich tijdens gerechtelijke procedures over elektronisch bewijsmateriaal moeten buigen, dat materiaal ontvangen in een vorm die uitsluitend met IT-apparatuur kan worden geraadpleegd en beoordeeld en er daarom specifieke kennis is vereist, onder meer voor het analyseren van de authenticiteit van het elektronische bewijsmateriaal, kan een forensische deskundige om advies worden verzocht.

- Volgens de bevindingen van de evaluatie zouden specifieke hoogtechnologische hardware en software voor een betere opsporing en vergaring van elektronisch bewijsmateriaal de autoriteiten van de lidstaten in staat stellen met vergelijkbaar elektronisch bewijsmateriaal te werken en samen te werken.

AANBEVELINGEN

- ***De lidstaten dienen te beschikken over passende hoogtechnologische hardware en software voor een betere opsporing en vergaring van elektronisch bewijsmateriaal die de autoriteiten van de lidstaten in staat stellen met vergelijkbaar elektronisch bewijsmateriaal te werken en samen te werken.***

- ***De lidstaten dienen ervoor te zorgen dat hun nationale procedureregels voldoende flexibel zijn om de ontvankelijkheid van elektronisch bewijsmateriaal te faciliteren, ook wanneer het, bijvoorbeeld via verzoeken om wederzijdse rechtshulp, van een ander land is verkregen.***

- ***De lidstaten dienen te overwegen in dialoog te treden met de particuliere sector en die dialoog te onderhouden en methoden te bespreken om ervoor te zorgen dat bewijsmateriaal op een zodanige manier wordt vergaard dat het in rechtbanken ontvankelijk kan zijn.***

XIII - CLOUDCOMPUTING

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Een aanzienlijk aantal lidstaten stelde nadrukkelijk dat in de cloud gepleegde cybercriminaliteit tot problemen leidt bij onderzoek en vervolging.

- Sommige lidstaten hadden op het tijdstip van de evaluatie geen ervaring met onderzoek naar cybercriminaliteit van dit type en bijgevolg was het vraagstuk over de rechtsmacht over opslag in de cloud voor hun nationale rechtbanken nog niet aan de orde gekomen, wat kan betekenen dat een aantal cybermisdrijven in de praktijk onopgemerkt blijft; er werd evenwel onderkend dat zij onvermijdelijk met dergelijke situaties zullen worden geconfronteerd.

- Dit fenomeen kan leiden tot ernstige problemen in de toekomst, aangezien cloud-oplossingen steeds populairder worden en het gebruik van opslag in de cloud en clouddiensten in toenemende mate uitgroeit tot een gangbare praktijk, niet alleen voor rechtspersonen en natuurlijke personen, maar ook voor delinquenten die illegale inhoud op een sluikse manier willen opslaan; met name plegers van seksueel misbruik van kinderen via het internet zijn steeds vaker verborgen omdat ze meer gebruik maken van onlineopslag in de cloud.

- Vanwege de gebruikte technologieën en vanwege de opslagcapaciteit in servers en schaalvoordelen, vliegen gegevens voortdurend de wereld rond en kunnen zij worden gesplitst in delen die weer bijeen moeten worden gebracht bij het opvragen. Een specifiek probleem bij strafbare feiten in verband met de cloud is daarom het achterhalen van de eigenlijke fysieke locatie waar het strafbare feit in feite wordt gepleegd, hetgeen moeilijk te bepalen, zeer ingewikkeld en tijdrovend kan zijn.

- Daarom is het niet makkelijk de plaats te bepalen van de informatie en de computers die de informatie verwerken in de cloud, waar voor het onderzoek van strafbare feiten belangrijke informatie kan worden opgeslagen, of deze informatie en computer te raadplegen.

- Het gebrek aan informatie kan het moeilijker maken de dader, het tijdstip van het strafbare feit, de plaats waar en het instrument waarmee het strafbare feit is gepleegd vast te stellen, en dit leidt tot gevallen waarin cybercriminaliteit ongestraft blijft en tot situaties waarin mensen er telkens opnieuw het slachtoffer van worden.

- Ook aanbieders van opslag in de cloud kunnen moeilijkheden ondervinden om de eigenlijke (territoriale) plaats van gegevens te bepalen; zelfs de eigenaren van de gegevens weten vaak niet waar de gegevens zich bevinden.

- De plaats waar de dader zich bevond op het moment van het begaan van het strafbare feit of waar de gevolgen zich voordeden, wordt vaak aangemerkt als de plaats van het in de cloud gepleegde strafbare feit. Afhankelijk van het type cybercriminaliteit kunnen de gevolgen worden toegerekend aan de jurisdictie van verschillende lidstaten, ook buiten de jurisdictie van andere EU-lidstaten.

- De methode van cloudcomputing leidt bijgevolg niet alleen tot problemen in verband met nationaal recht, maar ook in verband met internationaal recht, dat is gebaseerd op de erkenning van de onafhankelijkheid van staten en op het territorialiteitsbeginsel.

- Ook al is de locatie vastgesteld, dan nog biedt de nationale wetgeving van sommige lidstaten niet de mogelijkheid van extraterritoriale rechtsmacht, of kan cybercriminaliteit in de cloud slechts worden vervolgd indien dergelijke gegevens raadpleegbaar zijn vanuit de betrokken lidstaten.

- Wat betreft de bevoegdheid voor het uitvaardigen van een bevel om elektronisch bewijsmateriaal te verkrijgen, kunnen jurisdictiegeschillen ontstaan wanneer twee of meer lidstaten rechtsmacht met betrekking tot het strafbare feit kunnen vestigen; in die gevallen kunnen lidstaten om deze conflicten op te lossen gebruik maken van de diensten van Eurojust en van gezamenlijke onderzoeksteams.

- Er zijn twee mogelijkheden voor het verkrijgen van in de cloud opgeslagen gegevens: ofwel wordt rechtstreekse toegang tot de inhoud van dergelijke profielen en opslagfaciliteiten verkregen door toestemming van de gebruiker/eigenaar van het profiel of de account, ofwel moet de plaats van de informatie worden vastgesteld en moet een beroep worden gedaan op de tijdrovende en inefficiënte procedures voor wederzijdse rechtshulp.

- De andere optie, namelijk providers rechtstreeks opdragen bepaalde gegevens te verstrekken, blijkt vaak zeer moeilijk in de praktijk te brengen omdat er providers zijn die geen medewerking verlenen aan de buitenlandse politiediensten en niet elk verzoek beantwoorden.

- Om deze moeilijkheden te overwinnen, werd er in de evaluatie op gewezen dat met de belangrijkste cloudaanbieders (bv. Google, Yahoo, enz...) bijzondere regelingen zouden kunnen worden getroffen om vertragingen te beperken en informatie te verkrijgen in vormen die in rechtbanken ontvankelijk zijn.

- De Raad van Europa heeft verdragsovereenkomsten gesloten in verband met dergelijke aangelegenheden (onder meer met derde staten, zoals de Verenigde Staten van Amerika, Canada, Australië en Japan). Uit hoofde van het Verdrag inzake cybercriminaliteit is grensoverschrijdend optreden slechts mogelijk in een zeer beperkt aantal gevallen, d.w.z. met de rechtmatige instemming van de persoon die beschikt over de wettelijke bevoegdheid de gegevens prijs te geven, indien de rechtsmacht bekend is. Indien de plaats van de gegevens onbekend is, zijn deze bepalingen ontoereikend.

- Er is dus nog geen bevredigende oplossing gevonden voor het probleem van opslag in de cloud. De diverse bij internationaal recht geboden mogelijkheden om onafhankelijk of in onderlinge samenwerking (rechtshulp) op te treden bij onderzoeken van via de cloud gepleegde cybercriminaliteit blijken beperkt.

- Volgens de conclusies van de evaluatie moet op dergelijke situaties worden vooruitgelopen en moet worden nagedacht hoe de praktijk kan worden verbeterd, zodat doeltreffend onderzoek en doeltreffende vervolging kunnen worden gewaarborgd zonder dat zich jurisdictiegeschillen voordoen.

