Raad van de
Europese Unie

Brussel, 26 juni 2015
(OR. en)

7587/15
DCL 1

GENVAL 8
CYBER 22

DERUBRICERING

van document:	7587/15 RESTREINT UE/EU RESTRICTED
d.d.:	15 mei 2015
nieuwe status:	Publiek
Betreft:	Evaluatierapport van de zevende wederzijdse evaluatie "De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit" - Rapport over Nederland

Hierbij gaat voor de delegaties de gederubriceerde versie van bovengenoemd document.

De tekst van dit document is identiek aan die van de voorgaande versie.

Raad van de
Europese Unie

Brussel, 15 april 2015
(OR. en)

7587/15

RESTREINT UE/EU RESTRICTED

GENVAL 8
CYBER 22

VERSLAG

van:	het secretariaat-generaal van de Raad
aan:	de delegaties
Betreft:	Evaluatierapport van de zevende wederzijdse evaluatie "De praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit" - Rapport over Nederland

EVALUATIERAPPORT OVER DE
ZEVENDE WEDERZIJDSE EVALUATIE

"Praktische uitvoering en toepassing van het Europese beleid inzake preventie en bestrijding van cybercriminaliteit"

RAPPORT OVER NEDERLAND

1. SAMENVATTING

Het evaluatiebezoek was zeer goed georganiseerd en voorbereid door de Nederlandse autoriteiten. De keuze van de overheidsinstanties waaraan een bezoek werd gebracht en de deelnemers waarmee een ontmoeting plaatsvond, was goed. Het evaluatieteam apprecieerde met name de verwelkoming door het ministerie van Veiligheid en Justitie en zijn coördinerende rol gedurende het hele bezoek. De evalueerders kregen de kans om te spreken met een groot aantal professionals van de Nederlandse centrale overheid, en met vertegenwoordigers van de rechterlijke macht, de politie en de particuliere sector.

Nederland is sterk gedigitaliseerd, zowel economisch als maatschappelijk. Nederland gaat voort met het creëren van de noodzakelijke kennis, capaciteit en wetgeving om de cyberveiligheid te verbeteren en cybercriminaliteit te bestrijden. Dat is immers geen gemakkelijk proces en vergt veel middelen en de medewerking van de belangrijkste betrokkenen uit zowel de publieke als de private sector.

Nederland heeft een strategie uitgestippeld en prioriteiten ter bestrijding van cybercriminaliteit bepaald die duidelijk zijn weergegeven in de Nationale Cybersecuritystrategie (NCSS2). Daarin wordt strategische sturing op tactisch en operationeel niveau verstrekt, zoals over het aanscherpen van nationale en internationale wetgeving, het aanpakken van cybercriminaliteit, preventie en bewustmaking, het verbeteren van de samenwerking met alle relevante nationale en internationale actoren en capaciteitsopbouw. Al die doelen moeten worden bereikt met inachtneming van de grondrechten zoals vrijheid van meningsuiting en privacy.

Nederland beschikt over een consistent juridisch kader, zowel op inhoudelijk als procedureel vlak. De tenuitvoerlegging van Richtlijn 2013/40/EG over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad moet in 2015 worden afgerond en moet de Nederlandse wetgeving nog beter maken.

De Nederlandse strategie inzake cybercrime wordt, in praktisch opzicht op velerlei manieren ten uitvoer gelegd, onder meer door het deelnemen aan de Virtual Global Task Force, het aanstellen van een verbindingsambtenaar bij het Interpol "Global Complex for Innovation" van Interpol in Singapore, een geplande uitwisseling van personeel en kennis met Europol/EC3, het stationeren van twee flexibele verbindingsambtenaren in Zuid-Amerika en de Filipijnen om zich te buigen over aangelegenheden in verband met online seksueel misbruik van kinderen, en waardevol werk m.b.t. de subprioriteiten op het gebied van cybercrime (online kaartfraude, online seksueel misbruik van kinderen en cyberaanvallen) van de EU-beleidscyclus ter bestrijding van georganiseerde en zware internationale criminaliteit.

Die doelstellingen worden ook bereikt via publieke en private partnerschappen en via bewustmaking. Vele initiatieven zijn het vermelden waard. Het Nationaal Cyber Security Centrum (NCSC), dat gevestigd is bij het ministerie van Veiligheid en Justitie, richt zich op de vitale sectoren van het land en heeft op dat gebied een speerpuntfunctie. Zijn belangrijkste partners uit de private sector zijn derhalve energiebedrijven, en de telecommunicatie- en de financiële sector. Zij zullen verplicht worden alle cyberinbreuken die zich voordoen aan het NCSC te melden. Er staat echter geen sanctie op het niet melden aan het NCSC, al zullen de bevoegde autoriteiten (toezichthouder gegevensbescherming, toezichthouder banken, enz.) er wel rekening mee houden of een bedrijf een inbreuk gemeld heeft of niet). Doordat het niet verplicht is grootscheepse aanvallen op door particuliere bedrijven gerunde vitale infrastructuur te melden, wordt naar de mening van de evalueerders, de bevoegdheid om criminelen te bestrijden en voor de rechter te brengen daarom in handen gelegd van de particuliere sector.

Het andere succesvolle initiatief is de ECTF, die opgezet is om digitale bankfraude effectiever te bestrijden, met name phishing en financiële malware.

Nederland prioriteert de bestrijding van cybercriminaliteit en de respons op aanvallen tegen of verstoringen van informatiesystemen tevens door het versterken van zijn huidige opsporings- en vervolgingscapaciteit. De opsporing van zware gevallen van cybercriminaliteit op landelijk niveau wordt gecoördineerd door een kerndriehoek bestaande uit de Team High Tech Crime van de landelijke politie, het Nationaal Cyber Security Centrum (NCSC) en het Landelijk Parket, die vlot en efficiënt samenwerken. Het eigenlijk strafrechtelijk onderzoek wordt uitgevoerd door de politie en het Openbaar Ministerie.

De politie en het OM hebben verbindingsambtenaren bij het NCSC. Het onderzoek naar cybercriminaliteit op nationaal niveau wordt aangevuld met de structuur voor de bestrijding van cybercriminaliteit bij de regionale politie. Deze (teams in regionale politie-eenheden) zijn, in samenwerking met het Nederlands Forensisch Instituut (NFI) en het OM, betrokken bij de meeste cybercrimezaken. Volgens de informatie die is ingewonnen bij het bezoek ter plaatse, beschikken de verschillende regionale instanties niet over evenveel operationele middelen. Dat moet worden rechtgezet, met name omdat het bij de zaken die onder de bevoegdheid van de regionale autoriteiten vallen, juist gaat om zaken die de onbeschermde burger het meest aangaan en tot op zekere hoogte zichtbaarder zijn voor de gemeenschap.

Anderzijds is de Nederlandse praktijk van het combineren van de mogelijkheden van private bedrijven (zoals internetdienstaanbieders (ISP's) en socialemediabedrijven), overheidsinstanties (zoals bv. het ministerie van Veiligheid en Justitie) en gespecialiseerde eenheden die zich exclusief bezighouden met online seksueel misbruik van kinderen) en op het grote publiek gerichte campagnes om online seksueel misbruik van kinderen doeltreffend te bestrijden, naar de mening van het evaluatieteam het volgen waard.

Nederland werkt inzake cybercriminaliteit internationaal voorbeeldig samen binnen Europol/EC3 en Eurojust, en met Interpol en andere derden. De mogelijkheden van die samenwerking lijken op nationaal niveau goed bekend te zijn. Toch moeten de regionale politie en de rechterlijke macht verder worden opgeleid. Een verplicht opleidingsprogramma in verband met cybercriminaliteit, althans voor degenen die zich met cybercrimezaken bezighouden, kan de kloof inzake communicatie en wederzijds begrip tussen rechercheurs, aanklagers en rechters van cybercriminaliteit dichten (er zou meer gebruik kunnen worden gemaakt van initiatieven zoals het Kenniscentrum Cybercrime bij het Gerechtshof in de Haag). Een bindende, gemeenschappelijke begripsomschrijving van cybercriminaliteit voor statistische doeleinden zou ook helpen.

Hoewel de algemene evaluatie van cybercriminaliteit in Nederland niet compleet is door het gebrek aan gedetailleerde, gestandaardiseerde en volledige statistieken over opsporing, vervolging, veroordelingen en gemelde cybercriminaliteit-incidenten, had het evaluatieteam waardering voor de manier waarop het systeem werkt. De strategie in Nederland is duidelijk het land onaantrekkelijk te maken voor cybercriminelen. Gelet op de belangrijke rol van die Nederland speelt bij het bieden van infrastructuur en hostingdiensten, worden de inspanningen en de middelen die het land steekt in het tegengaan van cybercriminaliteit, en de effectiviteit daarvan, door de evalueerders als ronduit positief beoordeeld.

2. INLEIDING

Na de aanneming van Gemeenschappelijke optreden 97/827/JBZ van5 december 1997[1], is er een mechanisme ingesteld voor het evalueren van de toepassing en uitvoering, op nationaal niveau, van internationale initiatieven bij de bestrijding van georganiseerde criminaliteit. Overeenkomstig artikel 2 van het 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 het Europese beleid 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 van misdrijven valt, werd overeengekomen dat bij de evaluatie het accent zal liggen op misdrijven die volgens de lidstaten speciale aandacht behoeven. Daarom zal de evaluatie hoofdzakelijk gericht zijn op drie specifieke gebieden: cyberaanvallen, online seksueel misbruik van kinderen/kinderpornografie en online kaartfraude, en zal er uitgebreid worden ingegaan op de juridische en operationele aspecten van het tegengaan van cybercriminaliteit, grensoverschrijdende samenwerking en samenwerking met ter zake deskundige EU-agentschappen. In dit verband zijn met name van belang: Richtlijn 2011/93/EU van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie en ter vervanging van Kaderbesluit 2004/68/JBZ[2] (uiterste omzettingstermijn: 18 december 2013) en Richtlijn 2013/40/EU[3] over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (uiterste omzettingstermijn: 4 september 2015).

1 Gemeenschappelijk Optreden 97/827/JBZ van 5 december 1997, PB L 344 van 15.12.1997, blz. 7-9.
2 PB L 335 van 17.12.2011, blz. 1.
3 PB L 218 van 14.8.2013, blz. 8.

Voorts werd in de conclusies van de Raad over de strategie inzake cyberbeveiliging van de Europese Unie van juni 2013[4] vooruitgelopen op de spoedige ratificatie van het Verdrag van de Raad van Europa tegen cybercriminaliteit (het verdrag van Boedapest)[5] van 23 november 2001 door alle lidstaten, en in de preambule daarvan wordt benadrukt dat "de EU niet om nieuwe internationale rechtsinstrumenten inzake cyberkwesties vraagt". Het verdrag wordt aangevuld met een protocol betreffende handelingen van xenofobe of racistische aard via computersystemen[6].

De ervaring met eerdere evaluaties leert dat de situatie in de lidstaten wat betreft de uitvoering van de toepasselijke rechtsinstrumenten verschillend is, en dat het huidige evaluatieproces ook een nuttige inbreng kan leveren voor de lidstaten die niet alle onderdelen van de verschillende instrumenten geïmplementeerd hebben. Toch is het de bedoeling dat de evaluatie een breed en interdisciplinair karakter heeft en niet alleen gericht is op de uitvoering van de verschillende instrumenten met betrekking tot het bestrijden van cybercriminaliteit, maar ook op de operationele aspecten in de lidstaten.

Daarom gaat het hierbij, afgezien van samenwerking met de vervolgingsdiensten, ook over de wijze waarop politiële autoriteiten samenwerken met Eurojust, ENISA en Europol/EC3, en de wijze waarop de feedback van die organisaties doorgegeven wordt aan de juiste politie- en sociale diensten. De evaluatie is gericht op de uitvoering van het nationaal beleid met betrekking tot het uitbannen van cyberaanvallen, fraude en kinderporno. Zij omvat ook operationele praktijken in de lidstaten met betrekking tot internationale samenwerking en de steun die geboden wordt aan slachtoffers van cybercriminaliteit.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[5] ETS nr. 185 is op 23 november 2001 opengesteld voor ondertekening en op 1 juli 2004 in werking getreden.

[6] ETS nr. 189 is op 28 januari 2003 opengesteld voor ondertekening en op 1 maart 2006 in werking getreden.

De volgorde van de bezoeken aan de lidstaten werd door GENVAL op 1 april 2014 vastgesteld. Nederland kwam in deze evaluatieronde als tweede lidstaat aan de beurt. Overeenkomstig artikel 3 van het gemeenschappelijk optreden heeft het voorzitterschap een lijst van experts inzake de uit te voeren evaluaties opgesteld. De lidstaten hebben, op een schriftelijk verzoek van de voorzitter van GENVAL aan de delegaties van 28 januari 2014, experts met aanzienlijke praktische kennis op dit gebied aangesteld.

Het evaluatieteam bestaat uit drie nationale deskundigen, ondersteund door twee personeelsleden van het secretariaat-generaal van de Raad en waarnemers. Voor de zevende wederzijdse evaluatie, heeft GENVAL het voorstel van het voorzitterschap aanvaard om de Europese Commissie, Eurojust, ENISA en Europol/EC3 als waarnemers uit te nodigen.

De experts die belast werden met de evaluatie van Nederland waren de heren Attila Kökényesi-Bartos (Hongarije), Wolfgang Bär (Duitsland) en Ivan Bacigál (Slowakije). Als waarnemer waren ook aanwezig: De heren Michele Socco (Commissie), Lionel Ferette (ENISA), José Eduardo Guerra (Eurojust) en Philipp Amann (Europol/EC3), samen met de heren Francisco Rodríguez Rosales en Sławomir Buczma van het secretariaat-generaal van de Raad.

Dit rapport is opgesteld door het deskundigenteam met hulp van het secretariaat-generaal van de Raad, op basis van bevindingen na het evaluatiebezoek dat aan Nederland van 17 tot en met 21 november 2014 en van de gedetailleerde antwoorden van de Nederlanders op de evaluatie-vragenlijst, samen hun gedetailleerde antwoorden op de vervolgvragen.

3. ALGEMENE ZAKEN EN STRUCTUREN

3.1. Nationale Cybersecuritystrategie

In 2011 heeft de Nederlandse regering een Nationale Cybersecuritystrategie (NCSS) gelanceerd, met inbreng van een veelheid aan publieke en private actoren, kennisinstituten en maatschappelijke organisaties. Op 28 oktober 2013 heeft de minister van Veiligheid en Justitie de tweede editie van de Nationale Cybersecuritystrategie gepresenteerd ("NCCS2: Van bewust naar bekwaam").

De bedoeling van de Nederlandse overheid is veilige en betrouwbare ICT te bieden en een open, vrij internet te beschermen: doordat de maatschappij daar steeds afhankelijker van wordt, wordt zij ook kwetsbaarder voor misbruik en verstoring van ICT-systemen. De ambities in de NCSS2 zijn gebaseerd op strategische doelen die als richtsnoeren dienen voor het Actieprogramma 2014-2016. Het aanpakken van cybercriminaliteit is een van die doelstellingen. Cybercriminaliteit wordt als een veelvoorkomende en toenemende dreiging voor alle burgers en organisaties beschouwd. Om adequate bescherming tegen cybercriminaliteit te bieden, wordt in de NCSS2 prioriteit gegeven aan de bestrijding van het fenomeen, door middel van de volgende acties:

1. actualisatie en versterking (inter)nationale (straf)wetgeving (onder andere de Wet Computercriminaliteit III),
2. verbetering samenwerking met EC3 van Europol, onder andere door uitwisseling van kennis en personeel,
3. versterking van opsporing en vervolging van cybercrime als onderwerp meegenomen in discussie nieuwe landelijke beleidsdoelstellingen voor de politie in de gemeenschappelijke veiligheidsagenda (de huidige lopen tot 1 januari 2015) voor de Nederlandse landelijke politie,
4. versterking bestrijding cybercrime in de financiële sector door middel van samenwerking, onder meer met de particuliere sector,
5. aantal internationale onderzoeken wordt uitgebreid tot 20 in 2014,
6. toezien op de aansluiting tussen opsporings- en vervolgingsdiensten bij de digitalisering van criminaliteit,
7. versterking van het intake- en registratieproces van aangifte cybercrime bij de politie.

3.2. Nationale prioriteiten betreffende cybercriminaliteit

In de Nationale Cybersecuritystrategie (NCSS2) worden de algemene nationale prioriteiten voor cyberveiligheid omschreven. Verschillende acties uit hoofde van de andere doelen van de NCSS2, naast het aanpakken van cybercrime, zijn te karakteriseren als acties gericht op preventie, capaciteitsopbouw in zowel de publieke als de private sfeer en bewustmaking. Verwacht wordt dat de volgende acties zullen worden ondernomen:

Preventie

De strategie bevat verschillende specifieke acties ter verbetering van de preventie van cybercrimine. Die acties moeten ook de kwetsbaarheid voor cybercrime verminderen. Daartoe behoren onder meer het vergroten van de weerbaarheid tegen cyberaanvallen, het beschermen van vitale belangen (en infrastructuur), investeringen in veilige ICT-producten en -diensten, en het investeren in kennis en kunde op het gebied van cyberveiligheid.

Wetgeving

Actualiseren en versterken van de wetgeving (onder meer het Wetboek van Strafrecht) is essentieel voor het versterken van een internationale benadering van cybercriminaliteit. De minister van Veiligheid en Justitie werkt aan een nieuw wetsvoorstel over cybercriminaliteit (de Wet computercriminaliteit III) dat naar verwachting in 2015 naar het parlement zal worden gezonden. Doel van de nieuwe wet is maatregelen te nemen om de snelle ontwikkelingen op het gebied van technologie, internet en cybercriminaliteit aan te pakken, met als doel dataversleuteling ongedaan te maken, illegale acties op het internet aan te pakken en online kinderporno te bestrijden. Het wetsvoorstel zal regelgeving introduceren op de volgende gebieden:

- Onderzoek op afstand van de computers van criminelen onder Nederlandse jurisdictie door politiële en justitiële autoriteiten, waaronder, indien nodig, het vermogen om data te kopiëren of ontoegankelijk te maken. Het betreft het zogeheten "onderzoek in een geautomatiseerd werk" dat opsporingsambtenaren ruimte geeft onder strikte voorwaarden verschillende onderzoekshandelingen te verrichten bij de opsporing van ernstige delicten. Dat kan grensoverschrijdende toegang tot gegevens inhouden.

- Er wordt voorzien in de mogelijkheid om verdachten van het bezit en het verspreiden van kinderpornografie of van terroristische activiteiten te verplichten mee te werken aan het openen van versleutelde bestanden op hun computer. De officier van justitie geeft dan een zogenoemd decryptiebevel af aan de verdachte. Politie en justitie krijgen vervolgens toegang tot afgeschermde gegevens. Er gelden echter strikte waarborgen, waaronder een voorafgaande rechterlijke toetsing. Op het negeren van een decryptiebevel van de officier van justitie staat een gevangenisstraf.
- Heling van computergegevens wordt strafbaar. Daarmee wil de minister voorkomen dat na een inbraak in een computer derden de gestolen informatie in handen krijgen en vervolgens op websites plaatsen.
- Het strafbaar stellen van herhaalde fraude op onlinemarktplaatsen.
- Het lokken van kinderen via internet (groomen), waardoor dergelijke misdrijven kunnen worden onderzocht door undercover politieagenten.

Voorts is Nederland ook bezig met het omzetten van Richtlijn 2013/40/EU over aanvallen op informatiesystemen.

Capaciteitsopbouw en opleiding

De afgelopen jaren heeft Nederland geïnvesteerd in capaciteitsopbouw voor rechtshandhaving en strafgerechten. Op landelijk niveau heeft de politie een speciaal Team High Tech Crime voor het opsporen van geavanceerde cybercriminaliteit ingesteld. De nationale ondersteunende eenheid zal worden versterkt met cyberexperts ter ondersteuning van de opsporing van minder geavanceerde cybercriminaliteit, en ter ondersteuning van het verzamelen van digitaal bewijs. De regionale politie-eenheden zullen eenheden van cyberexperts instellen die dezelfde soort ondersteuning zullen bieden op lokaal niveau.

Bewustmaking

Zowel publieke als private partners werken aan bewustmaking en verstrekken informatie aan het publiek over het verbeteren van de cyberbeveiliging en het voorkomen van cybercriminaliteit. Het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie verleent routinematig beveiligingsadvies bij incidenten en specifieke kwetsbare punten (http://www.ncsc.nl en http://www.waarschuwingdienst.nl). In een paar geruchtmakende cybercrimezaken hebben de landelijke politie en het Openbaar Ministerie de bevolking advies verstrekt over het voorkomen van bepaalde soorten cybercriminaliteit.

Het Landelijk Meldpunt Internetoplichting is een samenwerking tussen de Landelijke Politie, het Openbaar Ministerie en de online marktplaats www.marktplaats.nl. Het is een voorziening voor internetklanten om na te gaan of een internethandelaar als onbetrouwbaar te boek staat, en om onlinehandelsfraude aan de politie te melden.

Publieke en private partners werken samen aan het initiatief Digibewust om het algemene bewustzijn inzake beveiliging te vergroten. Digibewust is een samenwerking tussen het ministerie van Economische Zaken, de Europese Commissie en particuliere partners zoals KNP, UPC, IBM en de Nederlandse Vereniging van Banken.