- Daartoe zou het nuttig kunnen zijn te overwegen om de bestaande toepasselijke rechtskaders aan te passen en/of onderzoekskwesties op te lossen om in verband met in de cloud gepleegde cybercriminaliteit over duidelijke regels en procedures te beschikken.

- De deelname van lidstaten als waarnemers in internationale fora, bijvoorbeeld in de commissie Cybercrimeverdrag, waar oplossingen voor deze problemen worden besproken, is in het kader van de evaluatie ook als nuttig aangemerkt.

- Eén lidstaat bracht voorstellen voor het raadplegen van in de cloud opgeslagen gegevens naar voren, zoals het bieden van de mogelijkheid om virtuele zoekopdrachten uit te voeren in datacentra in andere landen zonder eerst de fysieke locatie van de server te moeten vaststellen en/of de aanbieders van datadiensten te verplichten wachtwoorden te verstrekken aan rechtshandhavingsinstanties zodat deze toegang hebben tot de gegevens.

AANBEVELINGEN

- ***De lidstaten dienen te overwegen met de belangrijkste cloudaanbieders (bv. Google, Yahoo, enz...) bijzondere regelingen te treffen om vertragingen te beperken en informatie te verkrijgen in formaten die in rechtbanken ontvankelijk zijn.***

- ***De lidstaten dienen waar nodig na te denken over een herziening van hun bestaande rechtskaders met het oog op duidelijke regels en procedures in verband met in de cloud gepleegde cybercriminaliteit, onder meer door te voorzien in de mogelijkheid van extraterritoriale rechtsmacht voor onderling verband houdende strafbare feiten.***

- ***De EU-instellingen dienen de mondiale problematiek van cloudcomputing aan te pakken om manieren te vinden voor het vergroten van het vermogen om in de cloud gepleegde cybercriminaliteit op te sporen en bewijs van strafrechtelijke aansprakelijkheid dat in strafrechtelijke procedures kan worden gebruikt, te lokaliseren en er toegang toe te krijgen.***

XIV - BEWARING VAN ELEKTRONISCHE-COMMUNICATIEGEGEVENS

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- De ongeldigverklaring van Richtlijn 2006/24/EG (Richtlijn gegevensbewaring) heeft geleid tot een situatie van rechtsonzekerheid, vooral wat betreft de juridische status van de nationale omzettingsmaatregelen en de beschikbaarheid van elektronische-communicatiegegevens die zijn verzameld met het oog op toegang voor de rechtshandhavingsinstanties en gebruik tijdens strafrechtelijke procedures.

- De lidstaten die niet langer uit hoofde van een specifiek rechtsinstrument van de Unie verplicht zijn om een nationale regeling inzake gegevensbewaring in te voeren of te handhaven waardoor providers verplicht zijn elektronische-communicatiegegevens op te slaan, hebben de uitspraak een uiteenlopende invulling gegeven en zijn overgegaan tot de handhaving, wijziging, vervanging of intrekking van de omzettings-maatregelen of tot de ongeldigverklaring ervan door nationale rechtbanken.

- De evaluatie heeft bevestigd dat de lidstaten zich zorgen maken over het ontbreken van een gemeenschappelijk rechtskader inzake gegevensbewaring op Unieniveau en de daaruit voortvloeiende versnippering van de gegevensbewaringsregelingen in de Unie, hetgeen aanzienlijke problemen binnen de Unie en in de internationale samenwerking met derde landen doet ontstaan.

- Verscheidene lidstaten hebben de nadruk gelegd op de negatieve gevolgen van de bovengenoemde uitspraak voor de doeltreffendheid van strafrechtelijke onderzoeken en vervolgingen op nationaal niveau, vooral wat betreft de betrouwbaarheid en ontvankelijkheid voor rechtbanken van bewijsmateriaal dat is gebaseerd op de vergaring van elektronische-communicatiegegevens en op de grensoverschrijdende justitiële samenwerking tussen lidstaten en op internationaal niveau (een beperkt vermogen tot het verstrekken/verwerven van bewijsmateriaal).

- Het niet of slechts voor een beperkte periode bewaren van bepaalde gegevens maakt het moeilijk of zelfs onmogelijk om elektronisch bewijsmateriaal in de EU-lidstaten veilig te stellen via de toepassing van de standaardprocedures.

- Er werd met name op gewezen dat deze ontwikkeling een ernstige negatieve invloed had op het vermogen van de bevoegde nationale autoriteiten om cybercriminaliteit en andere criminaliteit waarbij elektronisch bewijsmateriaal en internet- of telecommunicatiegegevens in belangrijke mate zouden kunnen bijdragen tot de identificatie van de daders, doeltreffend te onderzoeken en te vervolgen.

- Verscheidene lidstaten beklemtoonden dat een gemeenschappelijke aanpak op Unieniveau, met onder meer de mogelijkheid tot een nieuw rechtskader dat de voorwaarden en perioden voor gegevensbewaring in de lidstaten zou harmoniseren, een meerwaarde zou bieden.

- Intussen heeft het Hof in de gevoegde zaken C-203/15 en C-698/15 van 21 december 2016 over "Tele2 en Watson" geoordeeld dat nationale wetgeving die verplicht tot het algemeen en ongedifferentieerd bewaren van alle verkeers- en locatiegegevens niet evenredig is, en het heeft duidelijkheid verschaft over de criteria en voorwaarden waaraan de nationale gegevensbewaringsregelingen van de lidstaten moeten voldoen.

- Momenteel is een gemeenschappelijk reflectieproces aan de gang waarbij de EU-instellingen en de lidstaten zijn betrokken, teneinde de kwestie van gegevensbewaring aan te pakken om juridische en praktische oplossingen te vinden voor de problemen die op dit vlak voortvloeien uit de jurisprudentie van het Hof van Justitie van de Europese Unie.

AANBEVELINGEN

- ***De lidstaten en de EU-instellingen dienen de gemeenschappelijke reflectie voort te zetten om juridische en praktische oplossingen te vinden voor de bewaring van elektronische-communicatiegegevens op nationaal en op EU-niveau, rekening houdend met de beginselen die zijn verankerd in recente HvJ-rechtspraak.***

XV - MAATREGELEN TEGEN KINDERPORNOGRAFIE EN SEKSUEEL MISBRUIK VAN KINDEREN VIA HET INTERNET

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie was op het tijdstip van de evaluatie door de meerderheid van de lidstaten omgezet.
  De huidige stand van zaken met betrekking tot de omzetting van deze Richtlijn in nationale maatregelen kan worden geraadpleegd via volgende link: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093

- Vanwege maatschappelijke en technologische ontwikkelingen, waardoor zowel de mogelijkheden voor communicatie en de verspreiding van informatie als de mogelijkheid tot het plegen van strafbare feiten op het internet zijn uitgebreid, is er de laatste jaren een sterke toename van het seksueel misbruik van kinderen via het internet (grooming, sexting, cyberpesten, enz.). Om dergelijke vormen van criminaliteit doeltreffend te bestrijden, wordt in de lidstaten een breed scala van zowel preventieve als repressieve maatregelen toegepast waarbij de overheidssector en de particuliere sector beide zijn betrokken.

- In sommige lidstaten bestaat er een nationale databank voor het identificeren van slachtoffers met het oog op de bestrijding van seksueel misbruik van kinderen, of werd er ten tijde van de evaluatie werk van gemaakt. In de meerderheid van de lidstaten bestaat er echter nog geen dergelijke nationale databank, of was die op het tijdstip van de evaluatie nog niet voldoende ontwikkeld. In deze gevallen gebruiken de rechtshandhavingsinstanties alleen internationale databanken en instrumenten, in het bijzonder de internationale databank van Interpol inzake seksuele uitbuiting van kinderen, die een krachtig instrument voor inlichtingen en onderzoek vormt voor de identificering van slachtoffers en daders, aangezien gespecialiseerde onderzoekers dankzij de databank gegevens uit de hele wereld kunnen delen.

- Indien de politie van een lidstaat een slachtoffer niet via de databank kan identificeren, maar beschikt over redelijke vermoedens over de mogelijke identiteit van een kind, toont zij een of meer afbeeldingen van het slachtoffer aan scholen om het kind te identificeren, en dit kan worden beschouwd als een goede praktijk.

- Om herhaald slachtofferschap te voorkomen, bestaan er verschillende benaderingen in de lidstaten. Maatregelen zijn, naast het blokkeren en/of verwijderen van materiaal betreffende seksueel misbruik van kinderen, onder meer het plaatsen op een lijst van gevaarlijke media die als schadelijk voor minderjarigen worden beschouwd, het beperken van de contacten met de dader, begeleiding van en advies voor slachtoffers door ngo's, alsmede specifieke maatregelen ter bescherming van slachtoffers en getuigen van seksueel misbruik van kinderen tegen de negatieve weerslag tijdens strafrechtelijke procedures.

- In enkele lidstaten zijn er geen specifieke maatregelen van kracht ter voorkoming van herhaald slachtofferschap, maar wordt met dit doel samengewerkt met ngo's, met gespecialiseerde niet-politiële instanties en instellingen met bevoegdheden op het gebied van de bescherming van minderjarigen of met de subprioriteit van cybercriminaliteit "kindermisbruik via het internet" van Empact.

- In de lidstaten worden er diverse juridische, technische, organisatorische en voorlichtingsmaatregelen getroffen om seksuele uitbuiting/seksueel misbruik via het internet, sexting, cyberpesten en kindersekstoerisme tegen te gaan. Verscheidene lidstaten hebben gespecialiseerde eenheden of speciale functionarissen die zich uitsluitend met seksueel misbruik van kinderen bezig houden om kinderen en daders te identificeren en onderzoeken te voeren. Een goede praktijk in één lidstaat is de beoordeling bij indienstneming en de jaarlijkse psychologische controle van gespecialiseerde politieagenten die op dit gebied actief zijn.

- Alle lidstaten hebben, in uiteenlopende mate, voorzien in preventieve maatregelen ter propagering van veilig gebruik van het internet door minderjarigen, die vaak zijn ontwikkeld onder toezicht van nationale overheidsinstanties en in samenwerking met de gespecialiseerde eenheden en de ngo's die met kinderen werken. Sommige projecten op dit gebied worden medegefinancierd door de EU, zoals het Europees netwerk voor een veiliger internet (Insafe) in het kader van het "Safer Internet"-programma van de Europese Commissie.

- Preventieve maatregelen omvatten onder meer opleidingsprojecten en voorlichtings-campagnes gericht op bewustmaking en het onderwijzen van specifieke doelgroepen (studenten, ouders, onderwijspersoneel en andere groepen) over de belangrijkste potentiële risico's waarmee minderjarigen op het internet worden geconfronteerd, en met het oog op het stimuleren van een verantwoord gebruik van het internet. De in één lidstaat gehanteerde moderne werkwijzen, waarbij kinderen leren van andere kinderen, werden als een goede praktijk beschouwd. In sommige lidstaten organiseert ook de politie deze activiteiten of neemt ze eraan deel.

- Media-onderwijs is ook een krachtig instrument voor het voorkomen van seksueel misbruik van kinderen, vooral van kinderen en adolescenten, en in sommige lidstaten wordt op gespecialiseerde websites informatie gepubliceerd over veilig gedrag op het internet voor kinderen. Andere lidstaten beschikken over uitvoerige brochures, handboeken of schoolgidsen voor een veilig en efficiënt gebruik van het internet, cyberpesten, enz...

- De meerderheid van de lidstaten heeft een alarmnummer dat anoniem kan worden gebruikt om inhoud met seksueel misbruik van kinderen te signaleren en dat vaak ook dienst doet als hulplijn voor kinderen, tieners en ouders en anonieme en kosteloze bijstand biedt via de telefoon en het internet (websites of platforms), ook met betrekking tot de vraag hoe een klacht kan worden ingediend bij de politie. Een Europees onlineplatform – www.reportchildsextourism.eu – bevat een vermelding van alle nationale alarmnummers in Europa.

- De meeste lidstaten hebben strafrechtelijke bepalingen inzake strafbare feiten en sancties voor reizende plegers van kindermisbruik, of passen andere maatregelen toe, onder meer tegen het reclame maken voor de mogelijkheden tot misbruik en kindersekstoerisme, zoals de maatregelen in artikel 21 van Richtlijn 2011/93/EU. Maatregelen ter verbetering van de opsporing van deze specifieke vorm van criminaliteit omvatten onder meer monitoring- of signaleringssystemen over reizen van seksuele delinquenten, acties met behulp van de toerisme- en reissector en de buitenlandse dienst, de detachering van verbindings-functionarissen in het buitenland, de inbeslagname van het paspoort van een veroordeelde kindermisbruiker, enz...

- Algemene maatregelen voor de vroegtijdige opsporing van seksueel misbruik van kinderen op het internet omvatten onder meer het monitoren van het internet en infiltratie-onderzoeken, die een doeltreffend instrument blijken om seksuele uitbuiting van kinderen via het internet in realtime tegen te gaan, alsmede filterinstrumenten, die echter niet in alle lidstaten worden toegepast en vaak niet verplicht zijn voor internetproviders.

- Repressieve maatregelen in gevallen van seksueel misbruik van kinderen op het internet, zoals het blokkeren van toegang, het verwijderen van inhoud en het van het internet halen van webpagina's, worden in de lidstaten niet op dezelfde wijze toegepast, onder meer wat betreft de procedurele vraag of een rechterlijk bevel nodig is vooraf of ter bevestiging van de door de politie getroffen maatregelen.

- In de meerderheid van de lidstaten worden juridische en praktische maatregelen genomen om audiovisueel materiaal betreffende seksueel misbruik van kinderen permanent van het internet te verwijderen. De "verwijder"-benadering kan worden beschouwd als een effectieve maatregel, aangezien zo kan worden voorkomen dat afbeeldingen/videobeelden van minderjarigen blijvend op het internet te zien zijn. Andere lidstaten gebruiken ook, of soms uitsluitend, de "blokkeren van de toegang"-benadering, die erin bestaat de toegang tot de websites met kinderpornografie te blokkeren door dergelijk materiaal tijdelijk ontoegankelijk te maken.

- Indien het materiaal zich op servers in het buitenland bevindt, wordt doorgaans een beroep gedaan op internationale kanalen, met name Europol en zijn beveiligd systeem van informatie-uitwisseling SIENA, of Interpol en zijn initiatief tot het blokkeren van toegang; de alarmcentrales kunnen tegelijk ook Inhope op de hoogte stellen (International Association of Internet Hotlines - internationale associatie van internet-alarmnummers), dat ervoor zorgt dat kinderpornografisch materiaal dat tot één staat is gericht, maar in het buitenland is opgeslagen, van het internet kan worden verwijderd.

- In enkele lidstaten worden websites met kinderpornografisch materiaal geblokkeerd en ontoegankelijk gemaakt, ongeacht of de site zich binnen of buiten de EU bevindt, hetgeen als een goede praktijk wordt beschouwd.

- Voor de toepassing van de bovenstaande repressieve maatregelen is een goede samenwerking tussen alle relevante belanghebbenden, met name de rechtshandhavingsautoriteiten, de alarmcentrales, ngo's en internetproviders, essentieel. In sommige lidstaten zijn internet-providers verplicht passende actie te ondernemen om het mogelijk gebruik van dergelijk materiaal te verstoren, door het blokkeren van de toegang of het verwijderen van inhoud van het internet, terwijl de nationale wetgeving van andere lidstaten die verplichting niet bevat, hoewel de bovenstaande maatregelen wel kunnen worden genomen in afzonderlijke gevallen op grond van een rechterlijk bevel.

- De samenwerking in de lidstaten tussen de politie en binnenlandse internetproviders verloopt over het algemeen vlot, en de providers verwijderen illegale kinderpornografische inhoud vaak onmiddellijk en spontaan wanneer zij een kennisgeving van de politie ontvangen, zelfs wanneer zij daar niet toe zijn verplicht. Een instrument dat in één lidstaat wordt gebruikt, waarbij alle providers hetzelfde interface-icoon gebruiken met een signaleringsknop waarop kan worden geklikt om aan te geven dat een bepaalde website kinderpornografisch materiaal bevat, werd genoemd als een voorbeeld van een goede praktijk.