Een ander voorbeeld van een particulier initiatief was de campagne "Hang op, klik weg, bel uw bank", die gelanceerd werd door de Nederlandse Vereniging van Banken (NVB) om de onlinezelfverdediging van de klanten te verbeteren. Die campagne liep tot eind 2014.

Internationale samenwerking

Nederland werkt actief aan nationale en internationale allianties. Bij de meeste grote cybercrimezaken is meer dan één land betrokken. Politie en OM werken regelmatig samen met internationale partnerorganisaties bij internationale zaken en bij de bewijsvergaring. Het actualiseren en versterken van (internationale) strafwetgeving (onder meer de Wet Computercriminaliteit III) en het verbeteren van de samenwerking met Europol/EC3 door uitwisseling van kennis en personeel zijn twee prioriteiten van NCSS2. De Landelijke Politie ondersteunt Europol/EC3 actief.

Nederland steunt ook de ontwikkeling van het Global Complex for Innovation van Interpol in Singapore. Het Openbaar Ministerie heeft, met de hulp van Eurojust en de International Association of Prosecutors, het initiatief genomen om de internationale samenwerking van openbaar aanklagers in cybercrimezaken te intensiveren. Nederland neemt actief deel aan internationale bijeenkomsten en daarmee verband houdende activiteiten, bijvoorbeeld van het Comité van Verdragsluitende Staten van het Cybercrimeverdrag van de Raad van Europa, de beleidscyclus van de EU over georganiseerde criminaliteit, en de besprekingen in de UNODC over een VN-verdrag op het gebied van cybercrime. Nederland investeert ook in kennis en expertise, en neemt deel aan gezamenlijke onderzoeken.

EU-prioriteit cybercriminaliteit

De activiteiten ter verbetering van de bestrijding van cybercriminaliteit vallen grotendeels samen met de doelstellingen van de prioriteiten inzake cybercriminaliteit van de EU. Online kaartfraude is een van de problemen die zijn aangepakt door middel van samenwerking tussen de financiële sector, de Landelijke Politie en het Openbaar Ministerie. Zij delen informatie over specifieke zaken en over nieuwe criminele activiteiten en methodes. Betaalkaarten met "geo-blocking" hebben de online kaartfraude aanzienlijk teruggedrongen.

3.3. Statistieken over cybercriminaliteit

Het ministerie van Veiligheid en Justitie publiceert jaarlijks een Cybersecuritybeeld Nederland (CSBN) in nauwe samenwerking met publieke en private partijen. Het CSBN wordt gepubliceerd ten behoeve van beleidsmakers bij de overheid en vitale economische sectoren, en biedt inzicht in de ontwikkelingen en evaluaties van mogelijke maatregelen voor het verhogen van de digitale weerbaarheid in Nederland. Het CSBN wordt opgesteld in samenwerking met alle ministeries, de inlichtingen- en veiligheidsdiensten, de Defence CERT (DefCERT), de Landelijke Politie, het Openbaar Ministerie, de belastingdienst, leden van ISAC's, wetenschappelijke instellingen en universiteiten, en andere experts in cyberbeveiliging. In het nieuwe CSBN worden cybercriminaliteit en cyberspionage als de grootste bedreigingen in cyberspace bestempeld.

Het ministerie van Veiligheid en Justitie publiceert om de twee jaar ook een Nationaal Dreigingsbeeld Georganiseerde Criminaliteit. Het Dreigingsbeeld laat de grote invloed van moderne ICT op de samenleving zien, en dus ook op de georganiseerde criminaliteit, waarvan het de verschijningsvorm en de methodes heeft veranderd. Dit heeft geleid tot een toename in het aantal en de ernst van high-techmisdrijven (hacken, botnets, de verspreiding van kwaadaardige software (malware)), en van het gebruik van ICT in meer traditionele vormen van misdaad, zoals fraude.

Voorts heeft het Centraal Bureau voor de Statistiek (CBS) in maart 2014 de jaarlijkse Veiligheidsmonitor gepubliceerd, en zich daarbij geconcentreerd op de slachtoffers van verschillende soorten misdrijven. Cybercriminaliteit is een van de thema's. De Veiligheidsmonitor hanteert een zeer ruime begripsomschrijving van cybercriminaliteit, waar onder meer cyberpesten en bedreigingen via sociale media onder vallen. In 2013 was 12% van de inwoners van Nederland ouder dan 15 slachtoffer van een of andere vorm van cybercriminaliteit. Ongeveer de helft van hen was slachtoffer van hacking. Een kwart

van hen was gepest via het internet en nog een kwart was ten prooi gevallen aan onlinehandelsfraude. Jongeren, die verhoudingsgewijs redelijk actief zijn op het internet, worden vaker het slachtoffer. Van alle respondenten in de leeftijd van 15-25 jaar, was bijna 20% ooit slachtoffer van cybercriminaliteit. Voor respondenten in de leeftijdscategorie 25-45, was het cijfer 15%. 20% van alle respondenten zeiden in 2013 het slachtoffer te zijn geweest van een misdrijf. Het document concludeert dat hacken de meest voorkomende vorm van cybercriminaliteit is, skimmen afneemt en onlinehandelsfraude in de lift zit.

De politie en het Openbaar Ministerie rapporteren regelmatig over het aantal onderzoeksrapporten dat aan de officier van justitie wordt toegezonden en over vervolgingen van cybercriminaliteit op grond van bepaalde artikelen van het Wetboek van Strafrecht. In 2013 heeft het gespecialiseerde Team High Tech Crime van de politie negen grote opsporingsonderzoeken verricht en gereageerd op zes internationale verzoeken om bijstand. Kleine onderzoeken zijn niet meegeteld. Andere misdrijven die met behulp van ICT worden begaan, zijn niet afzonderlijk geteld. De vorige jaren richtte het Team High Tech Crime zich vooral op grote opsporingsonderzoeken, en daarom zijn alleen die in aanmerking genomen.

Het evaluatieteam gaf er zich rekenschap van dat er op landelijk niveau geen gedetailleerde, gestandaardiseerde en volledige jaarlijkse statistieken bestaan over alle bedreigingen en incidenten die zich hebben voorgedaan in verband met cyberaanvallen. Meer bepaald is niet bekend hoeveel incidenten niet zijn geregistreerd vanwege de toepassing van het opportuniteitsbeginsel, en daarom geen aanleiding hebben gegeven tot een strafrechtelijk onderzoek. Ook is er geen cijfer beschikbaar voor cybercrime als percentage van de totale criminaliteit. De Nederlandse autoriteiten melden dat de Veiligheidsmonitor vele cijfers verstrekt op basis van meldingen van slachtoffers, maar dat die gegevens lastig te vergelijken zijn door de ruime begripsomschrijving van cybercrime die door verschillende mensen gebruikt wordt.

Naar de mening van de evalueerders, is het door het ontbreken van statistieken moeilijk om een helder beeld te krijgen van enerzijds de ontwikkeling van cybercriminaliteit, en anderzijds de doeltreffendheid van de bestrijding van dit verschijnsel. Sommige van de geregistreerde incidenten lijken op het eerste gezicht van gering belang, maar blijken bij grondiger evaluatie toch een grotere omvang te hebben. Daarom is het evaluatieteam van mening dat het verzamelen van algemene statistieken een gedetailleerde analyse mogelijk kan maken en zo een duidelijker beeld kan helpen scheppen van de effectiviteit van het rechtsstelsel bij de bescherming van burgers die het slachtoffer zijn van cybercriminaliteit.

3.4 Nationale middelen die zijn uitgetrokken ter voorkoming en bestrijding van cybercrime, en steun via EU-financiering

De politie heeft een specifieke capaciteit voor cybercrime en het verzamelen van digitaal bewijs. Het gespecialiseerde Team High Tech Crime zal eind 2014 zijn uitgebreid tot 119 voltijdse personeelsleden. Er worden thans landelijke en regionale centra voor digitale ondersteuning opgezet. Voorts voorziet de minister van Veiligheid en Justitie de politie van een specifiek budget van 13,8 miljoen EUR per jaar voor specifieke verbeteringen bij het voorkomen en bestrijden van cybercriminaliteit en gedigitaliseerde criminaliteit, en voor het versterken van digitaal onderzoek. Het Openbaar Ministerie heeft in elke regio in cybercrime gespecialiseerde officieren van justitie benoemd, alsmede een nationale openbaar aanklager voor cybercriminaliteit.

De Nederlandse autoriteiten hebben twee projecten gemeld die momenteel lopen met steun van het ISEC-fonds:

A. ITOM (Illegal Trade on Online Marketplaces)

- Het ITOM-project[7] is bedoeld om illegale handel op verborgen onlinemarktplaatsen tegen te gaan. Doel is in elke EU-lidstaat multidisciplinaire initiatieven op te zetten (door rechtshandhavingsinstanties en ander publieke en private actoren), kennis, expertise, informatie en inlichtingen te delen, en die acties waar mogelijk te coördineren. Het project wordt gecoördineerd door het Landelijk Parket. De doelstellingen van het ITOM-project betreffen het verkrijgen van inzicht in illegale handel op internet, het ondersteunen van de samenwerking tussen rechtshandhavingsinstanties, het coördineren van multidisciplinaire actie(s), het evalueren van multidisciplinaire interventies en het delen van kennis en expertise.

B. "in-4-mation"

De Nederlandse rechtshandhavingsorganisaties werken samen in het Europese "in-4-mation"-project, waarin de nationale databanken van de deelnemende landen met elkaar verbonden zijn die in beslag genomen en als zodanig aan te merken beelden van seksueel misbruik van kinderen bevatten. Deze "in-4-mation" databank is nog niet gereed, maar Nederland loopt voor op het schema en is al bezig met de implementatie ervan.

3.5 Conclusies

- Nederland beschikt over een integrale nationale cybersecuritystrategie. In 2011 heeft de Nederlandse regering een Nationale Cybersecuritystrategie (NCSS) naar buiten gebracht die in 2013 nader werd uitgewerkt tot de NCSS2.

[7] Het project wordt gesteund door de Portugese Procuradoria-Geral da República, het European Cybercrime Centre (EC3) bij Europol, Eurojust, de National Crime Agency, de Duitse Generalstaatsanwaltschaft Frankfurt am Main en Celle, en in Nederland de Landelijke Politie en het Openbaar Ministerie.

- De NCSS berust op een breed scala van publieke en private partijen, kennisinstellingen en maatschappelijke organisaties. Zij biedt een zeer ruim overzicht van de belangrijke aspecten die meegenomen moeten worden bij het aanpakken van cybercriminaliteit, zoals preventie, wetgeving, capaciteitsopbouw en opleiding, bewustmaking, internationale samenwerking en de prioriteiten van de EU op het gebied van cybercriminaliteit.

- Nederland heeft zijn nationale prioriteiten inzake het aanpakken van cybercriminaliteit duidelijk omschreven. Zij werden opgesteld in 2011 en worden voortdurend verder ontwikkeld. De onlangs aangenomen NCSS2 omvat een actieprogramma voor 2014-2016 met de doelstellingen voor de komende jaren, zoals het aanpakken van cybercriminaliteit, en een aantal acties in verband met het tegengaan van cybercriminaliteit in de financiële sector, nl. door middel van samenwerking, uitbreiding van het aantal internationale opsporingsonderzoeken en verbetering van de samenwerking met Europol/EC3 door het uitwisselen van kennis en personeel.

- Naar de mening van de evalueerders vormt deze strategie, samen met de door Nederland gedefinieerde prioriteiten, een solide basis voor een effectieve bestrijding van cybercrimine. Door nauwe samenwerking tussen organisaties uit de private en de publieke sector ontstaat een unieke kans om een veelheid aan entiteiten de handen in elkaar te doen slaan. Dit moet als beste praktijk worden beschouwd.

- Een van de belangrijkste verwezenlijkingen van het NCSS is het Cybersecuritybeeld Nederland (CSBN), dat het belangrijkste centrale rapportage- en informatiepunt is voor IT-bedreigingen en veiligheidsincidenten.

- Cybercrime heeft vele verschijningsvormen en is niet altijd de dominante factor bij criminele activiteiten. Als men er daarom in zou slagen gedetailleerde, gestandaardiseerde en complete statistieken over cybercrime op te stellen waaruit de totale cybercriminaliteitscijfers af te lezen zijn (gemelde incidenten, meldingen door slachtoffers, aantal besluiten om bepaalde soorten cybercrime niet te onderzoeken, aantal uitgevoerde onderzoeken, aantal vervolgingen en veroordelingen in verband met cybercriminaliteit) zou dat het makkelijker maken cybercrime adequaat te bestrijden en passende vervolgmaatregelen te nemen. Zo'n analyse zou een helderder beeld opleveren van de doeltreffendheid van het rechtsstelsel bij de bescherming van de particuliere belangen van burgers die het slachtoffer zijn van cybercrime. Het probleem kan ook te maken hebben met het ontbreken van een gemeenschappelijke definitie van cybercrime.

- Het evaluatieteam constateerde dat de verschillende betrokkenen (zoals officieren van justitie of politieagenten) een verschillende definitie van cybercriminaliteit hanteren.

- De Nederlandse autoriteiten beschouwen cybercrime als een ernstige bedreiging van de staat en de samenleving. Daarom is een breed spectrum van mensen betrokken bij de bestrijding van cybercriminaliteit. Enerzijds wil de publieke sector sterk inzetten op het aanpakken van dit verschijnsel. Het ministerie van Veiligheid en Justitie wil een totaalaanpak op centraal niveau bieden. Daarnaast zijn ook de (personele en financiële) middelen van de politie voortdurend verhoogd. Anderzijds lijkt de samenwerking met de particuliere sector doeltreffend en veelbelovend.

4. NATIONALE STRUCTUREN

4.1. Rechterlijke macht (OM en rechters)

4.1.1 Interne structuur

Cybercrime wordt opgespoord, vervolgd en berecht binnen hetzelfde juridische kader als "andere" misdrijven.

Het Openbaar Ministerie vormt samen met de Rechtspraak de rechterlijke macht. Het Openbaar Ministerie is de enige instantie die kan besluiten een persoon te vervolgen. Tijdens de rechtszitting eist de officier van justitie van het OM een straf. Daarna doet de rechter een uitspraak. Veroordeelden en officieren van justitie kunnen beroep instellen indien zij het niet eens zijn met het vonnis van een rechtbank, waarna het OM bij het gerechtshof de zaak verder vervolgt. Dat is zijn voornaamste taak. In beroepszaken, kan nieuw onderzoek worden uitgevoerd en kunnen nieuwe getuigen of deskundigen gehoord worden. Het gerechtshof doet dan een nieuwe uitspraak. In de meeste zaken kunnen de beslissingen van het gerechtshof worden aangevochten door cassatieberoep in te stellen bij de Hoge Raad van Nederland.

Officieren van Justitie

Het OM bepaalt wie voor de strafrechter moet verschijnen, en voor welk strafbaar feit. Het werkterrein van het OM is het strafrecht. De hoofdtaken van het OM zijn:

- de opsporing van strafbare feiten,
- de vervolging van strafbare feiten,
- toezicht houden op de uitvoering van strafvonnissen.

Er zijn in de rechterlijke macht tien arrondissementen die samenvallen met de door de regionale politie-eenheden bestreken geografische zone. Het OM heeft in elk arrondissement een vestiging, de parketten. Elk parket staat onder leiding van een hoofdofficier van justitie. Deze is ervoor verantwoordelijk dat het beleid van het OM in het arrondissement goed wordt uitgevoerd. Elk arrondissement heeft een gespecialiseerde cybercrime-officier en gespecialiseerde hulpofficieren van justitie. In totaal zijn er acht regionale cybercrime-officieren en tien regionale hulpofficieren van justitie, alsmede vier cybercrime-officieren en drie hulpofficieren van justitie op landelijk niveau.

Naast de regionale parketten zijn er het Landelijk Parket en het Functioneel Parket. Het Landelijk Parket houdt zich bezig met de aanpak van internationale vormen van georganiseerde misdaad en de coördinatie van de aanpak van zaken als terrorisme en mensensmokkel. Ook is het bevoegd voor high-tech (cyber-)criminaliteit. De Dienst Landelijke Recherche, die tot taak heeft dergelijke misdrijven op te sporen, en waaronder de Team High Tech Crime valt, werkt onder het gezag van het Landelijk Parket. Het Functioneel Parket is belast met de bestrijding van fraude en milieucriminaliteit en behandelt de complexe ontnemingszaken.

Het OM hanteert bij de toepassing van het strafrecht het opportuniteitsbeginsel, wat betekent dat het bepaalt of er een opsporing wordt uitgevoerd. Volgens de Nederlandse autoriteiten kan het OM op grond van dit beginsel prioriteiten stellen voor bepaalde vormen van criminaliteit of criminele verschijnselen. Wanneer er een verdachte is en indien er sprake is van slachtoffers, stelt de officier van justitie, indien hij besluit de zaak niet te vervolgen, deze laatsten daarvan in kennis. Artikel 12 van het Nederlandse Wetboek van Strafvordering regelt het recht van een belanghebbende om bij het gerechtshof klacht in te dienen wanneer een misdrijf niet wordt vervolgd. Het OM hanteert een integrale benadering bij criminaliteitsbestrijding, in samenwerking met de politie. De subversiebenadering combineert een fenomeengerichte aanpak, met een subjectgerichte aanpak (specifieke netwerken en criminelen) en een objectgerichte aanpak (hotspots en vrijplaatsen). In iedere regio zijn er integrale stuurgroepen om een gemeenschappelijk informatiebeeld te creëren en in gezamenlijk overleg uitgevoerde interventies in te stellen waarbij strafrechtelijke, fiscale, bestuurlijke en andere acties worden gecombineerd. Het in beslag nemen van crimineel verkregen vermogen maakt standaard deel uit van die aanpak.

Rechters

De rechtbank bestaat uit maximaal vijf sectoren. Die omvatten altijd de sectoren bestuur, civiel, straf en kanton. Familie- en jeugdzaken worden vaak in een aparte sector ondergebracht. De rechters van de sector strafrecht gaan over alle strafzaken die niet aan de kantonrechter worden voorgelegd. Die zaken kunnen door een alleensprekende rechter worden gehoord of door een meervoudige kamer van drie rechters. De meervoudige kamer behandelt de meer complexe zaken en alle zaken waarin de aanklager een gevangenisstraf van meer dan een jaar eist.

De gerechtshoven behandelen civiele en strafzaken waarin beroep is aangetekend tegen de uitspraak van de rechtbank. Een gerechtshof bekijkt de feiten in een zaak opnieuw en komt tot eigen conclusies.

Als hoogste rechter op het gebied van civiel recht, strafrecht en belastingrecht in Nederland, is de Hoge Raad belast met het behandelen van cassatieberoepen en met een aantal specifieke taken waarmee hij door de wet is belast.

4.1.2 Capaciteit en obstakels voor succesvol vervolgen

De Nederlandse autoriteiten meldden dat de bestaande wetgeving moet worden aangepast en dat zij onvoldoende handvatten biedt voor het ongedaan maken van dataversleuteling, het aanpakken van illegale handelingen op het internet en het bestrijden van onlinekinderporno.

Daarnaast blijkt wederzijdse rechtshulp volgens de Nederlandse autoriteiten vaak moeilijk en is het een probleem om tijdig rechtshulp te krijgen. Het duurt een tijd voordat een verzoek vertaald is en naar de aangezochte staat wordt verstuurd. In de digitale wereld is tijd van essentieel belang, daarom kunnen lange procedures een cruciale negatieve factor zijn.

Door recente ontwikkelingen op het gebied van cybercrime zijn complexe acties nodig, bijvoorbeeld voor het afweren van DDoS-aanvallen of malwareverspreiding, of wanneer criminelen betrokken zijn bij het platleggen van vitale delen van de samenleving door middel van botnets. Om een botnet onschadelijk te maken, is het noodzakelijk toegang te verkrijgen tot de servers die daar deel van uitmaken. Het optreden in cyberspace kan met zich meebrengen dat gegevens ontoegankelijk worden gemaakt, ook als deze zich op een server in het buitenland bevinden. Dit kan het geval zijn als de feitelijke locatie van de gegevens redelijkerwijs niet te achterhalen is, zoals bij gegevens in de Cloud.

Bij het aftappen van communicatie hebben politie en justitie steeds meer last van versleuteling van elektronische gegevens. Op internet worden speciale programma's aangeboden om gegevensbestanden te versleutelen. Informatiesystemen en programmatuur zijn vaak standaard ingesteld op versleutelde vormen van communicatie, bijvoorbeeld Gmail en Twitter. Internetgebruikers kunnen zelfs via bepaalde diensten gegevens anoniem transporteren. Dit speelt criminelen in de kaart. Weliswaar is de aanbieder verplicht mee te werken aan het ongedaan maken van versleutelde communicatie, maar daar is hij soms zelf niet toe in staat of de aanbieder is gevestigd in het buitenland.

Het wetsontwerp cybercriminaliteit voorziet in maatregelen die beter aangepast zijn aan het zich snel ontwikkelende gebied van technologie, internet en computercriminaliteit.