AANBEVELINGEN

- ***De lidstaten die dit nog niet hebben gedaan, dienen een specifieke nationale databank te ontwikkelen voor slachtofferidentificatie ter bestrijding van seksueel misbruik van kinderen.***

- ***De lidstaten die zulks nog niet hebben gedaan, dienen zich te beraden op het ontwikkelen van specifieke maatregelen ter voorkoming van secundair slachtofferschap, waaronder maatregelen ter bescherming van slachtoffers en getuigen van seksueel misbruik van kinderen tegen de negatieve weerslag tijdens strafrechtelijke procedures.***

- ***De lidstaten dienen te zorgen voor een goed functionerende samenwerking tussen alle relevante belanghebbenden, met name de rechtshandhavingsinstanties, teneinde strafbare feiten ten aanzien van kinderen op het internet efficiënt te bestrijden, en na te denken over het invoeren van een verplichting voor internetproviders om passende maatregelen te nemen, zoals het blokkeren van toegang, het verwijderen van inhoud en het van het internet halen van webpagina's.***

XVI -MECHANISME OM OP ERNSTIGE CYBERAANVALLEN TE REAGEREN

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Op het moment van de evaluatie was Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen door de meerderheid van de lidstaten omgezet. De huidige stand van zaken met betrekking tot de omzetting van deze Richtlijn in nationale maatregelen kan worden geraadpleegd via de volgende link: http://eur-lex.europa.eu/legal-content/NL/NIM/?uri=celex:32011L0093.

- Cyberaanvallen vormen een veranderende bedreiging, worden uitgevoerd met steeds verfijndere methodes en instrumenten en beslaan een uiterst ruim spectrum. De evaluatie wijst in het bijzonder op een aanzienlijke toename in de EU van de aanvallen met ransomware, een vorm van malware waarbij de toegang tot gegevens wordt geblokkeerd totdat er losgeld wordt betaald.

- Bij cyberaanvallen is er behoefte aan een technische beoordeling (digitale analyse van het materiaal dat tijdens de operaties in beslag is genomen, waaronder het zoeken naar virussen, het terughalen van verwijderde gegevens, enz.) waarvoor bepaalde lidstaten een beroep doen op de particuliere sector, die over een goede expertise en betere instrumenten beschikt en goedkoper kan werken. Daarnaast dient te worden nagegaan welke gevolgen mogelijke aanvallen hebben voor de infrastructuren en dient te worden overgegaan tot een brede situationele bewustmaking en beoordeling van de aanval, met inbegrip van de gebruikte methoden en instrumenten.

- Met het oog op de coördinatie van de reactie op de noodsituatie en het daaropvolgende herstel van de informatiesystemen worden passende tegenmaatregelen getroffen, evenals maatregelen om de gevolgen van de cyberaanvallen te beperken. Teneinde een behoorlijk beveiligingsniveau van de cyberruimte te waarborgen is het tevens essentieel dat preventieve maatregelen worden genomen (systematische samenwerking en informatie-uitwisseling onder alle openbare en particuliere actoren met betrekking tot de mondiale bewustmakings-maatregelen, betrokkenheid bij onderzoek inzake beveiliging, technische analyses en situatieverslagen).

- Doorgaans zijn het verschillende actoren die de gedeelde verantwoordelijkheid dragen voor de uitvoering van deze taken om de beveiliging van de mondiale cyberspace op nationaal niveau te verzekeren. Met het oog op een goede weerbaarheid van de nationale cyber-beveiligingssystemen ten aanzien van cyberdreigingen is er behoefte aan een passend juridisch en institutioneel kader en aan een geïntegreerd multidisciplinair mechanisme. Daarbij dient er sprake te zijn van een goede coördinatie tussen het strategische en het operationele niveau (met name in geval van kritieke infrastructuur en overheidssectoren), met inbegrip van een passend crisisbeheersingssysteem om de respons- en hersteloperaties te coördineren.

- In een aantal lidstaten wordt reeds een gestructureerde aanpak gehanteerd waarbij verschillende instanties betrokken zijn, en in sommige gevallen is deze gebaseerd op publiek-private partnerschappen. In andere lidstaten is een dergelijke aanpak nog niet voldoende ontwikkeld of zelfs geheel afwezig, en functioneert het coördinatiemechanisme om op cyberaanvallen te reageren voornamelijk op basis van informele samenwerking.

- Op het moment van de evaluatie hadden de meeste lidstaten reeds een nationaal computercrisisteam ingesteld of waren zij daarmee bezig. Voor enkele lidstaten was dat nog niet het geval.

- De voornaamste taken van computercrisisteams betreffen het monitoren van en reageren op cyberincidenten, het verstrekken van vroegtijdige waarschuwingen, signaleringen en risico- en incidentanalyses, alsmede het totstandbrengen van samenwerking met de particuliere sector.

- In bepaalde lidstaten gaat de rol van nationale computercrisisteams zelfs verder dan de bovengenoemde taken, doordat zij tevens databanken over bedreigingen en incidenten beheren; de uitwisseling van informatie tussen verschillende entiteiten ondersteunen; advies en bijstand verstrekken in verband met de bescherming van de computersystemen van de openbare en de particuliere sector; proactieve activiteiten verrichten voor het afzwakken van de risico's van incidenten in computerbeveiliging; bewustmakings- en opleidingsactiviteiten verrichten; optreden als tussenpersoon tussen de particuliere sector, de academische wereld en de politie; en het nationale contactpunt voor internationale samenwerking zijn.

- Computercrisisteams van de overheid zijn voornamelijk verantwoordelijk voor het beheersen van crises en het reageren op cyberdreigingen en -incidenten die de overheidssector treffen, maar in veel gevallen ook de kritieke infrastructuren, en in een beperkt aantal gevallen ook het particuliere domein, dat doorgaans tot de taak behoort van andere computercrisisteams, uit de particuliere sector.

- In een aantal lidstaten hebben computercrisisteams van de overheid coördinerende en toezichthoudende taken met betrekking tot andere relevante belanghebbenden. Dat blijkt met name nuttig in lidstaten waar het mechanisme om op cyberaanvallen te reageren heel complex is en/of een aanzienlijk aantal verschillende computercrisisteams uit de openbare en de particuliere sector naast elkaar bestaan.

- Computercrisisteams beschikken ten aanzien van particulieren niet over de bevoegdheden die rechtshandhavingsautoriteiten hebben, maar wat betreft aanvallen van criminele aard (niet alle IT-incidenten zijn strafbare feiten) spelen zij een belangrijke rol bij de ondersteuning van het onderzoek, aangezien zij kunnen helpen met het verstrekken van informatie en het veiligstellen van bewijsmateriaal. Het is derhalve zeer belangrijk dat computercrisisteams goed met rechtshandhavingsinstanties samenwerken, want het efficiënt verkrijgen van informatie en bewijsmateriaal over aanvallen is cruciaal voor het onderzoek van cyberaanvallen, aangezien elektronische gegevens uiterst dynamisch zijn en gemakkelijk verloren kunnen gaan. In voorkomend geval kunnen andere criminele-inlichtingendiensten en/of inlichtingendiensten bij het onderzoek van cyberincidenten worden betrokken.

- Overeenkomstig Richtlijn (EU) 2016/1148 (NIS-richtlijn), die uiterlijk op 9 mei 2018 in nationale wetgeving dient te zijn omgezet, moeten de lidstaten beschikken over goed functionerende CSIRT's (Computer Security Incident Response Teams), ook bekend als computercrisisteams (CERT's - Computer Emergency Response Teams), die voldoen aan bepaalde voorschriften ten behoeve van een doeltreffende capaciteit voor het aanpakken van incidenten en risico's en een doeltreffende samenwerking op het niveau van de Unie.

- Digitale weerbaarheid kan niet door de overheid alleen worden verwezenlijkt. In dit verband is ook een belangrijke rol weggelegd voor de particuliere sector, en met name voor exploitanten van kritieke infrastructuren, informatiesystemen en netwerken, die rechtstreeks zijn betrokken bij het beheersen van risico's en het beveiligen van hun netwerken en diensten.

- Overeenkomstig de NIS-Richtlijn zorgen de lidstaten ervoor dat aanbieders van essentiële diensten zorgen voor de beveiliging van hun netwerken en informatiesystemen en dat zij ieder incident dat substantiële gevolgen heeft voor de verlening van een dienst onverwijld aan de bevoegde autoriteit of de CSIRT's melden. Wanneer de NIS-Richtlijn volledig wordt geïmplementeerd, zullen de met kritieke infrastructuur belaste entiteiten wettelijk verplicht zijn cyberaanvallen van criminele aard te melden.

- Op het moment van de evaluatie gold in sommige lidstaten reeds een verplichting voor de particuliere sector om incidenten met elektronische aanvallen in de cyberruimte aan de wetshandhavingsinstanties te te melden. In een aantal gevallen was deze verplichting evenwel beperkt tot bepaalde takken van de particuliere sector of bepaalde soorten incidenten, of waren er geen sancties verbonden aan de niet-naleving van de meldingsplicht.

- In bepaalde gevallen geschiedt de melding op vrijwillige basis, zonder formele verplichting, maar, zoals in een aantal verslagen wordt benadrukt, worden incidenten dikwijls onvoldoende gemeld omdat aanbieders van diensten terughoudend zijn met het oog op mogelijke reputatieschade als gevolg van strafrechtelijke procedures (voor meer informatie, zie het hoofdstuk over samenwerking). Zoals in één landverslag uitdrukkelijk wordt gesteld, kunnen politiediensten, teneinde de melding te stimuleren, benadrukken dat onderzoek geheim kan zijn en dat goede resultaten kunnen worden geboekt zonder dat dit afbreuk doet aan hun reputatie.

- Uit de bevindingen van de evaluatie blijkt dat er zonder rapportageverplichting een reëel gevaar bestaat dat de meeste gevallen van cyberincidenten niet aan de autoriteiten worden gemeld, waardoor vervolging en bestraffing voor daarmee verband houdende cybermisdrijven afhankelijk worden gesteld van de belangen van de particuliere sector en niet van het algemeen belang.

- Een verplicht meldingssysteem, met name voor ernstige misdrijven, is niet alleen van belang voor rechtshandhavingsdoeleinden dankzij het faciliteren van een snelle en volledige situatiebeoordeling en een snellere uitvoering van gerichte tegenmaatregelen, maar is tevens nuttig om autoriteiten een beter overzicht van de dreigingen te geven, om volledige statistieken over het aantal cyberbeveiligingsincidenten te verzamelen en om de juiste voorzorgsmaatregelen te nemen. Het vaststellen van een meer bindend juridisch kader voor de melding door ondernemingen van cyberaanvallen, bijvoorbeeld door deze verplicht te maken, zoals in een aantal lidstaten reeds het geval is, wordt door de beoordelaars als een goede praktijk beschouwd.

- Met het oog op een hoog niveau van cyberveiligheid en beveiligingsbewust gedrag van leiders, systeemontwikkelaars en gebruikers, moet de veiligheid worden verbeterd.
  Dat betekent dat bewustmaking op alle niveaus, zoals dat in bepaalde lidstaten reeds gebeurt, een belangrijk onderdeel is van een doeltreffende aanpak van cyberbeveiliging.

- Omdat cyberdreigingen en -aanvallen soms een horizontale dimensie hebben, blijkt "Empact Cyber-attacks" een nuttig platform om de lidstaten, betrokken instellingen en instanties en partners uit de particuliere sector beter te doen samenwerken bij het ontwikkelen en verspreiden van antimalware en het beschermen tegen infrastructuuraanvallen via netwerken.

- Er zij gewezen op de nauwe samenwerking tussen de computercrisisteams van de drie Baltische staten, die in november 2015 een memorandum van overeenstemming ondertekend hebben ondertekend waarbij zij toezegden nauwer te zullen samenwerken op het gebied van cyberbeveiliging en de bescherming van IT-systemen en netwerken.

- Bij de aanpak van cyberaanvallen buiten de Unie worden formele kanalen voor wederzijdse rechtshulp gebruikt. Aangezien tijd een cruciale factor kan zijn bij cyberaanvallen (gezien de volatiele aard van gegevens), wordt, met het oog op snellere en efficiëntere samenwerking, ook rechtstreeks of via Europol en Interpol samengewerkt en informatie uitgewisseld tussen politiediensten. Een aantal lidstaten maakt tevens gebruik van het 24/7-netwerk van contactpunten van de G7.

- De digitale agenda voor Europa moedigt de lidstaten ertoe aan om uiterlijk in 2020 een goed functionerend EU-breed netwerk van computercrisisteams op nationaal niveau op te zetten. De Europese Commissie verzoekt de lidstaten om de samenwerking tussen de bestaande nationale computercrisisteams te versterken en de bestaande samenwerkingsmechanismen, waaronder de Europese groep van computercrisisteams van de overheid (European Governmental CERTs Group - EGC), uit te breiden.

- Ook op internationaal niveau wordt overleg gepleegd en samengewerkt via wereldwijde netwerken van computercrisisteams, zoals het International Watch and Warning Network (IWWN), FIRST, het European Government Cert network en TF-CSIRT, met het oog op samenwerking inzake cyberincidenten, met inbegrip van wederzijdse steun voor het beheer van IT-situaties en -crisisbeheer, aangezien deze netwerken regelmatig oefeningen uitvoeren. Netwerken van computercrisisteams kunnen zich deels toespitsen op dezelfde thema's, zoals netwerken met teams van overheden of autoriteiten, en deels op verschillende thema's, zoals netwerken met teams uit het bedrijfsleven, uit de wetenschappelijke wereld en van autoriteiten.

AANBEVELINGEN

- ***Om een passend niveau van bescherming en beveiliging van de nationale cyberruimte te waarborgen, dienen de lidstaten te zorgen voor een efficiënt institutioneel kader, dat gebaseerd is op een aanpak waarbij verschillende instanties betrokken zijn en op een goed functionerende samenwerking tussen alle belanghebbenden op het gebied van cyberbeveiliging, met inbegrip van de particuliere sector.***

- ***Overeenkomstig de NIS-Richtlijn dienen de lidstaten die nog geen nationaal computercrisisteam hebben ingesteld, dit alsnog te doen. Om een hoog niveau van cyberbeveiliging te waarborgen, dienen de lidstaten te overwegen computercrisisteams van de overheid taken toe te wijzen die hen in staat stellen om als centrale coördinatiepunten te fungeren voor andere computercrisisteams en belanghebbenden die betrokken zijn bij de voorkoming van cyberdreigingen en bij de reactie op cyberbeveiligingsincidenten.***

- ***Daartoe dienen de lidstaten tevens te overwegen om computercrisisteams van de overheid te belasten met het verzamelen en analyseren van cyberincidenten, om hun capaciteit om op dreigingen te reageren en hun softwaresystemen voor vroegtijdige waarschuwing te ontwikkelen, en om te voorzien in gerichte opleidingen inzake cybercriminaliteit en cyberbeveiliging.***

- ***Overeenkomstig de NIS-Richtlijn dienen de lidstaten die dit nog niet hebben gedaan, in hun nationale recht de gehele particuliere sector te verplichten om cyberaanvallen met aanzienlijke gevolgen voor de continuïteit van essentiële diensten onverwijld aan de rechtshandhavingsinstanties te melden.***

- ***De lidstaten worden aangemoedigd deel te nemen aan het platform "Empact Cyber-attacks", evenals aan Europese en wereldwijde netwerken van computercrisisteams.***

XVII - SAMENWERKING MET EU-INSTANTIES

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Aangezien dikwijls verschillende lidstaten bij cybercriminaliteit, cybergerelateerde misdrijven en het onderzoek daarnaar betrokken zijn, vormen samenwerking en informatie-uitwisseling met EU-instanties een prioriteit.