4.2 Rechtshandhavingsinstanties

Politie

Opsporingen worden geleid door een officier van justitie. Hij vertegenwoordigt het OM, waarbij de eindverantwoordelijkheid voor opsporingen ligt. Het opsporingswerk wordt echter door politierechercheurs verricht. Politiemensen zoeken naar sporen, horen getuigen en slachtoffers, houden verdachten tegen en leggen alles schriftelijk vast in een proces-verbaal. Veel politiebureaus of basiseenheden hebben hun eigen rechercheafdeling. Overeenkomstig het zogeheten "Inrichtingsplan politie" bestaat een regionale politie-eenheid uit:

- verschillende districten, die elk bestaan uit
- verschillende basisteams en een districtsrecherche
- een Dienst Regionale Recherche, en
- een flexteam van onderzoekers ter ondersteuning van de district- en basisteams ingeval van een piek in het aantal incidenten of plots opduikende tendensen.

Nederland heeft een vergaande hervorming van de landelijke politie doorgevoerd en de 25 regionale politiekorpsen gefuseerd tot een landelijk korps. De landelijke eenheid van de politie bestaat uit:

- Dienst Landelijke Recherche, die onder andere bestaat uit:
    - het Team High Tech Crime (HTC);
    - het Team Kinderporno
- andere centrale afdelingen, zoals de Dienst Landelijk Operationeel Centrum en de Dienst Landelijke Informatieorganisatie.

Dat proces heeft tal van organisatorische maatregelen noodzakelijk gemaakt, waaronder aanpassingen van de coördinatiemechanismen tussen alle belanghebbenden op regionaal (burgemeesters, aanklagers en de politie) en landelijk niveau (het ministerie van Veiligheid en Justitie).

Met de komst van cyberspace, behoort de bestrijding van cybercrime, zoals internetoplichting, nu ook tot het takenpakket van de lokale eenheden. Deze eenheden bestaan uit politiemensen zonder specialistische kennis van cybercriminaliteit. De politie zal eenheden van cyberexperts opzetten die ondersteuning zullen bieden op lokaal niveau. Op landelijk niveau heeft Nederland de Dienst Nationale Recherche voor de bestrijding van zware, georganiseerde en internationale criminaliteit en terrorisme.

Team High Tech Crime (THTC) en digitale ondersteuning

Op landelijk niveau heeft de politie een speciaal Team High Tech Crime opgezet als onderdeel van de Landelijke Eenheid. Het Team is belast met het opsporen van geavanceerde cybercriminaliteit. De landelijke ondersteunende dienst telt cyberexperts ter ondersteuning van de opsporing van minder geavanceerde cybercrime, en ter ondersteuning van het verzamelen van digitaal bewijs. De regionale politie-eenheden zullen eenheden van cyberexperts opzetten die hetzelfde soort steun zullen bieden op lokaal niveau.

Fiscale inlichtingen- en opsporingsdienst, FIOD

De FIOD is onderdeel van de Belastingdienst van het ministerie van Financiën en houdt zich bezig met het opsporen van fiscale, economische en financiële fraude. De FIOD draagt bij aan de bestrijding van georganiseerde criminaliteit en terrorisme, bijvoorbeeld door het opsporen van fraude en het in kaart brengen van de geldstromen van criminele en terroristische organisaties. De FIOD kan, in overleg met het OM, besluiten een strafrechtelijk onderzoek te starten.

De Koninklijke Nederlandse Marechaussee

De Koninklijke Nederlandse Marechaussee (KMar) is een gendarmeriekorps, d.w.z. een dienst bestaande uit militair personeel met volwaardige politiebevoegdheden. Afgezien van haar functie als militaire politie, vervult de Kmar civiele politietaken aan de grenzen, hoofdzakelijk op lucht- en in zeehavens. Tot de misdrijven waarmee zij te maken krijgen behoren mensenhandel en seksueel misbruik van kinderen, beide mogelijke gebieden van cybercriminaliteit.

4.3 Andere instanties/instellingen/publiek-private partnerschappen

Samenwerking tussen overheidsinstellingen (hoofdzakelijk rechtshandhavende) bij de bestrijding van cybercriminaliteit vindt plaats in de vorm van publiek-private informatie-uitwisseling. De Electronic Crimes Task Force (ECTF) en het Nationale Cyber Security Centrum (NCSC) zijn markante voorbeelden van publiek-private partnerschappen op het gebied van cybersecurity.

De Electronic Crimes Task Force is een gezamenlijke werkgroep waaraan wordt deelgenomen door het OM, de Landelijke Politie, de grote Nederlandse banken en de Nederlandse Vereniging van Banken. De hoofdtaken van de ECTF zijn het uitwisselen van informatie over specifieke zaken, het op het spoor komen van nieuwe criminele methoden en het bespreken van mogelijke acties om ze tegen te gaan. Nieuwe betaalmethodes, technologieën en mogelijke kwetsbaarheden zijn onderwerpen van bespreking in de ECTF. De ECTF stelt ook criminele dreigingsbeelden op en kan snel inlichtingen verstrekken in strafrechtelijke onderzoeken door concrete actieplannen voor te stellen. Er is een specifieke focus op financiële malware, phishingaanvallen en andere tegen de financiële sector gerichte cybercrimegerelateerde incidenten. De ECTF was betrokken bij 15 opsporingsonderzoeken naar digitale bankfraude. Sinds de ECTF in 2011 met haar werkzaamheden begon, zijn meer dan 100 verdachten aangehouden, onder meer ronselaars, katvangers en corrupte medewerkers van bedrijven. Volgens de Nederlandse Vereniging van Banken bedroeg de schade door bankfraude in 2010 9,8 miljoen EUR, terwijl dat in 2009 nog 1,9 miljoen EUR was.

Het Nationaal Cyber Security Centrum (NCSC) is een ander voorbeeld van publiek-private partnerschappen die een geïntegreerde aanpak van cybersecurity in het algemeen tot stand brengt. Het is operationeel sedert 1 januari 2012. De doelstellingen ervan zijn:

- de Nederlandse samenleving weerbaarder te helpen maken op cybergebied,
- te helpen een veiliger, opener en stabielere informatiemaatschappij te creëren.

Het NCSC richt zich hoofdzakelijk op de zogeheten vitale sectoren van het land. Enkele van zijn belangrijkste partners uit de private sector zijn daarom energiebedrijven, en de telecommunicatie- en de financiële sector. Deelnemers van overheidszijde zijn onder meer de ministeries van Veiligheid en Justitie, Economische Zaken, Landbouw en Innovatie, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken en Defensie. Daarnaast leveren het OM, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Landelijke Politie bijdragen aan het Centrum. Op het gebied van financiële misdaad is het publiek-private partnerschap van het Financial Information Sharing and Analysis Centre (FI-ISAC) vermeldenswaard.

Het NCSC lijkt goed uitgerust en goed opgeleid te zijn. Zijn taakstelling omvat echter alleen overheids- en vitale infrastructuur. Daarom moet er naar de mening van de evalueerders een mechanisme worden ontwikkeld om bijstand aan civiele slachtoffers van cybercrime te faciliteren.

Bovengenoemd partnerschap (FI-ISAC) is een samenwerking tussen de politie, het Openbaar Ministerie en de online marktplaats www.marktplaats.nl. Het is een voorziening voor internetklanten om na te gaan of een internetaanbieder als onbetrouwbaar te boek staat, en om onlinehandelsfraude aan de politie te melden. De financiële instellingen en overheidsinstanties delen informatie over cyberaanvallen.

4.4. Samenwerking en coördinatie op landelijk niveau

De minister van Veiligheid en Justitie speelt een essentiële rol bij de samenwerking en coördinatie over cybersecurity en het aanpakken van cybercrime op landelijk niveau. De ministeries van Economische Zaken (telecommunicatie en handel), Binnenlandse Zaken (handhaven van de grondwet en de nationale veiligheid), Defensie (cyberoorlogvoering) en Buitenlandse Zaken (cyberkwesties in het internationaal recht) ontwikkelen het cyberbeleid en voeren het uit, elk binnen hun eigen bevoegdheidsgebied. De minister van Veiligheid en Justitie is belast met de coördinatie van vraagstukken in verband met cybercrime, en voor het beleid ter bestrijding van cybercrime binnen de regering.

De samenwerking met de particuliere sector is vergevorderd in Nederland. De Cyber Security Raad, ingesteld in juni 2011, is nog een voorbeeld (naast die vermeld in punt 4.3). De Raad bestaat uit hooggeplaatste vertegenwoordigers van regeringsinstanties en ondernemingen. Het OM en de politie zijn ook vertegenwoordigd in de Raad.

In de NCSS2 worden verschillende acties genoemd om de samenwerking met het bedrijfsleven te intensiveren, zoals het verbeteren of ontwikkelen van normen in internationaal verband om de veiligheid en privacy van ICT-producten en -diensten te bevorderen.

4.4.1 Wettelijke of beleidsverplichtingen

Het Nederlandse recht legt de particuliere sector de volgende verplichtingen op wat betreft het melden aan overheidsinstellingen van verdachte incidenten:

1. Telecommunicatiewet - persoonsgegevens: de meldplicht geldt voor inbreuken op de technologische of organisatorische beveiliging van aanbieders van openbare elektronische communicatiediensten wanneer de inbreuk negatieve effecten heeft op de bescherming van persoonsgegevens. De melding moet worden gedaan aan de onafhankelijke Autoriteit Consument & Markt (ACM). Melding is niet vereist indien de aanvaller geen toegang krijgt tot de gegevens, bijvoorbeeld omdat ze versleuteld zijn.

2. Telecommunicatiewet - onderbreking van de continuïteit van dienstverlening: aanbieders van openbare elektronische communicatienetwerken en publiek beschikbare elektronische communicatiediensten moeten het Agentschap Telecom onmiddellijk op de hoogte brengen bij een inbreuk op de beveiliging of verlies van integriteit die de continuïteit van het netwerk of de dienst heeft onderbroken.
3. Wet op het financieel toezicht - integere bedrijfsvoering: op basis van de Wet financiële markten is een aantal financiële instellingen gehouden, de ACM of De Nederlandsche Bank (DNB) op de hoogte brengen van incidenten die de goede werking van hun instelling verstoren.

Er staat echter geen sanctie op het niet melden aan het NCSC.

Naar de mening van de evalueerders biedt verplichte melding op zich geen toegevoegde waarde en moeten de risico's die verbonden zijn aan het verlies van vertrouwen in dienstenaanbieders in aanmerking genomen worden bij de beoordeling van dit thema. Toch moet er rekening mee worden gehouden dat door het ontbreken van verplichte melding bij grootscheepse aanvallen tegen vitale infrastructuur die door private bedrijven wordt geëxploiteerd, de particuliere sector zich bij het besluit om criminelen al dan niet te bestrijden en voor de rechter te brengen, kan laten leiden door de eigen belangen en niet die van de bevolking. Tijdens het bezoek ter plaatse werd gezegd dat particuliere bedrijven om diverse redenen niet erg geneigd waren informatie door te geven.

Toch lieten de Nederlandse autoriteiten weten dat er momenteel wordt gewerkt aan een nieuwe meldplicht voor de particuliere sector.

4.4.2 Middelen die zijn toegewezen om de samenwerking te verbeteren

Het personeel van het NCSC (bij het ministerie van Veiligheid en Justitie) coördineert cybersecuritygerelateerde vraagstukken in het algemeen bij de betrokken ministeries. De dienst Rechtshandhaving van het ministerie van Veiligheid en Justitie is belast met het strafrechtbeleid en het beleid inzake bestrijding van criminaliteit, inclusief cybercriminaliteit. De dagelijkse coördinatie en de contacten worden beheerd op personeelsniveau.

Het Team High Tech Crime van de politie zal in 2015 zijn uitgebreid tot 119 voltijdse personeelsleden en over up-to-date apparatuur beschikken. De Nederlandse overheid is voornemens de politie in elke eenheid toe te rusten met een eenheid digitale ondersteuning om de rechercheteams te ondersteunen. Door die investeringen zouden de capaciteit en de kennis van de regionale politie-eenheden moeten verbeteren, zou het Team High Tech Crime zich meer moeten kunnen toeleggen op nieuwe en technologisch complexe misdaad, en zou het team in staat moeten zijn actief nieuwe kennis te delen met andere politie-eenheden.

Bij het bezoek aan de gebouwen van het digitale centrum van de Rotterdamse politie kreeg het evaluatieteam te horen dat de regionale politie-eenheden niet zo goed uitgerust zijn als de landelijke. Hoewel het bezoek veelbelovend was, is er volgens de evalueerders wat betreft expertise en operationele middelen om cybercriminaliteit te bestrijden een kloof tussen de nationale en regionale overheden (zowel bij politie als bij de vervolgende instanties).

4.5 Conclusies

- Nederland kent een zeer coherente territoriale verdeling wat betreft rechtshandhavende instanties, OM en gerechten, die geldt voor alle autoriteiten die aan criminaliteitsbestrijding doen. Daarnaast is er een zeer consequente toewijzing van bevoegdheden tussen de centrale en de regionale eenheden, zowel bij het OM als bij de politie, die tot goede samenwerking leidt. Naar de mening van het evaluatieteam stelt deze nauwe samenwerking op operationeel en strategisch niveau hen in staat cybercrime effectiever te bestrijden.

- Het OM heeft een aparte afdeling voor cybercrime, bestaande uit gespecialiseerde cybercrimeambtenaren en hulpofficieren van justitie, en een netwerk van officieren van justitie die deze zaken behandelen. Volgens de evalueerders is dit een nuttige methode om informatie en ervaring te delen.

- De ervaring bij de politie lijkt erg goed te zijn, ook al is men nog bezig met het opzetten van digitale centra. Daarom zou het bestaan van in cybercrime gespecialiseerde regionale officieren van justitie aanleiding kunnen geven tot het creëren van soortgelijke structuren bij de politie, omdat officieren van justitie en de politie wat juridische en operationele aspecten betreft nauw met elkaar in verbinding staan.

- Voorts zijn er geen rechters aangesteld die zich met cybercrime moeten bezighouden. Daarom vergt het verhogen van het bewustzijn bij rechters omtrent dit soort misdrijven naar de mening van de evalueerders regelmatige opleiding.

- Het ministerie van Veiligheid en Justitie speelt een belangrijke rol bij het coördineren van het overheidsoptreden tegen cybercriminaliteit, naast andere ministeries (Economische Zaken, Binnenlandse Zaken en Defensie) en de bijeenkomsten van de voorzitters op verschillende niveaus. Ook de Cyber Security Raad vervult een belangrijke rol op dat gebied, zowel als borger van een tijdige en gecoördineerde respons en als verstrekker van politieke en strategische sturing van de lagere coördinatielagen.

- Volgens de evalueerders, zijn publiek-private partnerschappen een zeer interessant initiatief dat het mogelijk maakt informatie informeel te verwerken, en vermoedelijke misdaden en verdachten op het spoor te komen met gebruikmaking van databanken van financiële instellingen en recherche. Deze methode van samenwerking lijkt te prevaleren boven de meer traditionele methode van officiële uitwisseling van documentatie op verzoek van de rechtshandhavende instanties. De traditionele methoden van misdaadopsporing worden gebruikt zodra de rechtshandhavende instanties ervan overtuigd zijn dat er een redelijk vermoeden van een misdaad bestaat en er een misdaad is begaan.

- De publiek-private partnerschappen die in Nederland zijn gevormd lijken een zeer positieve stap te zijn bij het voorkomen van cyberaanvallen op vitale infrastructuur en financiële diensten, en te zorgen voor schadebeperking bij dergelijke aanvallen (de ECTF en de NCSC). Volgens de evalueerders, wordt door de samenwerking tussen de publieke en de particuliere sector unieke en specifieke kennis, informatie en expertise bijeengebracht, waarbij de analyse- en interventievermogens in het kader van cybercriminaliteit fors worden verbeterd.

- Het bestaan van betrouwbare publiek-private partnerschappen is een extra troef bij het voorkomen van cybercriminaliteit en het handhaven van de wetgeving daarover. Volgens het evaluatieteam zijn deze partnerschappen echter ook sterk gericht op de bescherming van de financiële markten en de vitale infrastructuur van het land, en is er minder aandacht voor de bescherming van de belangen van secundaire slachtoffers, zoals de klanten van de belangrijkste slachtoffers en de gebruikers van de getroffen diensten, met name wanneer het melden van een cyberaanval schadelijk kan zijn voor het imago van de betrokken ondernemingen.

- Het Nederlandse recht kent verplichtingen om verdachte incidenten te melden aan overheidsinstanties. Die verplichtingen staan omschreven in de Telecommunicatiewet (bij inbreuk op de technologische of organisatorische beveiliging van aanbieders van openbare elektronische communicatiediensten wanneer die inbreuk negatieve effecten heeft op de bescherming van persoonsgegevens en een onderbreking van de continuïteit van de dienstverlening met zich meebrengt) en de Wet op het financieel toezicht (voor incidenten die een gevaar vormen voor de integere bedrijfsvoering van financiële instellingen). Toch is er geen verplichting om justitie of de politie op de hoogte te brengen van incidenten van criminele aard, inclusief cybercrime, die geen verband houden met het functioneren van de publieke of financiële instellingen.

- Het evaluatieteam kreeg te horen dat in 2015 een nieuwe wet moet worden aangenomen die de verplichting zal bevatten inbreuken te melden aan de NCSC. Er staan echter geen sancties op het niet-melden, al zullen de bevoegde autoriteiten (toezichthouder gegevensbescherming, toezichthouder banken, enz.) er wel rekening mee houden of een bedrijf een inbreuk gemeld heeft of niet). Vertegenwoordigers van het NCSC bevestigen dat er een algemene terughoudendheid is bij de organisaties uit de particuliere sector. Daarom zijn de evalueerders van mening dat moet worden overwogen een meer bindend juridisch raamwerk tot stand te brengen wat betreft de melding van cyberaanvallen door bedrijven.

- Naar de mening van het evaluatieteam, kan het in dienst nemen van IT-specialisten en het bieden van concurrerende arbeidsvoorwaarden helpen om capaciteit voor doeltreffende cybercrimebestrijding op te bouwen.

5. JURIDISCHE ASPECTEN

5.1. Materieel strafrecht in verband met cybercrime

Het Nederlandse recht kent geen wettelijke definitie van cybercrime.

5.1.1 Verdrag van de Raad van Europa over Cybercriminaliteit

Nederland heeft het Verdrag over Cybercriminaliteit in 2001 ondertekend en in 2006 geratificeerd.

5.1.2 Beschrijving van de nationale wetgeving

A. Kaderbesluit 2005/222/JBZ van de Raad over aanvallen op informatiesystemen en Richtlijn 2013/40/EG over aanvallen op informatiesystemen

Het Nederlandse recht kent uitvoerige bepalingen over cybercrime[8]. Kaderbesluit 2005/222/JBZ van de Raad over aanvallen op informatiesystemen is in het Nederlandse recht omgezet.

Nederland werkt momenteel aan een wet te volledige tenuitvoerlegging van Richtlijn 2013/40/EG over aanvallen tegen informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad. De Nederlandse autoriteiten lieten weten dat het Nederlandse recht reeds grotendeels in overeenstemming is met de Richtlijn, de strafbare feiten bijvoorbeeld zijn reeds neergelegd in het Nederlandse Wetboek van Strafrecht via eerdere herzieningen van het Nederlandse recht in 1993 en 2006.

De nieuwe wetgeving zal primair de straffen voor bepaalde strafbare feiten verhogen. Meer bepaald zullen de minimumstraffen worden verhoogd. Op bepaalde strafbare feiten zal een maximumstraf van twee jaar komen te staan. Bovendien zullen er drie verzwarende omstandigheden worden toegevoegd. De straf zal worden verhoogd tot maximaal drie jaar indien een botnet is gebruikt bij het begaan van het strafbaar feit, en vijf jaar indien het strafbare feit ernstige schade heeft aangericht of het gericht was tegen vitale infrastructuur.

[8] In het rapport is vanwege de lengte geen gedetailleerde beschrijving opgenomen. Voor meer informatie zie de bijlagen bij de Nederlandse antwoorden op de vragenlijst.

Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie

In 2014 heeft het Nederlandse parlement het wetsontwerp aangenomen ter tenuitvoerlegging van Richtlijn 2011/93/EU van het Europees Parlement en de Raad ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 101 van 15 april 2011) (hierna "de Richtlijn"). Aangezien Nederland reeds juridisch gebonden is aan het Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (ETS nr. 201), zijn de gevolgen op wetgevingsgebied van de Richtlijn voor het Nederlandse recht relatief gering. Volgens de Nederlandse autoriteiten is de Nederlandse wetgeving over seksueel misbruik van kinderen en kinderpornografie in vergelijking met het Verdrag van de Raad van Europa en de Richtlijn "bij de tijd".

C. Onlinekaartfraude

De samenwerking met banken is in Nederland niet direct gebaseerd op wettelijke bepalingen maar op private afspraken. De rechtshandhavingsinstanties en de financiële sector werken bijvoorbeeld samen in de Electronic Crimes Task Force (ECTF) en delen informatie over specifieke zaken, brengen nieuwe criminele methodes in beeld en bespreken mogelijke acties om die tegen te gaan.

Om het skimmingprobleem aan te pakken, hebben de rechtshandhavingsinstanties en de financiële sector samengewerkt in het Landelijk Skimming Point. De samenwerking heeft geleid tot het gebruik van nieuwe betalingsvoorzieningen zonder magnetische strook, en met het routinematig blokkeren van debit- en creditcards buiten Europa. Skimming is daardoor aanzienlijk teruggedrongen.

Binnen het verband van het Financial Information Sharing and Analysis Centre (FI-ISAC), delen financiële instellingen en overheidsinstanties informatie over cyberaanvallen. Het NCSC is verbonden met en steunt het FI-ISAC.

Door deze samenwerking is het totale bedrag aan schade door onlinebankfraude gedaald van 34,8 miljoen EUR in 2012 tot 9,6 miljoen EUR in 2013. Het totale bedrag aan schade door skimmen liep terug tot 6,8 miljoen EUR in 2013.

5.2. Procedurekwesties

5.2.1 Recherchetechnieken

In algemene zin zijn het strafrechtelijk onderzoek en de strafvervolging geregeld in het Wetboek van Strafvordering. Opsporingsbevoegdheden kunnen worden gebruikt naar gelang van de ingrijpendheid van de betrokken bevoegdheden en de ernst van het onderzochte strafbare feit. Misdrijven die voorhechtenis mogelijk maken, wat meestal het geval is voor strafbare feiten waarop maximaal tenminste vier jaar gevangenisstraf staat (artikel 67, lid 1, onder a) Sv), en bepaalde met name genoemde strafbare feiten (artikel 1, lid 1, onder b) Sv) kunnen nopen tot het gebruik van bijzondere opsporingsbevoegdheden. Omdat digitale opsporingsbevoegdheden ook vereist kunnen zijn voor "eenvoudige" cybermisdrijven, bijvoorbeeld hacken zonder verzwarende omstandigheden, zijn bij de Wet computercriminaliteit II vrijwel alle cybermisdrijven specifiek in artikel 67, lid 1, onder b) Sv ingevoegd. Bijgevolg is voor de meeste cybermisdrijven voorlopige hechtenis toegestaan, ongeacht de maximumstraf, en kunnen de meeste opsporingsbevoegdheden worden gebruikt om ze te onderzoeken.

Het Sv omschrijft de volgende opsporingsbevoegdheden voor de politie met betrekking tot cybercrime: doorzoeken van een plaats ter vastlegging van gegevens die op een gegevensdrager zijn opgeslagen (artikel 125i); verkrijgen van gegevens in andere geautomatiseerde werken op de plaats waar de doorzoeking plaatsvindt, voor zover de perso(o)n(en) die op die plaats verblijven,

rechtmatige toegang tot die andere geautomatiseerde werken hebben (artikel 125j); het ontoegankelijk maken van gegevens ter beëindiging of voorkoming van een strafbaar feit (artikel 125o);met een technisch hulpmiddel niet voor het publiek bestemde communicatie verkrijgen (artikel 126m); een aanbieder van een communicatiedienst bevelen gegevens te verstrekken over de gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker (artikel 126n); een aanbieder van een communicatiedienst bevelen persoonlijke gegevens van een gebruiker van een communicatiedienst te verstrekken (artikel 126na); de gebruiker van een communicatiedienst te identificeren met technische middelen (artikel 126nb); een persoon die de betreffende data in zijn bezit heeft bevelen identificerende gegevens over een verdachte te verstrekken (artikel 126nc); een persoon die toegang heeft tot de betrokken gegevens bevelen ze te verstrekken (artikel 126nd - artikel 125ng); een persoon (niet zijnde een verdachte) bevelen zijn medewerking te verlenen aan de ontsleuteling van gegevens (artikel 126nh); een persoon (niet zijnde een verdachte) bevelen de betrokken gegevens te bewaren gedurende een periode van ten hoogste 90 dagen (artikel 126ni).

• *Doorzoeken en in beslag nemen van gegevens uit informatiesystemen/computers*

Het Sv bevat geen specifieke bepalingen over het doorzoeken en in beslag nemen van gegevens uit computers. De algemene bepalingen inzake inbeslagname kunnen worden toegepast bij het in beslag nemen van apparatuur voor gegevensopslag. Gegevens als zodanig kunnen niet in beslag worden genomen, omdat ze niet als "zaken" worden beschouwd, maar ze kunnen worden gekopieerd door de rechtshandhavers tijdens een doorzoeking (te vergelijken met bijvoorbeeld het nemen van foto's van de plaats delict of het nemen van vingerafdrukken). Voorts is bij de Wet bevoegdheden vorderen gegevens van 1996 in artikel 125i Sv de bevoegdheid ingevoegd om te doorzoeken met het oog op de vastlegging van gegevens. In het belang van de openbare orde of de bescherming van slachtoffers (bv. kinderen jonger dan 18 die slachtoffer zijn van seksueel misbruik waarvan beelden zijn genomen en verspreid), volstaat louter kopiëren van de gegevens wellicht niet. In die gevallen staat artikel 125o Sv de officier van justitie toe een aanbieder van internetdiensten te bevelen de gegevens ontoegankelijk te maken. Artikel 125j Sv bevat de bevoegdheid om een netwerk te doorzoeken indien tijdens een doorzoeking is gebleken dat de betrokken gegevens elders op een netwerk lijken te zijn opgeslagen. Artikel 125j Sv stelt degene die een doorzoeking doet in staat ook computernetwerken te doorzoeken vanaf computers die zich op de doorzochte plaats bevinden. Doorzoeking van het netwerk vindt alleen plaats voor zover het netwerk rechtmatig toegankelijk is voor de personen die regelmatig op die plaats aanwezig zijn. Volgens de huidige uitlegging kan doorzoeking van een netwerk alleen binnen het Nederlandse rechtsgebied plaatsvinden.

Omdat er versleutelingstechnologie gebruikt kan zijn, is het mogelijk dat de politie moeilijk toegang verkrijgt tot de gegevens. Artikel 125k Sv stelt de opsporingsambtenaar in staat een beveiligingsmaatregel ongedaan te maken en de ontsleuteling of het overhandigen van een decryptiesleutel voor de versleutelde gegevens te bevelen. Het bevel mag niet gericht zijn tot verdachten.

Als algemene garanties in de procedures voor het doorzoeken van computers en gegevens, bestaat de verplichting de gegevens te vernietigen zodra zij van geen betekenis meer zijn voor het onderzoek - tenzij zij zullen worden gebruikt voor een andere zaak of zijn opgeslagen in het register zware criminaliteit (artikel 125n Sv) - en om de betrokkenen mee te delen dat er data zijn gekopieerd of ontoegankelijk gemaakt. De personen aan wie mededeling moet worden gedaan zijn verdachten (tenzij zij automatisch worden geïnformeerd via het strafdossier), de verantwoordelijke voor de gegevens, en de rechthebbenden van de plaats waar de doorzoeking heeft plaatsgevonden, behalve in gevallen waarin mededeling redelijkerwijs niet mogelijk is (artikel 125m Sv).

• *Onderscheppen/verzamelen van verkeers-/contentgegevens in real-time*

De officier van justitie kan op grond van artikel 126m Sv na machtiging van een rechter bevelen dat communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen. Onderschepping is toegestaan in zaken waarbij voorlopige hechtenis mogelijk is en er ernstige inbreuk is gemaakt op de rechtsorde. Indien blijkt dat de onderschepte communicatie versleuteld is, kan een bevel worden gericht tot degene van wie kan worden vermoed dat hij kennis draagt van ontsleutelingsmiddelen, maar niet tot de verdachte.

Communicatie kan worden onderschept indien het belang van het onderzoek dit vordert. De communicatie van personen die een wettelijk verschoningsrecht hebben (advocaten, notarissen, geestelijken, artsen) mag niet worden onderschept, tenzij zij zelf verdachten zijn; indien bij een reguliere telefoontap een gesprek met die persoon in zijn beroepsuitoefening wordt opgenomen, moet het worden gewist.

Onderschepping vanuit Nederland van de communicatie van iemand die in het buitenland gevestigd is, is mogelijk nadat de andere staat daarvoor toestemming heeft verleend. Ook kan om interceptie en directe doorgifte vanuit een andere staat naar Nederland worden verzocht; omgekeerd kan Nederland interceptie en directe doorgifte vanuit Nederland naar een andere staat toestaan.

Artikel 126l Sv staat de officier van justitie toe, na machtiging van de rechter-commissaris, te bevelen dat een opsporingsambtenaar vertrouwelijke communicatie opneemt met een technisch hulpmiddel, in zaken waarbij preventieve hechtenis mogelijk is en een ernstige inbreuk op de rechtsorde is gemaakt. Voorbeelden van dat soort technische apparatuur zijn richtmicrofoons, bugs en keyloggers. Indien nodig omvat die bevoegdheid het binnengaan van plaatsen om er apparatuur te installeren. Indien de plaats een private woning omvat, kan dit alleen plaatsvinden indien op het misdrijf een maximumstraf van ten minste acht jaar gevangenisstraf staat en de rechter de maatregel uitdrukkelijk heeft toegestaan.

Artikel 13, eerste lid, van de Telecommunicatiewet eist dat aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar stellen aan gebruikers indien deze aftapbaar zijn. Dit geldt voor internetaanbieders, maar niet voor hostingproviders.

• *Bewaren van computergegevens*

Artikel 126ni Sv staat de officier van justitie toe, in zaken waarbij voorlopige hechtenis mogelijk is en een ernstige inbreuk op de rechtsorde is gemaakt, iemand te bevelen gegevens te bewaren die zijn opgeslagen op een computer en in het bijzonder vatbaar zijn voor verlies of wijziging. Er kan worden gevorderd dat deze gegevens voor een periode van ten hoogste 90 dagen worden bewaard (deze termijn kan een keer worden verlengd).

• *Bevel tot overlegging van opgeslagen verkeers-/contentgegevens*

Het Sv voorziet in de bevoegdheden om het overleggen van gegevens te bevelen. In verband met die bevoegdheden wordt een onderscheid gemaakt tussen het identificeren van gegevens, "andere" gegevens en gevoelige gegevens. Het bevel kan worden gegeven aan personen die gegevens verwerken in een professionele hoedanigheid; een bevel voor opgeslagen gegevens en gevoelige gegevens kan evenwel ook gericht worden tot personen die gegevens verwerken voor persoonlijk gebruik. Volgens artikel 126nc Sv kan een opsporingsambtenaar in geval van een misdrijf (niet een overtreding) vorderen identificerende gegevens zoals naam, adres, postcode, geboortedatum, geslacht en administratieve nummers te verstrekken.

Krachtens artikel 126nd Sv kan de officier van justitie vorderen dat er andere gegevens worden verstrekt in zaken waarbij voorlopige hechtenis is toegestaan, onder meer toekomstige gegevens en, in dringende gevallen en met machtiging van de rechter-commissaris, de verstrekking in real-time van toekomstige gegevens gedurende een periode van vier weken, die kan worden verlengd (126ne Sv).

Krachtens artikel 126nf Sv kan de rechter-commissaris vorderen dat gevoelige gegevens zoals religieuze gezindte, ras, politieke overtuiging of seksuele gerichtheid, gezondheid of vakbondslidmaatschap, worden verstrekt in zaken waarbij het gaat om een misdrijf waarbij voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op rechtsorde vormt. Het verstrekken van gegevens die zijn opgeslagen bij een aanbieder van openbare telecommunicatie kan alleen worden gevorderd na machtiging van een rechter (artikel 126ng, lid 2, Sv).

• *Bevel tot overlegging van gebruikersinformatie*

Om gebruikersgegevens te verkrijgen, kan een opsporingsambtenaar op grond van artikel 126na Sv bij een misdrijf van een aanbieder van communicatiediensten vorderen dat hij gebruikersgegevens verstrekt. Gebruikersgegevens omvatten naam, adres, telecommunicatienummers en bepaalde soorten diensten. Artikel 126n Sv betreffende verkeersgegevens (zie hierboven), strekt zich ook uit tot het verzamelen van gebruikersgegevens. Het verstrekken van andere informatie in verband met de identiteit van een persoon kan worden gevorderd conform artikel 126nc Sv.

Algemeen gesproken heeft de Landelijke Politie ervaren dat het gebruik van opsporingsbevoegdheden vaak het best functioneert in combinatie met meer traditionele bevoegdheden. Bijvoorbeeld bij het arresteren van een verdachte kan het van belang zijn het IP-adres te tappen en/of te voorkomen dat de verdachte de computer of smartphone vergrendelt waarop bewijs opgeslagen kan zijn.

5.2.2 Forensische technieken en versleuteling

Op grond van het Sv kan een digitaal forensisch onderzoek en/of forensisch onderzoek op afstand worden uitgevoerd bij een netwerkzoeking. Hetzelfde geldt voor technische apparatuur zoals keyloggers.

Vanwege de snelle ontwikkelingen op ICT-gebied moeten de opsporingsbevoegdheden worden aangepast. Dat zal politie en justitie in staat stellen adequaat op te treden tegen cybercriminaliteit. Een aanzienlijke hoeveelheid communicatie en informatie, en daarmee ook potentiële opsporingsinformatie, loopt over het internet en computers, en is dus standaard versleuteld. Voorbeelden zijn gesprekken via Skype of chats via WhatsApp. De Nederlandse autoriteiten onderstrepen dat politie en justitie die berichten kunnen aftappen met een klassieke internettap, maar ze vaak niet kunnen ontsleutelen.

Het Team High Tech Crime van de politie en de forensische deskundigen van de regionale eenheden kunnen digitaal bewijs veiligstellen. Het Nederlandse Forensisch Instituut heeft daartoe op landelijk niveau digitale forensische experts in dienst.

De politie werkt ook samen met andere overheidsinstanties en de particuliere sector in het NCSC.

De ervaring in Nederland leert dat versleutelde bestanden en berichten vaak (deels) ontoegankelijk blijven. De door criminelen gebruikte algoritmen, en de toepassing daarvan, zijn technologisch vaak solide. Daarom is samenwerking essentieel voor een succesvolle opsporing. De politie, met name het Team High Tech Crime, werkt samen met het Nederlandse Forensisch Instituut en Europol/EC3. Particuliere bedrijven zijn niet betrokken bij ontsleuteling in een strafrechtelijk onderzoek.

De Nederlandse autoriteiten lieten weten dat een nieuwe wet in de maak is om de politie in staat te stellen onder strikte voorwaarden op afstand een geautomatiseerd werk binnen te dringen. Dat zou mogelijkheden bieden voor het onderscheppen van gegevens voordat ze verstuurd (en versleuteld) worden of nadat ze zijn ontvangen (en ontsleuteld).

5.2.3e-Bewijs

Het Wetboek van Strafvordering regelt de bewijsvergaring in het algemeen. Artikel 350 Sv bepaalt dat de rechtbank (gewoonlijk een college van drie rechters in eerste aanleg) beraadslaagt over de vraag of bewezen is dat de ten laste gelegde strafbare feiten door de verdachte zijn begaan. De rechters moeten ervan overtuigd worden dat de verdachte schuldig is aan het misdrijf, aan de hand van de wettige bewijsmiddelen (artikel 338 Sv). De wettige bewijsmiddelen zijn de eigen waarnemingen van de rechter, verklaringen van de verdachte, van getuigen en van deskundigen, en schriftelijke bescheiden (artikel 339 Sv).

Tot schriftelijke bescheiden worden verschillende officiële documenten gerekend die op zich bewijskracht hebben en alle "andere geschriften" die alleen gelden in verband met de inhoud van andere bewijsmiddelen (artikel 344, lid 1, Sv). Een proces-verbaal van de opsporingsambtenaar heeft speciale bewijskracht; het kan het bewijs leveren dat de verdachte het telastegelegde feit heeft gepleegd (artikel 344, lid 2 Sv). De "andere geschriften" die worden genoemd in artikel 344, lid 1, Sv zijn los van een drager en kunnen elektronische documenten omvatten. Forensisch digitaal bewijs kan in een rechtszaak op verschillende manieren worden gebruikt: als door experts opgestelde officiële documenten, als deskundigenverklaringen in de rechtszaal, als officiële rapporten van opsporingsambtenaren die hun waarnemingen beschrijven, of als opmerkingen van de rechter wanneer het bewijs wordt getoond op een computer in de rechtszaal.

Elektronisch bewijs wordt verzameld en opgeslagen door de Landelijke Politie. Het Sv en de Wet politiegegevens regelen de vergaring, de bewaring en de vernietiging van elektronisch bewijs. Analyses van elektronisch bewijs worden aan de procespartijen verstrekt als onderdeel van het strafdossier.

Er zijn geen aanvullende regelingen voor elektronisch bewijs dat buiten het Nederlandse rechtsgebied is vergaard. Het wordt voor de rechter behandeld als ander bewijs, gebaseerd op volledige openbaarmaking. Als echter niet is voldaan aan in het Sv neergelegde opsporingsprocedures, kan de rechter het bewijs niet-ontvankelijk verklaren. Als het land dat het bewijs heeft helpen te verkrijgen, speciale voorwaarden stelt, houden de politie en de aanklager zich aan die voorwaarden. Toch kan dit het gebruik van dat bewijs in de rechtszaal belemmeren.

5.3 Bescherming van de mensenrechten/fundamentele vrijheden

De Nederlandse Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg) vormen het juridisch kader voor toegang tot persoonsgegevens en de vernietiging van gegevens wanneer ze niet langer van betekenis zijn voor een strafrechtelijk onderzoek. Het College Bescherming Persoonsgegevens (CBP) ziet toe op de naleving van besluiten die het gebruik van persoonsgegevens regelen. Het ziet toe op de naleving en de toepassing van de Wet bescherming persoonsgegevens, de Wet politiegegevens en de Wet gemeentelijke basisadministratie. Bij het College Bescherming Persoonsgegevens moet het gebruik van persoonsgegevens worden gemeld, tenzij er een uitzondering geldt. Het raamwerk voor het uitvoeren van deze taak is neergelegd in de Wet bescherming persoonsgegevens en daarmee verband houdende wetgeving.

In strafrechtelijke onderzoeken, wanneer het gebruik van bijzondere opsporingsbevoegdheden nodig is, zijn de rechtshandhavende instanties gebonden aan het proportionaliteits- en het subsidiariteitsbeginsel. Het OM moet ervoor zorgen dat de opsporingsbevoegdheden zodanig worden gebruikt dat de grondrechten zo min mogelijk worden geschonden. Daarnaast mag de inbreuk niet groter zijn dan strikt noodzakelijk voor het bewuste opsporingsonderzoek.

Voorts voorziet het wettelijk bestel van strafvordering in een hiërarchie van bevoegde instanties. Bij een zwaardere inbreuk op rechten is een bevel van de officier van justitie nodig; voor de zwaarste inbreuken heeft de aanklager de machtiging van een rechter nodig. Het gebruik van opsporingsbevoegdheden wordt beoordeeld door een rechter in de rechtszaal wanneer de verdachte wordt berecht. Inbreuken op universele rechten, zoals het recht op privacy, zijn alleen mogelijk indien zij worden toegestaan op grond van en conform internationale verdragen, zoals artikel 8, lid 2, van het Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden. De fundamentele rechten en vrijheden zijn gewaarborgd in de Nederlandse grondwet.

Er is geen hiërarchie van wetten in de grondwet: alle grondrechten zijn in beginsel evenwaardig en even belangrijk. Sommige rechten zijn absoluut, andere kunnen worden beperkt door een parlementaire of "formele" wet, en vele kunnen worden beperkt door delegatie van beperkende bevoegdheden. Zij omvatten:

- Vrijheid van meningsuiting (artikel 7 Nederlandse grondwet).
- Recht van privacy (artikel 7 Nederlandse grondwet), dat door een formele wet kan worden beperkt, zij het dat delegatie alleen toegestaan is ten aanzien van databanken. Dit artikel verplicht de overheid bescherming te bieden tegen een bedreiging van de persoonlijke levenssfeer door eventueel misbruik van databanken (lid 2), en een regeling te geven voor het recht van personen om geïnformeerd te worden over de inhoud van die databanken betreffende hun persoon en het recht om eventuele fouten in die inhoud te verbeteren (lid 3).
- De vertrouwelijkheid van communicatie (artikel 13 van de Nederlandse grondwet), dat het brief-, telefoon- en telegraafgeheim betreft. Delegatie is niet toegestaan. Voor de meeste zaken is de rechter-commissaris de bevoegde instantie.

5.4 Bevoegdheid

5.4.1 Principes die van toepassing zijn op het opsporen van cybercriminaliteit

Artikel 2 van het Wetboek van Strafrecht regelt de materiële bevoegdheid en stelt dat de strafwet toepasselijk is op ieder die in Nederland van enig strafbaar feit wordt verdacht. Artikel 4 van het Wetboek van Strafrecht geeft de rechtsgronden voor veel specifieke misdrijven die buiten Nederland worden begaan. Die omvatten vervalsing, ook vervalsing met behulp van computers, in het buitenland gepleegd door een Nederlandse ambtenaar en computersabotage of knoeien met data gericht tegen een Nederlander indien de daad verband houdt met terrorisme.

Artikel 5 van het Wetboek van Strafrecht regelt de bevoegdheid voor bepaalde misdrijven die buiten Nederland door Nederlanders worden begaan. Die omvatten het onthullen van bedrijfsgeheimen die zijn ontdekt door zich toegang te verschaffen tot een computer, en kinderporno. De bevoegdheid strekt zich ook uit tot kinderporno die wordt gemaakt door buitenlanders met een vaste verblijfplaats in Nederland, ook wanneer zij in Nederland zijn komen wonen nadat het misdrijf is gepleegd. Dit omvat ook bevoegdheid voor vrijwel alle soorten cybercriminaliteit die worden begaan door Nederlandse burgers in het buitenland. Het Nederlandse recht kent het actieve nationaliteitsbeginsel.