- Europol/EC3, Eurojust, het EJN en het ENISA spelen een cruciale rol met een breed scala van activiteiten, waaronder analyses van trends in cybercriminaliteit, coördinatie van onderzoeken, uitwisseling van informatie en inlichtingen, gegevensanalyse en opleidingen in de hele EU. Hun deskundigheid en faciliteiten maken samenwerking tussen de lidstaten en hun respectieve rechtshandhavingsinstanties en openbare ministeries mogelijk.

- Eurojust speelt een cruciale rol bij de coördinatie van strafrechtelijke onderzoeken en bij de verlening van rechtshulp voor grensoverschrijdende samenwerking tussen de lidstaten, welke bijzonder nuttig blijkt in complexe zaken met cybergerelateerde feiten. Het draagt tevens bij tot het faciliteren en bespoedigen van de samenwerking met de bevoegde autoriteiten van de lidstaten en derde landen op het gebied van cybercriminaliteit.

- Eurojust verzamelt en verspreidt ook casestudies en beste praktijken, voorziet in opleidingsactiviteiten op het gebied van cybercriminaliteit, en bevordert de uitwisseling van ervaringen tussen gespecialiseerde rechters op het gebied van cybercriminaliteit.

- Het faciliteert samenwerking en informatie-uitwisselingen tussen de lidstaten, levert operationele producten en diensten aan onderzoeksdiensten, voorziet in forensische en operationele opleidingen, en verspreidt bewustmakingsmateriaal. Het EC3 fungeert als een Europese dienst die gespecialiseerd is in de bestrijding van cybercriminaliteit, verricht analyses van het fenomeen cybercriminaliteit als geheel, coördineert de activiteiten van alle betrokkenen, en blijkt zeer nuttig bij onderzoeken die in verschillende landen tegelijk worden verricht. Europol beschikt over verschillende instrumenten om de uitwisseling van kennis en inlichtingen op dit gebied tussen de rechtshandhavingsinstanties van de lidstaten onderling en met Europol mogelijk te maken, zoals het Empact-initiatief inzake cybercriminaliteit, het Siena-systeem en J-CAT. Uit operationele ervaring blijkt dat een voldoende vakkundige J-CAT-verbindingsofficier van de lidstaten betrokken moet zijn bij elke goed doordachte inspanning ter bestrijding van cybercriminaliteit.

- De lidstaten waarderen in het algemeen de door Europol/EC3, Eurojust en het EJN geboden steun en coördinatie bij de ondersteuning van de contactpunten, en zij zijn van oordeel dat hun rol cruciaal is voor het scheppen van meer vertrouwen tussen onderzoeksinstanties en openbare aanklagers en het faciliteren van internationale samenwerking, ook met derde landen.

- De rol die het ENISA speelt bij het verzamelen van cybersignaleringen en het doorzenden daarvan naar geautomatiseerde systemen is tevens essentieel voor het verbeteren van de technische beveiliging van informatiesystemen.

- De bevoegdheden en de diensten van Europol, Eurojust, het EJN en het Enisa met betrekking tot cybercriminaliteit zijn echter niet altijd volledig bekend, en hun producten en diensten worden niet ten volle benut door de betrokken beroepsbeoefenaars in de lidstaten.

AANBEVELINGEN

- ***De lidstaten dienen optimaal gebruik te maken van de door Eurojust, het EJN en Europol aangeboden diensten met betrekking tot cybercriminaliteit, en dienen nauwe samenwerking tussen de nationale computercrisisteams en het Enisa te faciliteren.***

- ***Eurojust, Europol en het ENISA dienen te overwegen om het publiek bewust te maken van hun diensten en van de bestaande mogelijkheden voor samenwerking en gespecialiseerde opleiding die zij op het gebied van cybercriminaliteit aanbieden, en om hun actieve steun te verlenen aan evenementen die de internationale samenwerking inzake de bestrijding van cybercriminaliteit versterken.***

- ***Europol dient tevens de implementatie van het Siena-systeem in de opsporingsdiensten te benutten, de zichtbaarheid van Empact-projecten te verbeteren, te bezien hoe J-CAT het best kan worden ingezet, te overwegen de lidstaten een voorstel te doen voor een gestandaardiseerde aanpak inzake structurele elementen voor databanken met criminele inlichtingen bij de bestrijding van cybercriminaliteit, en de vaststelling van een gemeenschappelijke taxonomie inzake cybercriminaliteit te faciliteren.***

- ***Het ENISA dient te onderzoeken hoe het concept van door geautomatiseerde systemen verzamelde en doorgezonden cybersignaleringen kan worden gestandaardiseerd, zodat de statistieken met betrekking tot deze signaleringen vergelijkbaar en geharmoniseerd zijn in de lidstaten.***

XVIII - GEZAMENLIJKE ONDERZOEKSTEAMS (GOT'S)

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Aangezien cybercriminaliteit dikwijls een grensoverschrijdende dimensie heeft, kan deelname aan internationaal gecoördineerde onderzoeken nuttig zijn voor het doeltreffend vervolgen van strafbare feiten in verband met cyberaanvallen.

- Binnen het EU-kader zijn de gemeenschappelijke onderzoeksteams (GOT's) een instrument voor internationale samenwerking in gevallen van grensoverschrijdende criminaliteit, op basis van een overeenkomst tussen de bevoegde autoriteiten van twee of meer lidstaten - op het gebied van zowel justitie als rechtshandhaving - met het oog op de gezamenlijke uitvoering van strafrechtelijke onderzoeken.

- Op het moment van de evaluatie hadden verschillende lidstaten, in uiteenlopende mate van frequentie, deelgenomen aan GOT's in verband met gevallen van cybercriminaliteit, terwijl andere lidstaten dat nog nooit hadden gedaan.

- De deelnemende lidstaten beschrijven deelname aan GOT's doorgaans als een positieve ervaring en zij beschouwen GOT's als een doeltreffend instrument voor grensoverschrijdende onderzoeken dat rechtstreekse informatie-uitwisseling tussen onderzoekers en tijdige inzameling van bewijsmateriaal mogelijk maakt zonder dat daarvoor afzonderlijke formele verzoeken om wederzijdse rechtshulp moeten worden ingediend.

- Gelet op de langdurige procedures voor wederzijdse rechtshulp draagt de inzet van GOT's bij tot kortere onderzoeken en tot meer vertrouwen tussen nationale autoriteiten.

- Hoewel de deelname van Europol en Eurojust aan het opzetten en optreden van GOT's niet verplicht is, zoals sommige lidstaten hebben opgemerkt, kunnen de twee organisaties een belangrijke rol spelen bij het waarborgen van de efficiëntie en de operationele capaciteit van GOT's. Voor een aantal lidstaten is het van cruciaal belang dat GOT's door Eurojust en Europol kunnen worden gefinancierd.

AANBEVELINGEN

- ***De lidstaten worden ertoe aangemoedigd om in grensoverschrijdende gevallen van cybercriminaliteit vaker gebruik te maken van GOT's met het oog op een efficiënter onderzoek, en om daartoe beroepsbeoefenaars bewuster te maken van de mogelijkheden en voordelen van GOT's.***

- ***De Europese instellingen, en in het bijzonder Europol en Eurojust, dienen het opzetten van GOT's verder te ondersteunen en te faciliteren en dienen adequate financiële middelen beschikbaar te stellen om de lidstaten te helpen meer gebruik te maken van GOT's.***

XIX - WEDERZIJDSE RECHTSHULP

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Cybercriminaliteit heeft dikwijls een grensoverschrijdend karakter, aangezien cyber-gerelateerde of gedigitaliseerde misdrijven vaak door buitenlandse onderdanen worden gepleegd en daarbij vaak buitenlandse IT-infrastructuur wordt gebruikt. Een soepele en goed functionerende internationale samenwerking is derhalve cruciaal om cybercriminaliteit efficiënt aan te pakken.

- Wederzijdse rechtshulp van een derde land kan in alle fasen van de procedure en voor alle procedurele en onderzoekshandelingen noodzakelijk zijn, afhankelijk van de aard van het cybermisdrijf dat de onrechtmatige gedraging vormt.