In cybercrimezaken kunnen interceptie en observatie over de landsgrenzen heen worden uitgevoerd. Het Schengenverdrag en het Verdrag aangaande de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie van 29 mei 2000 zijn van toepassing.

5.4.2 Regels bij jurisdictiegeschillen en verwijzing naar Eurojust

Nederland lost jurisdictiegeschillen op via overleg met de respectieve landen, en met Eurojust en Europol. Nederland heeft echter de regeling die is neergelegd in Kaderbesluit 2009/948/JBZ van de Raad van 30 november 2009 over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures, nog steeds niet ingevoerd. Niettemin neemt Nederland deel aan door Eurojust gecoördineerde gezamenlijke onderzoeken.

5.4.3 Bevoegdheid voor cybermisdrijven in de cloud

De Nederlandse autoriteiten benadrukten dat politie en justitie via internet toegang tot computers moet hebben om zware misdrijven in het digitale tijdperk op te sporen. Het in toenemende mate opslaan van gegevens in de cloud schept problemen voor politie en justitie. Ook al kan een aanbieder worden bevolen bepaalde gegevens te verstrekken, in de praktijk blijkt dit vaak erg moeilijk. Er zijn aanbieders die weigeren mee te werken met de politie ("rogue providers"). Soms wordt een aanbieder niet gevonden of is hij gevestigd in een land waarmee Nederland slechts zeer beperkte betrekkingen op het gebied van rechtshulp onderhoudt.

Voorts kunnen mensen het spoor van hun gegevensuitwisseling zo goed verbergen dat ze moeilijk te traceren zijn. Voor aanbieders van opslag in de cloud kan het moeilijk zijn de eigenlijke (territoriale) locatie van gegevens te achterhalen. Door de gebruikte technologie, en door de opslagcapaciteit in servers en de schaalvoordelen, worden gegevens wereldwijd heen en weer gezonden en kunnen zij in pakketjes worden opgedeeld die pas bij aankomst weer worden samengevoegd. Ook al koestert de politie de verdenking dat informatie zich niet in Nederland bevindt, het blijkt vaak onmogelijk om daar bevestiging van te krijgen en gegevens op een bepaalde territoriale locatie vast te pinnen. Bijgevolg is het voor rechtshandhavers moeilijk om, met name in de cloud, de locatie van informatie en de computers die ze verwerken te achterhalen en er toegang toe te krijgen.

De Nederlandse autoriteiten onderstreepten dat het tot dusver onmogelijk is gebleken een adequate oplossing voor dit probleem te vinden. Het internationale recht biedt de landen verschillende mogelijkheden om onafhankelijk of in onderlinge samenwerking (rechtshulp) op te treden, maar bij opsporingen in cyberspace is dat van beperkt nut gebleken. De Raad van Europa heeft daarover verdragen gesloten (onder meer met niet-lidstaten zoals de Verenigde Staten van Amerika, Canada, Australië en Japan). Overeenkomstig het Cybercrimeverdrag, is grensoverschrijdend optreden alleen mogelijk in een zeer beperkt aantal gevallen, bv. met de rechtmatige instemming van de persoon die

gerechtigd is om de gegevens te verstrekken, in een zaak waar bekend is waar de rechtsmacht ligt. In zaken waarbij de locatie van de gegevens onbekend is, zijn deze bepalingen niet adequaat. Dat leidt tot zaken waarin cybercrime onbestraft blijft, en situaties waarin mensen steeds opnieuw gedupeerd worden.

5.4.4 Zienswijze van Nederland over het wettelijk kader voor de bestrijding van cybercriminaliteit

Nederland acht het bestaande kader ontoereikend. Daarom werkt de minister van Veiligheid en Justitie aan een nieuwe wet over cybercriminaliteit. Nederland is het volledig eens met de bevindingen en aanbevelingen in het rapport van het Comité van het Cybercrimeverdrag over de grensoverschrijdende toegang tot gegevens[9]. In het rapport wordt besproken of het territorialiteitsbeginsel van toepassing is op het verkeer van gegevens in "cyberspace" en of het bijgevolg nodig is een aanvullend protocol bij het Verdrag van Boedapest aan te nemen.

In een aanvullend protocol zouden de volgende situaties tussen partijen kunnen worden geregeld:

- grensoverschrijdende toegang met instemming maar zonder de beperking van data die zijn opgeslagen "in een andere partij";
- grensoverschrijdende toegang zonder instemming maar met rechtmatig verkregen legitimatiebewijzen;
- grensoverschrijdende toegang zonder instemming, in goed vertrouwen of in dringende of andere omstandigheden;
- een doorzoeking van de originele computer uitbreiden tot verbonden systemen zonder de beperking "op zijn grondgebied";
- de bevoegdheid tot verwijdering als daarmee verbonden juridische factor.

9 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf

5.5 Conclusies

- Nederland heeft het Cybercrimeverdrag ondertekend en geratificeerd. De conceptwetgeving ter uitvoering van Richtlijn 2013/404EU over aanvallen tegen informatiesystemen wordt thans opgesteld. Niettemin lieten de Nederlandse autoriteiten weten dat het Nederlandse recht reeds grotendeels in overeenstemming is met deze Richtlijn.

- Richtlijn 2011/93/EU van het Europees Parlement en de Raad ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie is in 2014 ten uitvoer gelegd.

- Het bestrijden van creditcardfraude is meer gebaseerd op samenwerking met financiële instellingen dan op wetgevingsoplossingen.

- De bestaande wetgeving lijkt geen bindende en gemeenschappelijke delictsomschrijving van cybercriminaliteit te bevatten. Volgens de evalueerders kan dit ertoe leiden dat een beperkte of verschillende definitie van cybercriminaliteit voor statistische doeleinden gehanteerd wordt. Bijgevolg hebben de belanghebbenden bij de bestrijding van cybercriminaliteit niet per se dezelfde opvatting over of benadering van het concept.

- Met betrekking tot opsporingstechnieken is er een aantal maatregelen voor het in beslag nemen en bewaren van gegevens met het oog op bewijsvergaring (bv. iemand die toegang heeft tot de betrokken gegevens bevelen die gegevens te verstrekken, of iemand bevelen te helpen met de ontsleuteling van gegevens), maar ook om te voorkomen dat een criminele handeling gepleegd wordt (zoals het ontoegankelijk maken van gegevens om een einde te maken aan een activiteit). In Nederland hangt het gebruik van bijzondere opsporingsbevoegdheden doorgaans af van het feit of het misdrijf voorlopige hechtenis mogelijk maakt (voor misdrijven waar maximaal vier jaar gevangenis op staat). Opsporingsbevoegdheden kunnen ook, afhankelijk van het soort en de ernst van het misdrijf, worden gebruikt voor met name genoemde misdrijven (vrijwel alle cybermisdrijven vallen onder die categorie).

- Het ministerie van Veiligheid en Justitie werkt aan een nieuwe wet over cybercriminaliteit. Bij de hervorming van de wetgeving kan gedacht worden aan nieuwe opsporingsmaatregelen en -instrumenten, zoals het vermogen om een computer heimelijk of op afstand binnen te dringen (online), garanties en voorwaarden (bv. een bevel kan alleen worden gegeven bij dringende noodzaak in het belang van het onderzoek of de uitvoering kan worden voorbehouden aan daartoe aangewezen rechercheurs bij de politie), ontsleuteling door de verdachte, meer mogelijkheden voor het strafbaar stellen en het opsporen van het online groomen van kinderen, het strafbaar stellen van het helen van gestolen computergegevens, en van herhaalde fraude op onlinemarktplaatsen.

- De Nederlandse autoriteiten meldden dat zij het moeilijk hebben met het verlenen van volledige of gedeeltelijke toegang tot versleutelde bestanden en communicaties. Dat is met name problematisch wanneer e-bewijs zich in het buitenland bevindt. Daarom wijzen zij nadrukkelijk op het belang van samenwerking voor een succesvolle opsporing. Daartoe werkt de politie, met name het Team High Tech Crime, samen met het Nederlandse Forensisch Instituut en Europol/EC3. Particuliere bedrijven zijn niet betrokken bij ontsleuteling in een strafrechtelijk onderzoek.

- De Nederlandse Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg) vormen het wettelijk kader voor toegang tot persoonsgegevens en de vernietiging van gegevens wanneer deze niet langer van betekenis zijn voor een strafrechtelijk onderzoek. De fundamentele rechten en vrijheden worden ook beschermd door de Nederlandse grondwet.

- Het Nederlandse recht kent de verplichting om op het Nederlandse grondgebied begane misdrijven op te sporen. Voorts verschaft het Wetboek van Strafrecht de rechtsgronden voor veel specifieke misdrijven die buiten Nederland worden begaan. Het Wetboek van Strafrecht vestigt de rechtsmacht voor vrijwel alle cybermisdrijven die door Nederlandse onderdanen in het buitenland worden begaan. Het Nederlandse recht kent het actieve nationaliteitsbeginsel.

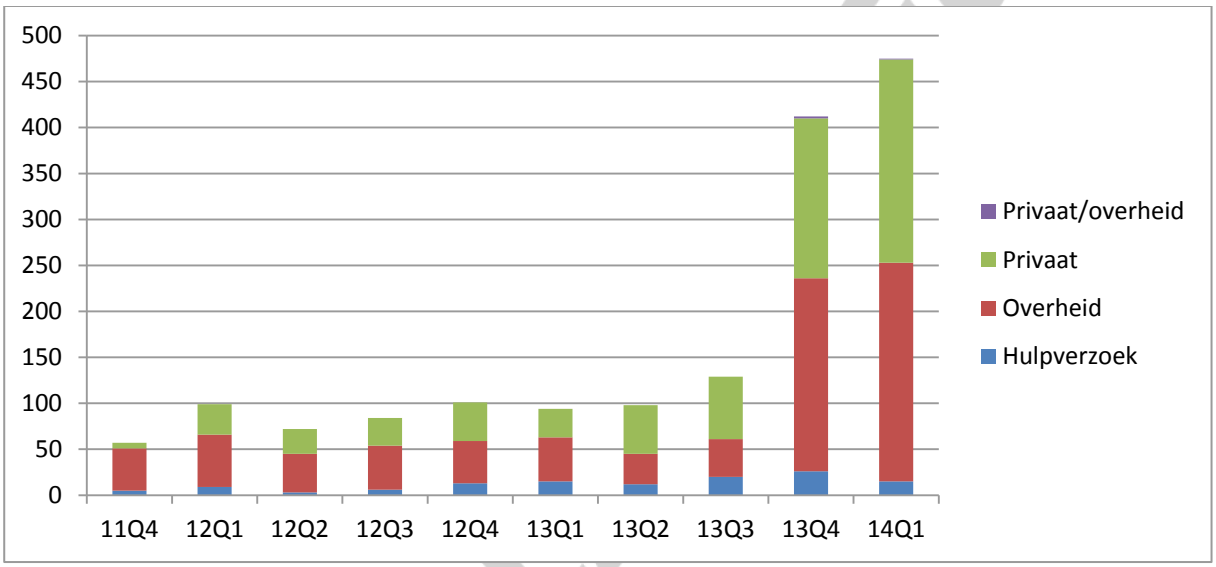
- Cybercriminaliteit in de cloud werd tijdens een evaluatiebezoek aangemerkt als een gebied waar problemen liggen voor de opsporing en de vervolging, met name waar het erom gaat de eigenlijke fysieke locatie van de gegevens te achterhalen. Cloudcomputing schept een probleem, niet alleen voor het nationale recht, maar ook voor internationale wetgeving die gebaseerd is op de erkenning van de onafhankelijkheid van staten. Toch kan het volgens de evalueerders nuttig zijn te overwegen zich te buigen over de bestaande juridische kaders/en of de opsporingsproblemen in verband met cybercriminaliteit in de cloud.

6. OPERATIONELE ASPECTEN

6.1. Cyberaanvallen

6.1.1 Aard van de cyberaanvallen

Elk jaar publiceert het ministerie van Veiligheid en Justitie het Cybersecuritybeeld (CSBN) over de ontwikkelingen in de afgelopen twaalf maanden. Het aantal beoordeelde incidenten omvat incidenten die vrijwillig aan het NCSC zijn gemeld. De primaire doelen van het NCSC zijn overheids- en vitale (private) infrastructuur. Daarom zijn niet alle incidenten aan het NCSC gemeld tijdens de verslagperiode.

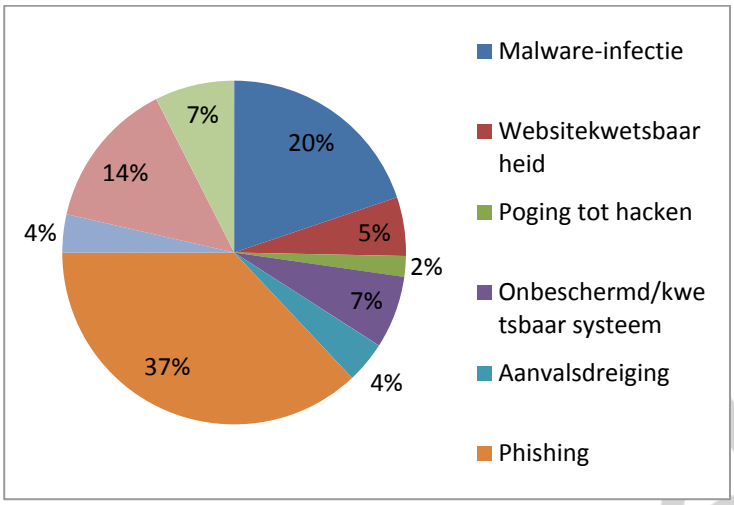


Figuur 1: Incidenten die door het NCSC zijn behandeld (4e kw. 2011-1e kw. 2014). [10]

De Nederlandse autoriteiten verklaarden dat de plotse toename van incidenten (4e kw. 2013 en 1e kw. 2014) in de eerste plaats toe te schrijven is aan de geautomatiseerde computercontrole waarmee in oktober 2013 is begonnen. Voorts is het aantal responsible disclosures aan de Nederlandse regering ook toegenomen vanaf september 2013.

[10] De beschrijvingen in figuur 1 dienen in het Engels in de volgende volgorde worden gelezen: private/public, private, public, request for assistance.

Als de via geautomatiseerde controle geregistreerde incidenten buiten beschouwing worden gelaten, is er nog altijd een stijging van de aan de overheid gemelde incidenten van 89 in het tweede kwartaal tot 163 in het eerste kwartaal van 2014. Deze stijging is misschien te verklaren door factoren zoals wijzigingen in de criteria die worden gebruikt om een incident te omschrijven, beter functionerende systemen en de grotere professionalisering van het NCSC. Ook is het aantal door de particuliere sector gemelde incidenten tijdens de verslagperiode toegenomen.



Figuur 2: Meldingen van impact-incidenten in verband met private partijen[11]

Het evaluatieteam gaf er zich rekenschap van dat het ontbreken van algemene landelijke statistieken over cybercrime, onder meer incidenten gerapporteerd door natuurlijke personen die gedupeerd zijn door cybercriminaliteit, een algemene beoordeling van dit fenomeen bemoeilijkt. Omdat een precieze definitie van cybercriminaliteit kennelijk ontbreekt - het is gebruikelijk een beperkte definitie te hanteren zoals die voor high tech-misdrijven (*gericht tegen computers en met gebruik van computers*) - en de totale cijfers inzake cybercriminaliteit (als percentage van alle criminaliteit) niet te bepalen zijn, is het moeilijk een duidelijk beeld te krijgen van het effect van het fenomeen cybercriminaliteit.

[11] De beschrijvingen in figuur 2 dienen in het Engels in de volgende volgorde worden gelezen: malware infection, website vulnerability, attempt to hack, unprotected/vulnerable system, attack threat, phishing.

6.1.2 Responsmechanismen voor cyberaanvallen

De Nederlandse autoriteiten hebben laten weten dat verhoging van de digitale weerbaarheid van Nederland niet door de overheid alleen kan worden verwezenlijkt. Zij zien een belangrijke rol weggelegd voor de particuliere sector, met name exploitanten van vitale infrastructuur en informatiesystemen, omdat de ICT-infrastructuur zelf en de kennis van die infrastructuur grotendeels in handen is van nationale en internationale private partijen. Daarom wordt cybersecurity in Nederland gezien als een gezamenlijke inspanning van overheidsinstanties, het bedrijfsleven en andere organisaties en burgers, zowel op nationaal als op internationaal niveau. Exploitanten van vitale infrastructuur zijn als eerste verantwoordelijk voor het nemen van maatregelen om de continuïteit van hun eigen diensten te garanderen. Mede door de toegenomen samenwerking tussen de verschillende particuliere bedrijven en overheidsorganisaties binnen Information Sharing and Analysis Centres (ISAC's) blijven de cyberincidenten of -bedreigingen gering. ISAC's zijn publiek-private partnerschappen, per sector georganiseerd, waarbinnen de deelnemers informatie en ervaringen over cyberbeveiliging uitwisselen.

De minister van Veiligheid en Justitie is voornemens melding van ICT-incidenten verplicht te maken voor aanbieders van producten of diensten waarvan de beschikbaarheid en betrouwbaarheid vitaal zijn voor de Nederlandse samenleving. Het gaat om: elektriciteit, gas en water; telecom; waterbeheer; financiën; vervoer (Rotterdamse haven en luchthaven Schiphol); en overheidsinstanties. Bij wet moet een meldplicht worden ingevoerd bij inbreuk op de veiligheid van een bedrijf of het verlies aan integriteit van elektronische informatiesystemen in componenten waarbij een inbreuk direct of indirect kan leiden tot sociale verstoring. De melding moet worden gedaan aan de minister van Veiligheid en Justitie en zal worden behandeld door het NCSC. De melding moet de volgende gegevens bevatten:

- aard en omvang van de inbreuk;
- datum van het begin van de ICT-inbreuk;
- potentieel effect van de inbreuk;
- raming van de duur van het herstel;
- door de aanbieder te nemen (of reeds genomen) maatregelen;
- contactgegevens van de ambtenaar die belast is met de melding.

Het Team Tech Crime en het NCSC hebben verbindingsambtenaren. Die partijen wisselen binnen de grenzen van de wet informatie uit over een incident. Indien incidenten een verstorend effect op de samenleving hebben of dreigen te hebben, staat het NCSC ten dienste van de nationale crisisstructuur. Het NCSC heeft tot taak een ICT-dreiging als eerste te constateren en te signaleren. De informatievergaring en -uitwisseling wordt door het NCSC gecoördineerd. Indien nodig activeert het NCSC de ICT Response Board (IRB). De IRB is een publiek-privaat adviserend orgaan dat belast is met het maken van een situatieanalyse en het interpreteren ervan, en het verstrekken van advies bij ernstige ICT-incidenten. Het advies kan worden gebruikt door de nationale crisisstructuur van de overheid, en door de andere IRB-partijen. In de IRB zijn thans vertegenwoordigd telecombedrijven, energieleveranciers, banken en overheidsorganisaties zoals de politie. Het Nationaal Crisis Centrum (NCC) neemt, na advies te hebben ingewonnen bij de IRB, maatregelen om te reageren op een ernstig cyberincident. Vervolgens monitort en/of ondersteunt het NCSC de uitvoering van de maatregelen door het NCSC.

Voorts coördineerde het NCSC de oprichting van het Nationaal Respons Netwerk (NRN) in april 2014. Het NRN is een samenwerkingsverband tussen publieke en private organisaties die de digitale weerbaarheid van vitale systemen in het land moet vergroten. Doel van het NRN is informatie te delen en de respons te coördineren bij grootschalige cybersecurity-incidenten. De aanvankelijke deelnemers waren de Belastingdienst, SURFnet, DefCERT, de Informatiebeveiligingsdienst voor gemeenten (IBD) en het NCSC. Via het NRN, faciliteert het NCSC de optimale respons bij ernstige cyberincidenten. Verwacht wordt dat meer publieke en particuliere partners zich in de nabije toekomst bij het NRN zullen aansluiten.

De overheid zet in op het intensiveren van de samenwerking bij operationele respons tussen de CERT-organisaties in Europa, zoals vastgelegd in zowel NCSS1 als NCSS2. Nederland werkt, hoofdzakelijk op informele basis, mee aan internationale netwerken zoals het International Watch and Warning Network (IWWN), FIRST, the European Government Cert network, en TF-CSIRT, en via bilaterale contacten.

Volgens de NCSS2 wordt voorts van burgers verwacht dat zij samenwerken met overheidsinstanties, het bedrijfsleven en instellingen waar het gaat om aangetroffen kwetsbaarheden in hun ICT-beveiliging. Het evaluatieteam heeft echter de indruk dat veel meer is gedaan aan het betrekken van burgers bij het tegengaan van kinderporno dan bij andere vormen van cybercriminaliteit.

6.2 Maatregelen tegen kinderporno en online seksueel misbruik

In verband met seksueel misbruik van kinderen hebben de Nederlandse autoriteiten voor 2013 de volgende cijfers meegedeeld: 3790 meldingen, tegen 542 verdachten is vervolging ingesteld, 130 slachtoffers zijn geïdentificeerd, en er waren vijf zaken van kindersekstoerisme.