- Zoals uit een groot aantal individuele verslagen blijkt, hebben op dit gebied de meest voorkomende verzoeken om wederzijdse rechtshulp van en aan de lidstaten betrekking op criminaliteit in verband met het internet, zoals computergerelateerde fraude en vervalsing, op aanvallen op computers en op strafbare feiten met kredietkaarten. Daarom wordt in veel rechtshulpverzoeken met betrekking tot cybercriminaliteit gevraagd om specifiek bewijsmateriaal dat in handen van aanbieders van diensten is (traceren van telecommunicatie en identificatie van IP-gebruikers), om onderzoek en inbeslagneming van computersystemen en om bankinformatie.

- In geen enkele lidstaat bevat de nationale wetgeving een specifieke bepaling inzake wederzijdse rechtshulp in verband met cybercriminaliteit, zodat de algemene procedures en voorwaarden voor de verzoeken om wederzijdse rechtshulp van toepassing zijn in gevallen van cybercriminaliteit.

- Wederzijdse rechtshulp, onder meer op het gebied van cybercriminaliteit, kan worden verleend op basis van multilaterale verdragen, bilaterale overeenkomsten of wederkerigheid. De nationale instanties die verantwoordelijk zijn voor de ontvangst of verzending van verzoeken om wederzijdse rechtshulp verschillen naargelang het toepasselijke internationale instrument.

- De meerderheid van de EU-lidstaten is partij bij het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie van 29 mei 2000 (Rechtshulpverdag), dat overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie werd gesloten, en bij het Aanvullend Protocol van 2001 bij dat Verdrag. De meerderheid van de EU-lidstaten neemt tevens deel en geeft uitvoering aan het Schengenacquis, zodat de in de Schengenovereenkomst vervatte bepalingen inzake justitiële samenwerking ook van toepassing zijn, hetgeen vooral van belang is voor lidstaten die geen partij zijn bij het Rechtshulpverdrag.

- Deze instrumenten maken rechtstreekse communicatie tussen de justitiële autoriteiten (rechtbanken en openbare ministeries) van de lidstaten mogelijk, ongeacht de fase waarin het verzoek wordt gedaan (onderzoek, vervolging, berechting of tenuitvoerlegging). Daarom worden verzoeken om wederzijdse rechtshulp rechtstreeks verzonden van de bevoegde justitiële autoriteiten van de verzoekende lidstaat naar de bevoegde justitiële autoriteiten van de uitvoerende lidstaat, die bevoegd is beslissingen over de verzoeken te nemen.

- In geval van verzoeken tussen lidstaten die de bovengenoemde instrumenten niet toepassen of verzoeken om hulp van en aan derde staten, afhankelijk van de toepasselijke bilaterale of multilaterale overeenkomsten, worden verzoeken om wederzijdse rechtshulp rechtstreeks (tussen bevoegde of centrale nationale justitiële autoriteiten) of langs diplomatieke weg (via het ministerie van Buitenlandse Zaken) doorgestuurd.

- Wanneer het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken van 20 april 1959 en de bijbehorende Aanvullende Protocollen van 1978 en 2001 van toepassing zijn, moeten rogatoire commissies aan het ministerie van Justitie van de verzoekende staat worden gericht en via dezelfde kanalen worden teruggezonden. Tijdens onderzoeken, of in spoedeisende gevallen, kan een verzoek echter rechtstreeks door de nationale justitiële autoriteit van de verzoekende lidstaat (actieve wederzijdse rechtshulp) aan de nationale justitiële autoriteit van de uitvoerende lidstaat (passieve rechtshulp) worden doorgezonden.

- Justitiële verzoeken om wederzijdse rechtshulp worden doorgaans voorafgegaan door verzoeken om spoedbewaring van digitaal bewijsmateriaal in de vorm van opgeslagen computergegevens als bedoeld in artikel 29 van het Verdrag van Boedapest inzake cybercriminaliteit van 22 november 2001.

- Ten aanzien van staten die geen partij zijn bij de bovengenoemde multilaterale verdragen en de relevante bilaterale overeenkomsten kan wederzijdse rechtshulp plaatsvinden op basis van het wederkerigheidsbeginsel.

- De gemiddelde termijn voor de beantwoording van een verzoek om wederzijdse rechtshulp bedraagt gewoonlijk enkele maanden maar varieert naargelang de wederzijdse rechtshulp op grond van een internationale overeenkomst of op grond van wederkerigheid wordt verleend. In dat laatste geval is de beantwoordingstermijn zelfs langer omdat eerst een waarborg van wederkerigheid moet worden toegekend/ontvangen.

- Op het snel veranderende gebied van cybercriminaliteit, leiden langdurige procedures tot inefficiënte formele kanalen voor wederzijdse rechtshulp, hetgeen negatieve gevolgen heeft voor de uitvoering en het welslagen van het onderzoek. Digitaal bewijsmateriaal is immers volatiel en moet snel en efficiënt worden behandeld, aangezien gegevens verloren kunnen gaan als gevolg van vertragingen. Er is dus een algemene behoefte aan een snellere afhandeling van verzoeken om wederzijdse rechtshulp in onderzoeken naar cyber-criminaliteit. De verbetering van de kwaliteit van verzoeken om wederzijdse rechtshulp kan de uitvoering ervan in andere landen aanzienlijk versnellen.

- Als alternatief voor de formele kanalen voor wederzijdse rechtshulp, maken sommige lidstaten, met het oog op een snellere beantwoording, gebruik van kanalen van Europol, Eurojust en het EJN, waaronder J-CAT bij het EC3, of van Interpol, het netwerk van contactpunten van de G7, netwerken van verbindingsofficieren of bilaterale contacten. Niettemin moet in aanmerking worden genomen dat de geldigheid van de gegevens moet worden gecontroleerd indien deze minder formele kanalen worden gebruikt.

- De steun van Eurojust bij het faciliteren van communicatie en bij het versnellen van de uitvoering van urgente verzoeken aan en door niet alleen EU-lidstaten maar ook derde landen, wordt door verschillende lidstaten als zeer nuttig beschouwd, mede gezien de fysieke aanwezigheid van openbare aanklagers uit de VS, Noorwegen en Zwitserland bij Eurojust die een verbindingsfunctie vervullen.

- Wat niet-EU-landen betreft, gaat het bij verzoeken om wederzijdse rechtshulp in strafzaken waarbij cybercriminaliteit een rol speelt, voornamelijk om verzoeken aan en van de Verenigde Staten; het is van cruciaal belang dat daarmee soepel wordt samengewerkt omdat veel internetproviders zich binnen zijn rechtsgebied bevinden.

- Veel lidstaten ondervinden in dit verband evenwel belemmeringen, met name op het gebied van gegevensbewaring en de openbaarmaking van de IP-adressen van gebruikers van Facebook en andere sociale netwerken. Zoals de beoordelaars in een aantal individuele verslagen hebben aangegeven, vormt toegang tot de databanken van uit de VS afkomstige sociale netwerken op het internet een permanent probleem waaronder alle lidstaten lijden.

- De Verenigde Staten stellen in het algemeen sterke formele en inhoudelijke eisen aan dergelijke verzoeken, met name wat betreft het verband tussen het strafbare feit en het specifieke bewijsmateriaal dat het voorwerp van het overdrachtsverzoek uitmaakt.

- Volgens de evaluatie zou het nuttig zijn werk te maken van internationale oplossingen ter verbetering van procedures voor wederzijdse rechtshulp met derde staten, waaronder, zoals in één lidstaat gebeurt, het gebruik van een formulier voor verzoeken om versnelde overlegging zoals overeengekomen door uitvoerende autoriteiten in een bepaalde lidstaat, hetgeen als een beste praktijk kan worden beschouwd.