6.2.1 Softwaredatabanken voor het identificeren van slachtoffers en maatregelen om herhaald slachtofferschap te voorkomen

De Nederlandse politie is al jarenlang bezig met het opslaan in haar databank van een groot aantal afbeeldingen van seksueel misbruik van kinderen die op grond van het Nederlandse Wetboek van Strafrecht als illegale afbeeldingen worden aangemerkt. Om het effectieve gebruik van deze databank te verbeteren zijn de beelden van een hashcode voorzien.
De Nederlandse rechtshandhavingsorganisaties werken samen in het Europese "in-4-mation"-project, waarin de nationale databanken van de deelnemende landen met elkaar verbonden zijn. Die "in-4-mation" databank is nog niet helemaal gereed, maar Nederland loopt voor op het schema en is al bezig met de implementatie ervan. De Nederlandse rechtshandhavingsinstanties, in het bijzonder de politie, werkt actief mee aan de inspanningen van Interpol om slachtoffers te identificeren. Dit omvat bijdragen aan en gebruik maken van de ICSE-databank.

In 2008 heeft de minister van Economische Zaken een juridisch niet bindende overeenkomst gesloten met een groot aantal internetdienstaanbieders over een op vrijwilligheid gebaseerd model van "notice and take down" van illegale uitingen op het internet. Meer dan 95% van de internetdienstaanbieders vallen onder deze overeenkomst.

6.2.2 Maatregelen om seksuele uitbuiting/misbruik online, sexting en cyberpesten aan te pakken

Volgens de Nederlandse autoriteiten bevindt cyberpesten zich op het snijvlak tussen crimineel en niet-crimineel gedrag. Sexting is ook een verschijnsel dat zich op de grens tussen legaal en illegaal gedrag bevindt. Enerzijds is het zo dat kinderen hun eigen seksualiteit verkennen, maar anderzijds kunnen zij ongewild het slachtoffer worden van seksueel misbruik. Als er meldingen komen, reageert de politie daarop en is het mogelijk dat een onderzoek wordt geopend. De belangrijkste respons op cyberpesten en sexting is preventie, nl. kinderen bewust maken van veiligheid online.

6.2.3 Preventieve maatregelen tegen sekstoerisme, kinderpornografie en andere fenomenen

De Nederlandse autoriteiten hebben gemeld dat de aanpak van kindersekstoerisme de afgelopen jaren naar een hoger niveau getild is. In oktober 2013 heeft het ministerie van Veiligheid en Justitie het parlement een actieplan toegezonden ter bestrijding van kindersekstoerisme (of grensoverschrijdende seksuele misdrijven met kinderen). Het actieplan legt een grotere nadruk op het voorkomen van kindersekstoerisme, betere opsporing en vervolging, en betere nationale en internationale samenwerking. De Nederlandse politie heeft onder meer twee flexibele verbindingsambtenaren gestationeerd in Brazilië (waar het wereldkampioenschap voetbal plaatsvond) en de Filipijnen (bestemming van seksmisdadigers). Die liaisons intensiveren de strijd tegen kindersekstoerisme en dragen bij aan internationale samenwerking. Voorts is een Nederlands bewijs van goed gedrag opgesteld en gepubliceerd, met het oog op wereldwijd gebruik.

Andere maatregelen omvatten de mogelijkheid het paspoort van een veroordeelde kindermisbruiker in te nemen, en voorts ook het wetsvoorstel over het toezicht op delinquenten die zijn veroordeeld wegens gewelddadig seksueel misbruik. Op die manier zullen bekende plegers van seksuele misdrijven met groot recidiverisico niet buiten Europa kunnen reizen om aan kindersekstoerisme te doen (reizende kindermisbruikers).

Vertoningen van kinderporno in real-time op het web, bijvoorbeeld met een webcam, vormen een nieuwe dreiging. Binnenslands behelst dit het groomen van kinderen, waarbij kinderen er geleidelijk toe worden overgehaald en/of worden gechanteerd om naakt te poseren en /of seksuele handelingen te verrichten. In andere landen, vooral landen waar kindermisbruik veel voorkomt zoals in Zuid-OostAzië, kan dit leiden tot het online bekijken van seksueel misbruik van kinderen. Het is moeilijk om adequate oplossingen te vinden.

Momenteel werken de Nederlandse rechtshandhavende instanties aan methodes om vroege detectie en aansluitend de opsporing en vervolging van online groomers (kinderlokkers) te verbeteren, door undercoveroperaties uit te voeren waarbij politieagenten zich voordoen als een kind in onlinechatrooms om de identiteit van de groomer te achterhalen en/of een online afspraak te maken om de groomer te arresteren. De nieuwe wet cybercriminaliteit stelt groomen strafbaar met het oog op de ondersteuning van deze werkmethode.

Mediaeducatie is een krachtig instrument ter voorkoming van seksueel misbruik van kinderen, met name voor kinderen en adolescenten. Ouders en scholen spelen een cruciale rol in mediaeducatie. Vanaf 2008 runnen de ministeries van Volksgezondheid en Jeugd en Gezin een speciaal kenniscentrum voor mediaeducatie. Dit centrum (www.mediawijzer.net) wil de mediaeducatie van de bevolking verbeteren, met name die van jongeren (10-14-jarigen). In het kader van het centrum werken vele verschillende organisaties samen en bieden zij lesmateriaal, campagnes, enz. aan. Voorts wordt mediaeducatie georganiseerd en aangemoedigd door een publiek-privaat partnerschap met de naam "Digivaardig-Digiveilig".

Het Nederlandse ministerie van Veiligheid en Justitie subsidieert samen met de EU een meldpunt voor het signaleren van seksueel misbruik van kinderen, dat lid is van het internationale INHOPE-netwerk. Naast het ontvangen van eigenlijke meldingen houdt het meldpunt zich ook bezig met de (digitale) educatie van kinderen die het risico lopen seksueel te worden misbruikt, zoals het risico van grooming (www.helpwanted.nl). Een ander initiatief van dit meldpunt is het introduceren van een zogenoemde meldknop die op een browser gedownload kan worden. Die knop brengt gebruikers naar de website van het meldpunt, waar seksueel misbruik van kinderen kan worden gemeld en tips worden gegeven om weerbaar te worden tegen seksueel misbruik van kinderen. De website richt zich hoofdzakelijk op 11- tot 16-jarigen.

Het ministerie van Veiligheid en Justitie heeft nauwe contacten met socialemediabedrijven zoals Twitter. Het voornaamste doel van deze samenwerking is nieuw kindermisbruik-materiaal zo spoedig mogelijk te verwijderen. Tijdens deze contacten werd de "PhotoDNA" besproken, software die kindermisbruik-materiaal erkent.

De Nederlandse politie host een wekelijks onlinevragenuurtje, waarbij kinderen kunnen chatten met politie-agenten (http://www.vraaghetdepolitie.nl). Deze site wordt sterk gepromoot en geniet brede bekendheid bij het publiek. Hij is voornamelijk gericht op jongeren: die kunnen er vragen stellen over hun onlineactiviteiten of over specifieke onderwerpen zoals onlinemisbruik.

6.2.4 Actoren en maatregelen bij de bestrijding van websites die kinderporno bevatten of verspreiden

Artikel 125o Sv verleent de aanklager de bevoegdheid om de content van een webpagina te verwijderen als tijdelijke maatregel, indien dat noodzakelijk is in een concreet opsporingsonderzoek naar seksueel misbruik van kinderen. Bij rechterlijk uitspraak wordt dan besloten de content te verwijderen.

Benadrukt moet worden dat in Nederland particuliere bedrijven sterk betrokken zijn bij publieke initiatieven zoals het bestrijden van kinderporno. Een op vrijwilligheid gebaseerd model van "notice and take down" van illegale uitingen dient als voorbeeld te worden genoemd. Daartoe wordt een uniforme tijdsgebonden procedure gebruik waarbij een internetdienstaanbieder een melding van de aanwezigheid van illegaal materiaal op websites waartoe hij toegang verleent, natrekt en vervolgens een gemotiveerd besluit neemt om dat materiaal al dan niet te verwijderen. Wordt besloten het materiaal te verwijderen, dan wordt er naar de persoon die de domeinnaam geregistreerd heeft, onderzoek ingesteld naar gelang van de nationaliteit. Indien het om een Nederlander gaat wordt verder opsporingswerk gedaan. Dat gebeurt een of twee keer per jaar. In alle overige gevallen is de geregistreerde een buitenlander.

In 2009 is een publiek-privaat partnerschap van internetaanbieders, rechtshandhavende instanties en de ministeries van Veiligheid en Justitie en Economische Zaken met een werkgroep over internet en beveiliging begonnen. De groep hield zich meer bepaald bezig met het (destijds lopende) project van het blokkeren van beelden van seksueel misbruik van kinderen door de DNS. In dit project hebben de internetaanbieders en het Nederlandse meldpunt "meld kinderporno op het internet" een methode ontwikkeld om websites die bekende beelden van seksueel misbruik van kinderen bevatten, te blokkeren. Het meldpunt is ter beschikking gesteld door de Nederlandse politie op DNS-niveau. Een proefstudie heeft tot de conclusie geleid dat deze DNS-blokkeermethode op een zodanig klein aantal websites kon worden toegepast dat de resultaten niet opwogen tegen de kosten. Het project werd in 2011 beëindigd.

Een ander project dat in 2012 werd gestart, en waarbij het uploaden van beelden via een in Nederland gebaseerde grote hostingprovider werd gekoppeld aan de databank met hashcode van bekende beelden van seksueel misbruik van kinderen, bleek van weinig nut voor de opsporing. De Nederlandse politie besefte echter dat het wèl nuttig zou kunnen zijn als de private sector verder de mogelijkheden van "whitelisting"-tools en -toepassingen zou kunnen verkennen om te voorkomen dat private of zakelijke netwerken bekende beelden van seksueel misbruik van kinderen verspreiden.

Voorts wisselen de INHOPE-meldpunten onderling informatie over beelden uit die volgens hen afkomstig zijn uit hun landen (althans wat betreft de locatie waar de websites met de bewuste beelden gehost worden). Het betrokken meldpunt stuurt die beelden naar de bevoegde rechtshandhavende organisaties.

De Nederlandse politie werkt actief mee aan de inspanningen van Interpol om slachtoffers te identificeren, en draagt meer bepaald bij aan en maakt gebruik van de ICSE-databank (voor meer details zie punt 7.2).

De Nederlandse politie werd in 2013 lid van de Virtual Global Taskforce. De meest recente internationale conferentie van de VGT vond in november 2014 in Nederland plaats en werd ook door Nederland georganiseerd. Het thema van deze conferentie was "Transnational Child Sex Offences" en het accent lag op seksmisdrijven tegen kinderen met een internationale component.

Er zijn ook gespecialiseerde eenheden die zich uitsluitend met kinderpornografie bezighouden. Sedert oktober 2012 opereren de rechercheurs die zich bezighouden met kinderporno en kindersekstoerisme in landelijk georganiseerde uniforme eenheden. De landelijke eenheid en de 10 regionale eenheden hebben een uniform team voor het rechercheren van kinderporno en kindersekstoerisme. Bij die eenheden werken 150 rechercheurs en ze worden als één organisatie geleid. Om hun mentale weerbaarheid te versterken heeft de Nederlandse overheid een programma geestelijke gezondheid ontwikkeld. De politie en het OM hebben een landelijke stuurgroep ingesteld om een nationaal strategisch raamwerk en nationale prioriteiten vast te stellen voor het opsporen van kinderporno en kindersekstoerisme. De landelijke stuurgroep bewaakt ook de tenuitvoerlegging van het raamwerk en de prioriteiten. Voorts stuurt een tactische adviesgroep de uitvoering en houdt hij toezicht op de resultaten van concrete opsporingen. De tactische groep heeft de accentverschuiving bij de recherche van downloaders naar de slachtoffers van seksueel misbruik, de eigenlijke misbruiker en de belangrijkste verspreiders, op de voet gevolgd. Op landelijk niveau zijn vier aanklagers aangesteld om de te zorgen voor de koppeling tussen de landelijke aanpak en de regionale vervolgingen.

6.3 Onlinekaartfraude

6.3.l Online melden

Het samenwerkingsplatform tussen de politie, het OM en de onlinemarktplaatsen is het Financial Information Sharing and Analysis Centre (FI-ISAC). Het is een voorziening voor internetklanten om na te gaan of een internetaanbieder als onbetrouwbaar te boek staat, en om online handelsfraude aan de politie te melden.

6.3.2 Rol van de private sector

De private sector speelt een vooraanstaande rol in het Nederlandse systeem ter bestrijding van onlinekaartfraude. Die rol is omschreven in de punten 4.3 en 5.1.2.

Er zijn vele platforms voor het uitwisselen van informatie over specifieke zaken, het op het spoor komen van nieuwe criminele methoden en het bespreken van mogelijke acties om ze tegen te gaan. Niettemin verdient de Electronic Crimes Task Force (ECTF) naar de mening van het evaluatieteam speciale aandacht omdat deze een unieke gelegenheid biedt om informeel gegevens en informatie uit te wisselen over nieuwe betaalmethodes, technologie en eventuele kwetsbaarheden waarmee de rechtshandhavende instanties eventueel aan de slag kunnen.

6.4 Conclusies

- Nederland maakt jaarlijkse statistieken over cybercriminaliteit. Het ministerie van Veiligheid en Justitie publiceert het Cybersecuritybeeld (NSCB) over de ontwikkelingen in de voorbije twaalf maanden.

- Omdat de statistieken ook betrekking hebben op vrijwillig aan het NCSC gemelde incidenten, is het moeilijk om tot een algemeen beeld te komen van door de politie en de private sector gedetecteerde cybercriminaliteit. De situatie kan in de toekomst veranderen omdat de Nederlandse overheid het gamma van incidenten die door de particuliere sector aan de rechtshandhavende instanties moeten worden gemeld, wil uitbreiden.

- De nieuwe conceptwetgeving introduceert een meldplicht bij inbreuk op de veiligheid van een bedrijf of het verlies van integriteit van elektronische informatiesystemen in componenten waarbij een inbreuk direct of indirect kan leiden tot sociale verstoring. Het NCSC zal die melding behandelen.

- Mede door de toegenomen samenwerking tussen de verschillende particuliere bedrijven en overheidsorganisaties blijft het aantal cyberincidenten of -bedreigingen laag. Toch moeten de cybercrimebestrijders - het OM, de landelijke politie en de publiek-private structuren - volgens de evalueerders een evenwichtiger aanpak hanteren en meer aandacht schenken aan de belangen van secundaire slachtoffers. Volgens de evalueerders zijn de publiek-private partnerschappen te zeer gericht op het beschermen van de financiële markten en de infrastructuur van het land, en is er minder aandacht voor de belangen van secundaire slachtoffers.

- Nederland heeft structuren en capaciteit opgezet om online seksuele uitbuiting van kinderen aan te pakken, waarbij er ook aandacht geschonken wordt aan slachtoffers. De rechtshandhavende instanties werken samen met andere internationale entiteiten op dit gebied, zoals de NCMEC, en steunt initiatieven voor het aanpakken van het probleem van reizende kindermisbruikers.

- Het nationaal programma tegen beelden van seksueel misbruik van kinderen en grensoverschrijdende kinderseksmisdrijven is een voortreffelijk initiatief voor het tegengaan van deze specifieke aspecten van seksuele uitbuiting van kinderen, seksueel misbruik van kinderen en kinderporno. De op vrijwilligheid gebaseerde benadering "notice and take down" lijkt erg effectief te zijn door het aantal internetaanbieders dat eraan meewerkt. De vraag blijft echter of, wil het zijn volle potentieel realiseren, er niet een grotere overheidsbetrokkenheid noodzakelijk is, wellicht met flankerende wettelijke maatregelen.

- De publieke campagnes tegen kinderporno, en met het werk van de gespecialiseerde eenheden die zich uitsluitend met kinderporno en kindersekstoerisme bezighouden, verdienen bijzondere aandacht. Ook levert de nauwe samenwerking met Europol en Eurojust en internationale samenwerking met partners van buiten Europa resultaten op wat betreft toenemende detectie van kinderporno. Het detacheren van verbindingsambtenaren door de Nederlandse politie in landen waar sekstoerisme voorkomt, draagt bij aan het tegengaan van kinderporno.

- Het Nederlandse programma geestelijke gezondheid voor rechtshandhavers die zich bezighouden met de seksuele uitbuiting van kinderen is opmerkelijk. De mentale weerbaarheid van ambtenaren die op een zaak zitten waarbij er sprake is van beelden van seksueel misbruik van kinderen, het identificeren van slachtoffers en het leggen van verbanden, vergt speciale aandacht, zodat ze gezond blijven ondanks het veeleisende werk dat ze verrichten.

- Naar de mening van de evalueerders, zal voortgezette actie om de samenleving en lokale rechercheurs en aanklagers bekend te maken met de wijze waarop kinderpornografie moet worden aangepakt en bewijs moet worden vergaard, deze aanpak versterken.

- De Electronic Crime Task Force (ECTF) is een zeer goed voorbeeld van politiële en financiële samenwerking gebaseerd op het delen van relevante informatie, die het mogelijk maakt onlinekaartfraude dagelijks op dezelfde plaats efficiënt aan te pakken. De resultaten van deze samenwerking zijn veelbelovend aangezien de statistieken een dalende trend in onlinekaartfraude in Nederland laten zien.

- Het succes van publiek-private partnerschappen moet worden beschouwd als beste praktijk om na te gaan hoe de beste resultaten kunnen worden bereikt met de nauwe samenwerking tussen de publieke sector (politie en OM) en de private sector (bv. internetaanbieders, sociale netwerken online, ngo's, meldpunten, enz.).

7. INTERNATIONALE SAMENWERKING

7.1. Samenwerking met EU-instanties

7.1.1. Formele vereisten om samen te werken met Europol/EC3, Eurojust, Enisa

De Nederlandse autoriteiten onderstreepten dat het verbeteren van de samenwerking met Europol/EC3 een prioriteit is in de NCSS2. De Nederlandse politie biedt actieve ondersteuning aan Europol/EC3. Dat moet ook helpen bij de bestrijding van online-uitbuiting van kinderen.

Het Openbaar Ministerie heeft, met de hulp van Eurojust, het initiatief genomen om de internationale samenwerking van openbaar aanklagers in cybercrimezaken te intensiveren.

Nederland investeert ook in kennis en expertise, en neemt deel aan gezamenlijke onderzoeken.

Het evaluatieteam constateerde echter op lokaal niveau dat de officieren van justitie van de OM-regio's en de regionale eenheden van de politie slechts een vage en ontoereikende kennis van de mogelijkheden van Eurojust lijken te hebben en die daarom niet zo vaak benutten als nodig om de justitiële samenwerking te faciliteren of steun te verlenen wanneer coördinatie nodig is.

7.1.2. Evaluatie van de samenwerking met Europol/EC3, Eurojust, Enisa

Volgens de Nederlandse autoriteiten zit de waarde van Europol en Eurojust precies in het verbinden van landen bij specifieke opsporingen en coördinatie. Daarom kan Eurojust de focus houden op de algemene strategie bij de rechtshandhavende benadering van eventuele strafrechtelijke onderzoeken.

In voorkomende gevallen, wordt contact met Enisa opgenomen via het NCSC of het ministerie van Veiligheid en Justitie.

7.1.3. Operationele prestaties van GOT's en cyberpatrouilles

Naar de mening van de Nederlandse overheid kan een gemeenschappelijk onderzoeksteam (GOT) bijdragen aan een goede samenwerking tussen Europol and Eurojust. Het college van procureurs-generaal heeft op 11 februari 2008 een instructie voor het OM uitgevaardigd om een gemeenschappelijk beleid inzake het gebruik van GOT's te ontwikkelen. Daarin worden regels gegeven voor de oprichting, het werkterrein, de samenstelling en de bevoegdheden van internationale GOT's.

Nederland heeft goede ervaringen met het werken met GOT's. Onlangs waren twee GOT's actief met betrekking tot cybercrime, waaraan Nederland heeft meegedaan. Europol en Eurojust hadden daarbij een centrale rol. Het meest recente opsporingsonderzoek was de zogenoemde Operatie Blackshades. Er waren EU-middelen uitgetrokken om deze samenwerking te vergemakkelijken, maar die waren beperkt tot een reisbudget om ontmoetingen te hebben met GOT-partnerlanden.

Volgens de Nederlandse autoriteiten is het gebruik van open bronnen een methode die gebruikt wordt door de Landelijke Eenheid.

De teamleider van het Team High Tech Crime neemt deel aan de Strategic Group of the Heads of National High Tech Crime Units van de Europese Unie bij Europol. De Nederlandse politie is ook actief in het project over seksueel misbruik van kinderen in het Empact-programma, en in voorkomende gevallen in de Europese Financiële Coalitie tegen seksuele uitbuiting van kinderen op het internet.

7.2 Samenwerking tussen de Nederlandse autoriteiten en Interpol

De Nederlandse politie werkt actief mee aan de inspanningen van Interpol om slachtoffers te identificeren. Dit houdt onder meer in dat wordt bijgedragen aan en gebruik gemaakt van de ICSE-databank. Voorts is in de ICSE-databank van Interpol een nieuwe omgeving gecreëerd met de naam "Baselinelist", die gebruikt wordt om beeldanalyses sneller te laten verlopen. In nauwe samenwerking met de Nederlandse rechtshandhaving zijn er specifieke criteria ontwikkeld om ervoor te zorgen dat de inhoud van die "Baselinelist" internationaal kan worden uitgewisseld. De baseline is het materiaal dat in ieder deelnemend land strafbaar is op grond van het strafrecht. Dat deel van de ICSE is nog niet klaar, maar de Nederlandse rechtshandhaving is gereed om te beginnen met het uploaden naar die databank.

Voorts heeft Nederland zijn steun uitgesproken voor de ontwikkeling van het Global Complex for Innovation (IGCI) van Interpol in Singapore. Het Team High Tech Crime van de politie steunt de verwezenlijking van het IGCI. Een verbindingsambtenaar van de politie en een deskundige van het team zullen bij het IGCI worden gedetacheerd om ervaringen en expertise uit te wisselen.

De overheid zet in op het intensiveren van de samenwerking bij operationele respons tussen de CERT-organisaties in Europa, zoals vastgelegd in zowel NCSS1 als NCSS2. Nederland werkt, hoofdzakelijk op informele basis, mee aan internationale netwerken zoals het International Watch and Warning Network (IWWN), FIRST, het European Government CERT network, en TF-CSIRT, en via bilaterale contacten.

7.3 Samenwerking met derde landen

De Nederlandse autoriteiten benadrukten dat zij in derde landen cybersecuritycapaciteit aan het ontwikkelen zijn via bilaterale of regionale initiatieven. Op nationaal en internationaal niveau moeten schaarse vermogens worden ingezet voor kwetsbare sectoren en groepen. Afgezien van de overheden, is een belangrijke rol weggelegd voor partijen uit de private sector en maatschappelijke organisaties. Nederland promoot deze benadering op internationaal vlak – bij de Verenigde Naties, tijdens internationale conferenties over cyberspace, zoals die welke plaatsvonden in Londen, Boedapest en Seoul en de aanstaande Global Cyber Space Conference in Nederland in april 2015, alsmede in multi-stakeholder initiatieven zoals het Internet Governance Forum – door de cybersecurity-principes te propageren die zijn gepubliceerd door het World Economic Forum, en door vertrouwenscheppende maatregelen tussen staten te ontwikkelen, zoals de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE).

Tijdens het bezoek ter plaatse werd het evaluatieteam medegedeeld dat er een overeenkomst is tussen de VS en Nederland die de Nederlandse autoriteiten in staat stelt om rechtstreekse rechtshulpverzoeken toe te zenden aan Amerikaanse bedrijven. Naar de mening van het evaluatieteam is dit te beschouwen als een geschikt instrument om de opsporingen te bespoedigen.

De Nederlandse autoriteiten zijn van mening dat samenwerking met Europol/EC3 en Eurojust toegevoegde waarde heeft opgeleverd in zaken waarbij derde landen betrokken waren. Als voorbeeld kan worden genoemd hun bijdrage aan het welslagen van opsporingsonderzoeken naar cybercriminaliteit, zoals:

- Onderzoek naar seksueel misbruik van kinderen: de gezamenlijke Operation Atlantic, uitgevoerd door het Federal Bureau of Investigation (FBI) en verschillende EU-lidstaten, werd afgerond in 2011, en Europol had daarbij een coördinerende rol. Na meer dan een jaar van opsporingen in de lidstaten werden 37 kindermisbruikers geïdentificeerd. Daarvan werden er 17 gearresteerd wegens het seksueel molesteren van kinderen en het produceren van illegale content. Ook zijn acht slachtoffers geïdentificeerd.

- Het Blackshades-opsporingsonderzoek: gedurende twee dagen van operaties in 16 landen wereldwijd, gecoördineerd door Eurojust en met de steun van Europol/EC3, richtten de justitiële en rechtshandhavende instanties in mei 2014 hun acties op makers, verkopers en gebruikers van Blackshades-malware.

7.4 Samenwerking met de particuliere sector

De Nederlandse wet stelt internetaanbieders aansprakelijk voor illegale content die via hun systemen op internet wordt geplaatst indien zij daarvan volledig op de hoogte zijn, overeenkomstig de EU-wetgeving. De Nederlandse autoriteiten meldden echter dat veel internetaanbieders slechts een doorgeefluik zijn en in die situatie is er een uitzondering op de aansprakelijkheid van internetaanbieders.

Om het verwijderen van illegale uitingen van het internet te faciliteren, is het op vrijwilligheid gebaseerde model van "notice and take down" geïntroduceerd om zelfregulering in de bedrijfstak te stimuleren (voor nadere informatie, zie de punten 6.2.1 en 6.2.4).

Voorts heeft de officier van justitie de bevoegdheid om een organisatie te bevelen illegale content van het internet te halen (artikel 125o Sv). Voorts worden in het Sv verscheidene bevoegdheden genoemd om bevelen uit te vaardigen voor het verzamelen van bewijs via doorzoeking en inbeslagname van informatiesystemen/computergegevens, het bewaren van computergegevens, opgeslagen verkeers-/contentgegevens, en gebruikersinformatie. Die bevelen kunnen gericht zijn tot private bedrijven indien zij hun hoofdkantoor in een derde land hebben. Internetaanbieders die zich in het buitenland bevinden, kunnen direct worden benaderd om vrijwillig samen te werken in het kader van verzoeken/bevelen, mits de regering van het land waar een bedrijf gevestigd is, daarin toestemt. Nederland zegt in de praktijk vele goede ervaringen met deze methode te hebben.

In 2010 is het THTC een publiek-privaat partnerschap voor het bestrijden van botnets begonnen. Samen met leden van de CERT-gemeenschap, het bedrijfsleven en internetinfrastructuur hebben zij een drieledige aanpak ontworpen, bestaande uit inlichtingen, interventie en opsporing. Alle partners hebben hun botnetinformatie samengebracht en alle botnets werden in real time opgespoord met gebruikmaking van een door universiteiten ontwikkelde tool. Doel was notice and takedown voor de meeste botnets en een nader onderzoek naar een aantal onder hen. Een van de partners, een grote internetaanbieder, vond een botnetcommando- en controleserver in zijn infrastructuur. De partners begonnen met de opsporing en troffen een cluster van 143 kwaadaardige servers aan, waarvan er zeven direct verbonden waren met een botnet met de naam Bredolab. Op dat ogenblik had Bredolab reeds 30 miljoen unieke IP-adressen geïnfecteerd. De partners zijn erin geslaagd over een periode van tien weken de infrastructuur van het botnet in beeld te brengen. Zij konden ook iemand identificeren die ervan verdacht werd het netwerk te exploiteren, een Armeniër die van plan was naar Nederland te komen voor een dance party. Bedoeling was het netwerk te ontmantelen op de dag dat de Armeniër in de luchthaven van Amsterdam zou aankomen. De Armeniër zou bij aankomst worden gearresteerd maar is vanwege visumproblemen niet komen opdagen. In plaats daarvan kreeg hij in de gaten dat iemand zijn botnet aanviel, dacht hij dat het een concurrent was en voerde hij een tegenaanval uit. Na diverse backdoors te hebben geprobeerd, besloot hij een DDoS-aanval uit te voeren op het resterende deel van zijn eigen botnet. Door goede internationale samenwerking kon de commando- en controleserver van het DDoS-botnet snel worden ontmanteld. Naar aanleiding van een red notice van Interpol kon de verdachte de volgende dag op de luchthaven van Erevan worden gearresteerd. Hij werd in Armenië en tot vier jaar gevangenisstraf veroordeeld.

7.5 Instrumenten van internationale samenwerking

Internationale samenwerking in cybercrimezaken berust op dezelfde regels die gelden bij wederzijde rechtshulp, wederzijde erkenning, overlevering en uitlevering in Nederland.

7.5.1 Wederzijdse rechtshulp

Nederland ontvangt een groot deel van zijn rechtshulpverzoeken of verzoeken om wederzijdse erkenning van andere EU-lidstaten. Beide soorten verzoeken kunnen rechtstreeks naar (regionale) parketten worden gestuurd, die de diensten zijn voor internationale rechtshulp in strafzaken (IRC's). Zij zijn belast met de efficiënte en snelle afwikkeling van verzoeken. Door de instelling van de Internationale Rechtshulp Centra (IRC's) in 2003 is de afhandeling van rechtshulpverzoeken efficiënter geworden, omdat het personeel van de IRC's zich nu exclusief bezighoudt met rechtshulpverzoeken. Daarvoor was het verlenen van rechtshulp voor aanklagers onderdeel van hun reguliere werkzaamheden. De IRC's fungeren nu ook als kennis- en expertisecentra voor internationale hulp. De justitiële instanties in andere lidstaten kunnen hun ambtgenoten in Nederland rechtstreeks benaderen, maar betrekken dan het bevoegde IRC daarbij. De IRC's zijn ingesteld in Nederland met als enig doel rechtshulpverzoeken in strafzaken te registreren, te behandelen en de uitvoering ervan te coördineren.

Voor landen buiten de EU is de minister van Veiligheid en Justitie in Nederland de centrale autoriteit voor internationale justitiële samenwerking in strafzaken en ontvangt hij alle rechtshulpverzoeken rechtstreeks of via diplomatieke kanalen. Bij ontvangst van een verzoek gaat het ministerie van Veiligheid en Justitie, vertegenwoordigd door de Afdeling Internationale Rechtshulp in Strafzaken (AIRS) na of aan alle vereisten van het Nederlandse recht is voldaan, zoals (indien nodig) dubbele strafbaarstelling en het bestaan van een verdragsbasis. Verzoeken die tot de bevoegdheid van het Regionaal Parket behoren, worden met het oog op uitvoering doorgezonden naar het regionale IRC. Zaken die tot de bevoegdheid van het Landelijk Parket behoren worden afgehandeld door het landelijke IRC (LIRC).

Voorts kan naast formele wederzijdse rechtshulp, ook interpolitiële samenwerking plaatsvinden. Indien informatie over gegevens wordt gedeeld voordat een formeel verzoek om doorgifte is ontvangen, kan informatie worden uitgewisseld op interpolitiële basis met toestemming van de officier van justitie, met dien verstande dat de informatie alleen voor opsporingsdoelen mag worden gebruikt. Het verzoekende land moet een formeel rechtshulpverzoek toezenden om informatie als bewijs in een strafproces te kunnen gebruiken. In bepaalde specifieke zaken zenden landen zoals Nederland spontaan informatie naar andere landen.

Het 24/7-contactpunt voor dringende verzoeken is ondergebracht bij het Team High Tech Crime (THTC), dat korte lijnen heeft met het Landelijk Parket voor high-techcrime. Het Landelijk Parket beoordeelt het verzoek en besluit, samen met het Team High Tech Crime van de politie, of het verzoek moet worden uitgevoerd door het Team of door de regionale politie-eenheden. In dat laatste geval zal het Landelijk Parket het verzoek doorzenden naar een lokaal IRC.

De politiële autoriteiten lieten weten dat een van de moeilijkste aspecten van de samenwerking erin bestaat de locatie van gegevens in de cloud te vinden. Ook al kan een aanbieder worden bevolen bepaalde gegevens te verstrekken, in de praktijk blijkt dit vaak erg moeilijk. Er zijn aanbieders die weigeren mee te werken met de politie ("rogue providers"). Soms wordt een aanbieder niet gevonden of is hij gevestigd in een land waarmee Nederland slechts zeer beperkte betrekkingen op het gebied van rechtshulp onderhoudt.

De volgende statistieken bevatten formele informatie over rechtshulp en interpolitiële informatie:

INKOMEND

Terminologie waarop is gezocht	**2012**	**2013**
• computercriminaliteit • cybercrime • Europees aanhoudingsbevel ICT-criminaliteit • internetoplichting • kinderporno	1111	1270

UITGAAND

Terminologie waarop is gezocht	**2012**	**2013**
• computercriminaliteit • cybercrime • Europees aanhoudingsbevel ICT-criminaliteit • internetoplichting • kinderporno	103	226

Gemiddeld wordt binnen 24 uur een eerste antwoord gegeven. Dat kan een aanwijzing zijn van de daadwerkelijk benodigde tijd voor de gevraagde hulp.

Via een rechtshulpverzoek in verband met cybercriminaliteit kan om de volgende maatregelen worden verzocht:

- Bevel tot het verstrekken van gegevens (artikel 126na alsmede de artikelen 126nc, 126nd, 126nf van het Sv)
- Bewaren van computergegevens (artikel 126ni Sv)
- Doorzoeken en in beslag nemen van gegevens uit informatiesystemen/computers (artikel 125i Sv)
- Onderscheppen/verzamelen van verkeers-/contentgegevens in real-time (artikel 126m Sv)

7.5.2 Instrumenten voor wederzijdse erkenning

Er zijn geen specifieke statistieken verstrekt betreffende de toepassing van de verschillende instrumenten voor wederzijdse erkenning.

7.5.3 Overlevering/Uitlevering

Er zijn geen specifieke statistieken verstrekt betreffende overleverings-/uitleveringszaken die alleen op cybercrime betrekking hadden.

7.6 Conclusies

- De Nederlandse politie werkt nauw samen met Europol/EG 3. Dit wordt ook als een prioriteit van de NCSS2 beschouwd. De op Europees niveau bepaalde prioriteiten (met name Empact) zijn terug te zien in de prioriteiten van de politie. De Nederlandse autoriteiten stellen daarnaast de samenwerking met Eurojust op prijs, en steunen actief de acties die zijn ondernomen met de betrokkenheid van Nederland.

- Het evaluatieteam kwam tot het inzicht dat er landelijk goed wordt samengewerkt met Eurojust en Europol/EC3 door het Landelijk Parket en de Landelijke Politie. De vertegenwoordigers van de lokale autoriteiten waarmee een ontmoeting plaatsvond tijdens het bezoek ter plaatse leken niet goed op de hoogte van de mogelijkheden die specifiek worden geboden door Eurojust of Enisa. Op dit punt valt dus nog wel iets te verbeteren.

- Nederland verklaart dat het actief streeft naar nationale en internationale allianties en internationaal samenwerkt op het gebied van cybercrime (in bilateraal verband), en indien nodig door het instellen van GOT's.

- De Nederlandse autoriteiten werken in derde landen aan de opbouw van cybersecuritycapaciteit via bilaterale of regionale initiatieven, meer bepaald om de meest kwetsbare sectoren en groepen te beschermen. Nederland propageert die aanpak internationaal, bv. bij de Verenigde Naties of tijdens internationale conferenties over cyberspace. Uit het besluit om in 2015 de Global Cyber Space Conference te organiseren blijkt de internationale betrokkenheid van Nederland wat de cyberproblematiek betreft.

- De overeenkomst tussen de VS en Nederland die de Nederlandse autoriteiten in staat stelt om rechtstreekse rechtshulpverzoeken toe te zenden aan Amerikaanse bedrijven moet worden beschouwd als een geschikt instrument om de opsporingen te bespoedigen.

- De samenwerking met Interpol lijkt goed te zijn. Nederland heeft een samenwerkingsmodel met de private sector ontwikkeld. Deze benadering helpt bij het bestrijden van online-uitbuiting van kinderen en andere digitale fenomenen als botnets. Het op vrijwilligheid gebaseerde model van "notice and take down" kan ook dienen als beste praktijk om zelfregulering in de bedrijfstak te stimuleren en illegale content van de websites te verwijderen.

- Rechtshulpverzoeken van EU-lidstaten kunnen rechtstreeks worden toegezonden aan de bevoegde IRC's, die onderdeel zijn van het OM. Het IRC-personeel bestaat uit zowel rechtshandhavers als officieren van justitie. Volgens de evalueerders lijkt de ervaring van het Landelijk Parket als expertisecentrum dat met de opsporingen naar high-techcybercrime is belast of de meer complexe rechtshulpverzoeken op dit gebied behandelt en steun verleent aan de regionale officieren van justitie bij andere opsporingen of rechtshulpverzoeken in verband met digitaal bewijs, effectief en dus het bestuderen waard te zijn.

- Verzoeken van landen van buiten de EU worden behandeld door het ministerie van Veiligheid en Justitie, vertegenwoordigd door de Afdeling Internationale Rechtshulp in Strafzaken (AIRS), die nagaat of aan alle vereisten naar Nederlands recht is voldaan, zoals (indien nodig) dubbele strafbaarstelling en het bestaan van een verdragsbasis.

- Voorts kan naast formele wederzijdse rechtshulp ook interpolitiële samenwerking tot de mogelijkheden behoren. Indien informatie over gegevens wordt gedeeld voordat een formeel verzoek om doorgifte is ontvangen, kan er, met toestemming van de aanklager, op interpolitiële basis informatie worden uitgewisseld, met dien verstande dat de informatie alleen voor opsporingsdoelen mag worden gebruikt.

- De Nederlandse autoriteiten verklaarden dat nauwe samenwerking en informatie-uitwisseling tussen de verschillende bij internationale samenwerking betrokken organen van het grootste belang is. De statistieken van 2012 en 2013 vertonen een stijgende trend in het aantal inkomende en uitgaande rechtshulpverzoeken in verband met cybercrime.

8. OPLEIDING, BEWUSTMAKING EN PREVENTIE

8.1. Specifieke opleiding

Het Studiecentrum Rechtspleging (SSR) verzorgt programma's voor initiële opleiding en biedt geavanceerde opleiding voor rechters, officieren van justitie en juridisch personeel, uitgaande van het beginsel dat leren en permanente educatie essentieel blijven gedurende de volledige duur van de loopbaan bij de rechterlijke macht. Het SSR biedt praktische programma's, cursussen, opleiding, coaching en leiderschapsontwikkeling, met onder meer een speciale module digitaal rechercheren (inclusief een cursus onderschepping en een basiscursus cybercriminaliteit).

Voorts heeft de rechterlijke macht geïnvesteerd in aanvullende opleiding over cybercrime. De rechtscolleges hebben een Kenniscentrum Cybercrime ingesteld bij het gerechtshof in Den Haag, waar twee rechters en een griffier werken. Het Kenniscentrum Cybercrime publiceert en verspreidt een nieuwsbrief met berichten over cybergerelateerde thema's zoals recente publicaties, conferenties, seminars en de resultaten daarvan, basisinformatie over lopende strafzaken waarbij sprake is van cybercrime, jurisprudentie, toepasselijke wetgeving en regulering, en uitleg over de basistermen in verband met cybercriminaliteit.

Het Openbaar Ministerie heeft twee gespecialiseerde officieren van justitie benoemd in de OM-regio's en bij het Landelijk Parket. Ook is een intern netwerk opgezet om de officieren van justitie beter bekend te maken met cybercrimethema's. Daarnaast hebben verschillende rechter-commissarissen zich gespecialiseerd in cybercrime. Hoewel iedere officier van justitie of rechter aan cybercrimezaken kan werken, bleek duidelijk uit de meningen van de praktijkmensen waarmee het evaluatieteam een ontmoeting had, dat er behoefte is aan aanvullende gespecialiseerde opleiding over cybercrime.

De politie verzorgt opleidingen op maat van gemiddeld vier dagen per cursus. Er is een regeling getroffen om digitale experts vier weken aanvullende opleiding per jaar te geven om hun kennis en vaardigheden op peil te houden. Voor 2014 zijn de opleidingskosten op 300 000 EUR geraamd. Met name voor gedegen opleiding van digitaal rechercheurs zou een fors hoger bedrag meer capaciteit en deskundigheid opleveren. Dit zou helpen bij opsporingen naar cybercrime en het vergaren van digitaal bewijs. Er dient evenwel te worden opgemerkt dat een deel van het door de minister van Veiligheid en Justitie aan de politie toegewezen budget van 13,8 miljoen EUR specifiek bestemd is voor het opleiden van de politie met betrekking tot cybercriminaliteit.

8.2. Bewustmaking

Volgens de Nederlandse autoriteiten, is bewustmaking over cybergerelateerde thema's een permanente uitdaging, en daarom moet daar op gezette tijden speciale aandacht aan worden besteed. Sedert 2012 heeft het ministerie van Veiligheid en Justitie een jaarlijkse campagneweek voor vergroting van het bewustzijn over cybercriminaliteit georganiseerd. Die week heet Alert Online en wordt georganiseerd met de medewerking van verschillende ministeries en private partners. Alert Online is gericht op de bewustmaking van overheid, bedrijfsleven en burgers. In 2014 liep het programma over bijna twee weken. Het vond plaats in het kader van de jaarlijkse Europese Cybersecuritymaand. Het programma voor die week bestond uit bijdragen van publieke en private organisaties.

Bekendheid met de risico's en kennis van eventueel te nemen maatregelen om die risico's te verkleinen zijn van cruciaal belang voor cyberbeveiliging. In 2013 zijn verschillende campagnes en initiatieven gestart, zoals:

- Cybersecuritymaand (oktober 2013, Enisa);
- Alert Online (28 oktober - 5 november 2013);
- Veilig online bankieren (NVB);
- Safer Internet Day 83 (februari 2014, DigiBewust).

De taskforce onderwijs is een van de centrale thema's in de NCCS2. Om de pool van cyberbeveiligingsexperts te vergroten en gebruikers beter te leren omspringen met cyberbeveiliging, hebben het bedrijfsleven en de overheid de handen in elkaar geslagen om de kwaliteit en het bereik van ICT-educatie op alle onderwijsniveaus (basis-, middelbaar en beroepsonderwijs) te verbeteren. Er is een Taskforce Cybersecurity Onderwijs opgezet als publiek-privaat partnerschap. Deze zal zich toeleggen op adviesverlening over het leerplan cyberbeveiliging, in verband met het erkennen van informatiebeveiligingsexperts en de nadere ontwikkeling van leermodules. Er wordt aansluiting gezocht bij lopende initiatieven over onderwijs in informatiewetenschappen en het Technologiepact 2020.