- Op grond van de wetgeving van de Verenigde Staten inzake het zoeken naar een locatie of het verkrijgen van e-mailgegevens en om het even welke inhoud van een bij een internet-provider opgeslagen communicatie, is een rechterlijk bevel (huiszoekingsbevel - "search warrant") vereist. De hoeveelheid bewijs die vereist is om een huiszoekingsbevel te verkrijgen, staat bekend als het redelijk vermoeden van schuld ("probable cause").
  Dit betekent dat de autoriteiten van de VS bijkomende informatie zullen verzoeken in geval van een verzoek om wederzijdse rechtshulp met het oog op het verkrijgen van inhoud van opgeslagen communicatie van een internetprovider. Deze procedure is erg tijdrovend en resulteert in veel gevallen niet in de uitvoering van het verzoek.

- Vaak zijn aan de VS gerichte verzoeken om wederzijdse rechtshulp niet uitgevoerd, hoewel in een aantal verzoeken werd gewezen op het belang van de zaak en de noodzaak van het gevraagde bewijsmateriaal.

- Voor een aantal lidstaten is de ontwikkeling van informele en persoonlijke contacten met de bevoegde autoriteiten van derde staten voorafgaand aan de verzending van een verzoek om wederzijdse rechtshulp nuttig gebleken met het oog op een betere en snellere samenwerking bij de uitvoering van dergelijke verzoeken.

- Het opzetten van een registratiesysteem en een beheersysteem voor wederzijdse rechtshulp waarbij zaken vanaf de registratie tot aan de verzending van het antwoord aan het verzoekende land kunnen worden gevolgd, kan als een goede praktijk worden beschouwd.

AANBEVELINGEN

- ***De lidstaten dienen de kwaliteit van de verzoeken om wederzijdse rechtshulp aan andere landen te verbeteren, met name om ervoor te zorgen dat zij voldoende volledig zijn, en te onderzoeken hoe de snelheid en de kwaliteit van de antwoorden kunnen worden verbeterd.***

- ***De lidstaten wordt aanbevolen het communicatieproces met andere lidstaten en derde landen doeltreffende te maken door het opzetten van een registratiesysteem en een beheersysteem voor wederzijdse rechtshulp waarbij zaken vanaf de registratie tot aan de verzending van het antwoord aan het verzoekende land kunnen worden gevolgd.***

- ***De lidstaten worden aangemoedigd frequenter gebruik te maken van de instrumenten van Eurojust, het EJN, en Europol, en om informele contacten aan te knopen met de bevoegde buitenlandse autoriteiten teneinde van derde landen sneller antwoord te krijgen op verzoeken om wederzijdse rechtshulp.***

- ***De EU dient na te denken over het coördineren van de inspanningen ter vaststelling van een effectieve manier van communiceren en uitvoeren van verzoeken om wederzijdse rechtshulp van haar lidstaten aan derde landen, of over het instellen van een kader voor rechtstreekse samenwerking met relevante internetproviders buiten de EU.***

- ***De EU dient te werken aan oplossingen voor een beter en sneller communicatieproces tussen de lidstaten en derde landen, in het bijzonder de Verenigde Staten, met name wat betreft de uitwisseling van operationele informatie en verzoeken om wederzijdse rechtshulp en de uitvoering ervan.***

XX - OPLEIDING

BELANGRIJKSTE BEVINDINGEN EN CONCLUSIES

- Rekening houdend met de snelle technologische vooruitgang en de evoluerende aard van cybercriminaliteit, en dus ook met de behoefte om gelijke tred te houden met nieuwe tendensen en geavanceerdere modi operandi, is het voor het welslagen van onderzoeken en vervolgingen van cybergerelateerde en gedigitaliseerde misdrijven van cruciaal belang dat beroepsbeoefenaars op alle niveaus gespecialiseerde, regelmatige en voortdurende opleidingen volgen, ook in het begin van hun loopbaan.

- In de meeste lidstaten worden aanzienlijke inspanningen, middelen en mensen geïnvesteerd in gespecialiseerde opleidingen op het gebied van cybercriminaliteit voor rechts-handhavingsautoriteiten, maar de magistratuur heeft niet in alle lidstaten hetzelfde opleidingsniveau en in sommige lidstaten zijn magistraten niet verplicht opleidingen te volgen.

- Gelet op de specifieke technische kenmerken van cybercriminaliteit in het kader van onderzoeken en op het feit dat daders van cybercriminaliteit voor de rechter moeten worden gebracht, moeten de betrokken rechters ook over een grote mate van inzicht ter zake beschikken. Gespecialiseerde opleidingen, onder meer over hoe elektronisch bewijsmateriaal moet worden verzameld, geanalyseerd en gebruikt, zijn dan ook essentieel voor openbare aanklagers en rechters die met cybercriminaliteit te maken hebben.

- Naast de opleidingen door openbare instellingen (politie, rechtscolleges of -instituten) worden in bepaalde lidstaten ook opleidingen in verband met cybercriminaliteit georganiseerd door externe partijen, zoals universiteiten en privé-ondernemingen uit de sector, waarvan de expertise zeer nuttig blijkt met het oog op hoogwaardige opleidingen. Sommige lidstaten hebben uiterst gespecialiseerde kenniscentra opgezet die opleidingen op het gebied van cybercriminaliteit organiseren voor zowel de publieke als de particuliere sector.

- In een aantal lidstaten worden dergelijke opleidingen ook georganiseerd in de vorm van afstandsonderwijs, e-learning of podcasts, hetgeen als een goede praktijk en een doeltreffende opleidingsmethode kan worden beschouwd.

- In aanvulling op opleidingen op nationaal niveau organiseren relevante EU-organen - EC3/Europol, de ECTEG (*Europese groep voor opleiding in verband met cybercriminaliteit*), Eurojust, OLAF, Cepol en het Enisa — gespecialiseerde opleidingen op het gebied van cybercriminaliteit. Die mogelijkheid wordt door de lidstaten doorgaans niet ten volle benut.

- Een aantal lidstaten heeft een specifiek budget vrijgemaakt voor opleidingen op het gebied van cybercriminaliteit. Bepaalde lidstaten dienen bijkomende inspanningen te leveren om betere gespecialiseerde opleidingen op het gebied van cybercriminaliteit aan te bieden aan alle categorieën ambtenaren die bij zaken van cybercriminaliteit zijn betrokken.

- Volgens de evaluatie kan een geïntegreerde benadering inzake gemeenschappelijke opleidingen voor rechters, openbare aanklagers en vertegenwoordigers van rechts-handhavingsinstanties bijdragen aan de verspreiding van de kennis over cybercriminaliteit en dienstdoen als platform voor de uitwisseling van ervaringen en beste praktijken op het gebied van cybercriminaliteit en voor het bespreken van belemmeringen inzake de ontvankelijkheid van bewijs. Uit de wederzijdse evaluatie bleek evenwel dat slechts enkele lidstaten deze soort van gezamenlijke opleidingen reeds aanbieden.

AANBEVELINGEN

- ***De lidstaten dienen te zorgen voor een alomvattend opleidingsprogramma voor het gehele verloop van cybercriminaliteitszaken dat bestemd is voor alle belanghebbenden en beroepsbeoefenaren die bij de bestrijding van cybercriminaliteit betrokken zijn, en met name voor meer regelmatige opleidingen voor magistraten. Zij dienen tevens te overwegen een specifiek budget vrij te maken voor opleidingen op het gebied van cybercriminaliteit.***

- ***De lidstaten dienen te overwegen een gezamenlijke opleiding op het gebied van cybercriminaliteit voor politiefunctionarissen, openbare aanklagers en rechters te organiseren, en de e-learning-aanpak te hanteren.***

- ***De lidstaten dienen optimaal gebruik te maken van de opleidingsmogelijkheden die worden aangeboden door EU-organen, zoals EC3/Europol, de ECTEG, Cepol, Eurojust, OLAF en het Enisa, en door academische instellingen en privé-ondernemingen, en dienen te overwegen hoogst gespecialiseerde kenniscentra op te zetten met het oog op gespecialiseerde opleidingen op het gebied van cybercriminaliteit.***

- ***De EU-instellingen dienen meer EU-financiering aan te bieden om de lidstaten te helpen meer gespecialiseerde opleidingen te organiseren voor personen die zich in de lidstaten beroepsmatig bezighouden met cybercriminaliteit.***