8.3. Preventie

Volgens de Nederlandse autoriteiten wordt van particulieren verwacht dat zij basale beveiligingsmaatregelen treffen en een zekere mate van persoonlijke verantwoordelijkheid nemen. De overheid en het bedrijfsleven van hun kant faciliteren dit door hun digitale vaardigheden te verbeteren en door hun zorgplicht jegens hun klanten zeer serieus te nemen. Dat betekent ook het aanbieden van veilige ICT-producten en -diensten. De overheid speelt een actievere rol in het cyberdomein. Dat gebeurt door enerzijds meer te investeren in de beveiliging van haar eigen netwerken en diensten en anderzijds de partijen samen te brengen en actie te ondernemen indien de beveiliging van bedrijven en particulieren of de privacy van laatstgenoemden wordt bedreigd. Waar nodig is de overheid norm- en kaderstellend opgetreden, bijvoorbeeld met betrekking tot de beveiligingseisen voor vitale diensten en processen.

Onderzoek en innovatie zijn een speerpunt van de Nationale Cybersecuritystrategie. Daaraan is invulling gegeven via:

- het onderhouden van relaties met de wetenschappelijke en onderzoeksinstituten;
- het initiëren en coördineren van onderzoek;
- het deelnemen aan onderzoek;
- het bevorderen van samenwerking op nationaal en internationaal vlak en tussen de private sector en onderzoeksinstellingen.

Zoals hierboven vermeld, is de Taskforce Cybersecurity Onderwijs een van de belangrijkste acties om de strategische doelen van NCSS2 te halen. Een ander centraal thema in de NCCS2 is innovatie. Er is behoefte aan een betere afstemming van vraag en aanbod, en daarin kan worden voorzien door innovatie-initiatieven te koppelen aan een leidende-sectorbeleid. Voorts zullen de overheid, het bedrijfsleven en de wetenschappelijke wereld een innovatieplatform voor cyberbeveiliging lanceren, waar starters, gevestigde bedrijven, studenten en onderzoekers met elkaar in verbinding kunnen treden, elkaar kunnen inspireren en vraag naar en aanbod van onderzoek op elkaar kunnen afstemmen waar het algemene onderwerpen als security by design and privacy by design betreft.

Om de veiligheid en het vertrouwen van burgers en de beveiliging en betrouwbaarheid van infrastructuur te vergroten is de National Cyber Security Research Agenda (NSCRA) opgesteld.
De doelen van de NCSRA zijn:

- verbeteren van de veiligheid van en het vertrouwen in ICT-infrastructuur en -diensten;
- Nederland voorbereiden op de veiligheidsuitdagingen van de komende 6-12 jaar;
- de Nederlandse cyber security economie stimuleren en innovatie in deze sector bevorderen;
- het Nederlandse onderzoek op beveiligingsgebied intensiveren en verbreden door samenwerking tussen onderzoeksinstituten en de betrokken publieke en private organisaties te bevorderen.

8.4. Conclusies

- Nederland lijkt een gemakkelijk toegankelijk opleidingsprogramma cybercrime voor rechters en aanklagers te hebben opgezet. Opleidingssessies worden regelmatig aangeboden op landelijk niveau bij het Studiecentrum Rechtspleging.

- Voorts heeft de rechterlijke macht geïnvesteerd in het opzetten van een Kenniscentrum Cybercrime bij het Gerechtshof in Den Haag, dat gespecialiseerde opleiding in cybercrime aanbiedt voor rechters, naar gelang van hun behoeften, en periodiek een nieuwsbrief publiceert om rechters meer bewust te maken van en beter bekend te maken met de meest recente trends, wetgeving en gebeurtenissen in verband met cybercriminaliteit.

- Het Openbaar Ministerie heeft een intern netwerk voor officieren van justitie opgezet, waar iedere aanklager die op een cybercrimezaak is gezet, kennis kan verwerven over onderwerpen in verband met cybercrime. De politie voorziet ook in specifieke opleiding voor digitaal rechercheurs.

- Naar de mening van de evalueerders zijn zowel initiatieven, zoals het Kenniscentrum Cybercrime, als het interne netwerk bij het Openbaar Ministerie nuttig om de kennis van de mensen in het veld over cybercriminaliteit te vergroten. Daarom moeten zij als beste praktijk worden beschouwd.

- Hoewel opleiding beschikbaar is voor alle belanghebbenden die over cybercrimezaken gaan, geschiedt deelname nog altijd op vrijwillige basis. Het evaluatieteam kreeg te horen dat de meeste rechters niet dagelijks met cybercrimezaken te maken krijgen, omdat niet veel zaken voor de rechter komen. Mede door algemene opleiding kunnen tegenstrijdige rechterlijke uitspraken, waarnaar tijdens het bezoek ter plaatse werd verwezen, worden voorkomen. Daarom zou deelneming vaker verplicht kunnen worden gesteld, althans voor rechters en aanklagers die met cybercriminaliteit en daaraan gekoppeld wederzijdse rechtshulp te maken kunnen krijgen.

- Voorts moet er volgens de evalueerders verdere opleiding worden aangeboden aan personeelsleden die meldingen registreren, en moeten zij ook bijgestaan worden door een ondersteuningsgroep voor digitaal onderzoek. Tijdens het bezoek ter plaatse werd een paar keer de mening geopperd dat politieagenten niet goed voorbereid zijn om die situaties zelfstandig op te lossen. De huidige methode behelst alleen dat de Regionale Ondersteuningsgroepen helpen op lokaal niveau, en dat is geen rechtstreekse en nuttige voorbereiding om met de situatie om te gaan. Ook kan de Regionale Ondersteuningsgroep met capaciteitsproblemen te maken krijgen indien het aantal klachten onverwacht toeneemt.

- Preventie en bewustmaking zijn samen met opleiding en capaciteitsopbouw enkele van de belangrijkste pijlers van de strategie, naast wetgeving en samenwerking. Aangezien het individu vaak de zwakste schakel is als het op cyberbeveiliging aankomt, komt men al een heel eind met effectieve preventie- en bewustmakingsmaatregelen. Er is een aantal praktische voorbeelden van gevallen waarin Nederland die maatregelen reeds heeft geïmplementeerd (bv. de "Hang op, klik weg, bel uw bank"- campagne van de Nederlandse Vereniging van Banken). Dit betekent ook dat de strategie actief wordt gebruikt en ten uitvoer gelegd.

- Het evaluatieteam realiseerde zich dat Nederland veel middelen heeft geïnvesteerd in bewustmakingscampagnes. Doel is bewustmaking van overheid, bedrijfsleven en burgers. Niet duidelijk was evenwel of er wel een omvattende communicatiestrategie is ontwikkeld om alle burgers te bereiken in situaties waarin ze mogelijk bedreigd worden door cybercriminaliteit.

9. SLOTOPMERKINGEN EN AANBEVELINGEN

9.1. Suggesties van Nederland

Vanuit Nederlands perspectief is er op drie punten verbetering nodig om de capaciteit voor het tegengaan van cybercriminaliteit te verhogen:

- meer internationale overeenstemming over jurisdictie in cyberspace;
- intensiveren van de internationale samenwerking in cybercrimezaken, bijvoorbeeld via Europol/EC3 en Interpol;
- zorgen voor capaciteitsopbouw in landen die doelwit en/of bron zijn van cybercrime, om hun capaciteit op peil te brengen en de gezamenlijke preventie-inspanningen en opsporingen te verbeteren.

9.2 Aanbevelingen

Wat de praktische tenuitvoerlegging en werking van het Kaderbesluit en de Richtlijnen betreft, heeft het deskundigenteam dat Nederland heeft geëvalueerd het Nederlandse systeem als bevredigend beoordeeld.

Nederland moet 18 maanden na de evaluatie de mate van opvolging van de aanbevelingen in dit rapport beoordelen en daarover rapporteren aan de Groep algemene aangelegenheden, waaronder evaluatie (GENVAL).

Het evaluatieteam achtte het zinvol de Nederlandse autoriteiten een aantal suggesties te doen. Voorts worden op basis van diverse beste praktijken soortgelijke aanbevelingen ook gedaan aan de EU, haar instellingen en agentschappen, Eurojust, Europol en Enisa.

9.2.1 Aanbevelingen aan Nederland

1. Nederland moet een mechanisme ontwikkelen om gedetailleerde, gestandaardiseerde en volledige statistieken te verstrekken over de opsporing, vervolging en veroordelingen en de gemelde incidenten in verband met cybercrime, zodat de totale cijfers over cybercrime op landelijk niveau getoetst kunnen worden; (zie 3.3 en 3.5)

2. Nederland moet overwegen de verplichting voor private bedrijven, zoals internetaanbieders, om cyberincidenten van criminele aard te melden, uit te breiden tot rechtshandhavende of andere overheidsinstanties en de mate van dwingendheid ervan te vergroten (zie 4.4.1 en 4.5)

3. Nederland moet worden aangespoord de politiehervorming op regionaal niveau af te ronden, zodat de regionale politie meer capaciteit krijgt om cybercriminaliteit te bestrijden, voldoende opgeleid is en over voldoende middelen beschikt; (zie 4.4.2, 4.5 en 6.4)

4. Nederland moet overwegen een gemeenschappelijke begripsomschrijving van cybercrime voor statistische doeleinden op te stellen, die moet worden toegepast opdat cybercrimebestrijders, zoals de rechtshandhavingsinstanties, het Openbaar Ministerie en de gerechten, in grote lijnen hetzelfde verstaan onder dat begrip ; (zie 5.1 en 5.5)

5. Nederland moet nagaan of de bescherming van overheidsinstanties en vitale nationale infrastructuur beter in evenwicht kan worden gebracht met de bescherming van de burgers, om de burgers weerbaarder te maken tegen cybercrime; (zie 6.1.2 en 6.4)

6. Nederland moet bekijken hoe de strategie inzake openbare communicatie kan worden verbeterd, zoals de strategie die wordt gevolgd bij het tegengaan van onlinekindermisbruik, zodat ook burgers worden bereikt die te lijden hebben onder verschillende vormen van cybercrime (zie 6.1.2 en 6.4)

7. Nederland moet een omvattend programma opstellen voor opleiding over cybercrime en over de mogelijkheden die Eurojust, Europol en Enisa in dat verband bieden ten behoeve van al wie bij de bestrijding van cybercrime betrokken is, waaronder politieagenten, officieren van justitie en rechters; (zie 4.5, 7.1.1, 7.6, 8.1 en 8.4)

9.2.2 Aanbevelingen aan de Europese Unie, aan haar instellingen en aan andere lidstaten

1. De lidstaten worden aangespoord om een consistente begripsomschrijving van cybercriminaliteit op te stellen die moet worden gehanteerd door al degenen die bij cybercrimebestrijding van betrokken zijn, om gedetailleerde, gestandaardiseerde en volledige statistieken over cybercrime te kunnen verstrekken; (zie 3.3, 3.5, 5.1 en 5.5)

2. De lidstaten moeten overwegen nuttige instrumenten te ontwikkelen om aanklagers en rechters die met cybercriminaliteit te maken hebben bij te staan en hun werk te vergemakkelijken. Voorbeelden zijn gespecialiseerde eenheden die zich met cybercrime bezighouden en/of een netwerk van aanklagers die deze zaken bij het Openbaar Ministerie behandelen, of een Kenniscentrum Cybercrime bij het gerechtshof in Den Haag; (zie 4.1.1, 4.5 en 8.1)

3. De lidstaten moeten streven naar oplossingen om de lacune op te vullen die is ontstaan door het ontbreken van wetgeving die het mogelijk maakt de locatie van gegevens in de cloud te bepalen en er toegang toe te verkrijgen; (zie 4.1.2, 5.4.3, 5.5 en 7.5.1)

4. De lidstaten moeten overwegen na te gaan of het voordelig en haalbaar is om het succesvolle voorbeeld van de ECTF in Nederland te volgen voor het doeltreffender bestrijden van digitale bankfraude, met name phishing en financiële malware; (zie 4.3, 5.1.2 en 6.4)

5. De lidstaten moeten overwegen tot een vorm van samenwerking met de private sector te komen met het oog op het beschermen van de vitale sectoren van hun land (energiebedrijven, en de telecommunicatie- en de financiële sector), zoals het NCSC in Nederland; (zie 4.3, 4.4.2, 4.5 en 6.1.2)

6. De lidstaten moeten overwegen de Nederlandse praktijk om de mogelijkheden van particuliere bedrijven (zoals internetaanbieders en socialemediabedrijven, overheidsinstanties (bv. het ministerie van Veiligheid en Justitie en gespecialiseerde eenheden die zich uitsluitend met het bestrijden van onlinemisbruik van kinderen bezighouden) en publieke campagnes te bundelen voor een effectieve bestrijding van online seksueel misbruik van kinderen, tot beste praktijk te verheffen; (zie 6.2.1 t/m 6.2.4 en 6.4)

7. De lidstaten moeten de mensen in het veld praktische richtsnoeren verstrekken inzake de bewustmaking van lokale autoriteiten (meer bepaald de rechtshandhavende instanties en het OM) omtrent de bevoegdheden en diensten van Eurojust, Europol en Enisa met betrekking tot cybercrime; (zie 4.5, 7.1.1, 7.6, 8.1 en 8.4)

8. De Europese instellingen moeten de EU-middelen voor cybercrimebestrijding vrijmaken en verhogen, bijvoorbeeld om via Eurojust GOT's in te stellen; (zie 3.4 en 7.1.3)

9.2.3 Aanbevelingen aan Eurojust/Europol/Enisa

1. Eurojust, Europol en Enisa moeten overwegen om de bekendheid met de diensten en de door hen geboden mogelijkheden tot samenwerking met betrekking tot cybercrime te vergroten; (zie 7.3 en 7.6)

2. Eurojust, Europol en Enisa moeten overwegen om evenementen die de internationale samenwerking bij het bestrijden van cybercrime ondersteunen, zoals de Global Cyber Space Conference, actief te steunen; (zie 7.3 en 7.6)

BIJLAGE A: PROGRAMMA VOOR DE BEZOEKEN TER PLAATSE EN GEÏNTERVIEWDEN/PERSONEN WAARMEE EEN ONTMOETING PLAATSVOND

7e Wederzijdse Evaluatie - Nederland – 17-21 NOVEMBER 2014

Maandag 17-11Den Haag

- PM aankomst GENVAL-experts in Den Haag (naar verwachting na de middag)
- Tussen 17.30 – 19.00 Informele ontmoeting en introducties in de hotelbar.

Dinsdag 18-11 Den Haag

- 9.00 – 9.30 Receptie op het Ministerie van Veiligheid en Justitie (Turfmarkt 147)
- 9.30 – 10.00 Welkomsttoespraak en inleiding door de heer Arie IJzerman, plaatsvervangend directeur-generaal, directeur Rechtspleging en Rechtshandhaving (DGRR)
- 10.00 -11.00 Nederlands strafrechtsysteem; inleiding en overzicht (Erik Planken van DGRR/DRC en Frans van de Doelen / Pim Albers van DGRR/DRB)
- 11.00-11.15 Koffiepauze
- 11.15-11.30 het gezelschap begeeft zich naar het Nationaal Cyber Security Centrum (in hetzelfde gebouw)
- 11.30-13.00 Bezoek Nationaal Cyber Security Centrum (NCSC): informatie over beleid en operationele taken (Michel van Leeuwen/Aart Jochem)
- 13.00-14.30 Lunch op het ministerie
- 14.30-15.30 Rechtshandhaving in Nederland (beleid ten aanzien van en bestuur van politie en OM (Jacos van Zelst van het Directoraat-Generaal Politie en Erik Planken van DGRR/DRC)
- 15.30-15.45 Koffiepauze
- 15.45 -16.45 Informatie over Nederlands justitieel raamwerk en het conceptwetsvoorstel ter uitbreiding van de rechtshandhavende bevoegdheden (Luut Mol Lous van de afdeling wetgeving)
- 17.00-17.30 Sluiting

Woensdag 19-11 Driebergen (Korps landelijke politiediensten; Dienst Nationale Recherche, Team High Tech Crime, Nationaal programma tegen seksueel misbruik van kinderen)

- 08.30- 10.00 reis naar Driebergen (er is vervoer geregeld)
- 10.00- 10.30 Verwelkoming en inleiding door de heer Wilbert Paulissen (hoofd van de Dienst Nationale Recherche van het Korps landelijke politiediensten)
- 10.30- 12.00 bezoek aan de Electronic crimes taskforce (ECTF) en inleiding in de Dienst Nationale Recherche door Eric van Schilt (projectleider (ECTF) en Michel Zandbergen (ABN/AMRO bank)
- 12.00 – 13.30 Lunch met de heer Wilbert Paulissen en teamleiders THTC
- 13.30-14.30 Inleiding tot het Team High Tech Crime ((THTU): organisatie, groei, taken en werkprocessen door outreach officers THTC (Peter Zinn THTU)
- 14.30 – 16.00 Bezoek aan werkstations THTC en informatie over de praktijk, werkprocessen, internationale samenwerking en zaken)
- 16.00 – 16.00 Informatie over de Nederlandse aanpak van seksueel misbruik van kinderen, online en offline, alsmede in andere landen door de heer Ben van Mierlo (Nationaal Programma kindermisbruik, NPKK)
- 17.00 -18.00 reis naar Den Haag (er is vervoer geregeld)
- 19.30- 22.00 Diner in aanwezigheid van de heer Jan Willem Schaper (directeur Politie bij het ministerie van Veiligheid en Justitie)

Donderdag 20-11 Rotterdam (Landelijk Parket, rechterlijke macht Nederland en de Rotterdamse regionale eenheid van de landelijke politie)

- 09.00- 10.00 reis naar Rotterdam (er is vervoer geregeld)
- 10.00 -10.30 Verwelkoming en inleiding door de heer Fred Westerbeke, hoofdofficier van justitie van het Landelijk Parket van het Openbaar Ministerie
- 10.30 – 11.45 Informatie door de heer Lodewijk van Zwieten, landelijk officier van justitie cybercrime over de Nederlandse praktijk, dilemma' s bij de vervolging, wederzijdse rechtshulp en internationale samenwerking

11.45 - 12.00 Koffiepauze

- 12.00 – 13.15 Informatie door de heer Christiaan Baardmans, rechter bij het gerechtshof in Den Haag en bij het Kenniscentrum Cybercrime
- 13.15 – 14.30 Lunch in het gebouw van het landelijk parket van het Nederlandse Openbaar Ministerie
- 15.00 – 17.30 Bezoek aan de regionale eenheid Rotterdam van de Landelijke Politie: informatie over praktijk, werkprocessen, internationale samenwerking en zaken (Erik Venema, Politie)
- 17.30 – 18.00 Sluiting, inventaris van mogelijke vervolginterviews op vrijdag 21
- 18.00- 19.00 reis naar Den Haag (er is vervoer geregeld)

Vrijdag 21-11 Den Haag

- 09.30 – 10.00 Start met koffie
- 10.00 - 12.30 besloten zitting voor GENVAL-experts en/of mogelijkheid voor nog meer gedachtewisseling, interviews, enz.
- PM 12.30 – 13.00 Sluiting met lichte lunch

-/-

BIJLAGE B: GEÏNTERVIEWDEN/PERSONEN MET WIE EEN ONTMOETING PLAATSVOND

Vergaderingen 18 november 2014

Locatie: ministerie van Veiligheid en Justitie, den Haag

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Arie IJzerman	ministerie van Veiligheid en Justitie
Erik Planken	ministerie van Veiligheid en Justitie
Michel van Leeuwen	Nationaal Cyber Security Centrum
Aart Jochem	Nationaal Cyber Security Centrum
Joost Raeven	ministerie van Veiligheid en Justitie
Barbara Perels	ministerie van Veiligheid en Justitie

Locatie: Directoraat-Generaal Politie, Den Haag

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Jacos van Zelst	Directoraat-Generaal Politie
Erik Planken	ministerie van Veiligheid en Justitie
Luut Mol Lous	ministerie van Veiligheid en Justitie

Vergaderingen 19 november 2014

Locatie: Politie, Dienst Nationale Recherche, Driebergen

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Inge Philips	Dienst Nationale Recherche
Eric van der Schild	Electronic Crimes Taskforce
Michel Zandbergen	ABN AMRO Bank
Roelandt van Zeijst	Team High Tech Crime
Marijn Schuurbiers	Dienst Nationale Recherche
Peter Zinn	Team High Tech Crime
Ben van Mierloo	Nationaal Programma tegen Kindermisbruik

Vergaderingen 20 november 2014

Locatie: Landelijk Parket, Rotterdam

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Sander de Haas	Openbaar Ministerie
Lodewijk van Zwieten	Openbaar Ministerie
Lisanne van Dijk	Openbaar Ministerie
Odette Zonneveld	Openbaar Ministerie
Christiaan Baardmans	Gerechtshof, Den Haag

Locatie: Regionale Eenheid Landelijke Politie, Rotterdam

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Rob Hokke	Landelijke Politie
Erik Venema	Landelijke Politie
Erik Planken	ministerie van Veiligheid en Justitie

Vergaderingen 21 november 2014

Locatie: ministerie van Veiligheid en Justitie, den Haag

Geïnterviewden/personen met wie een ontmoeting plaatsvond	**Organisatie die zij vertegenwoordigen**
Erik Planken	ministerie van Veiligheid en Justitie
Joost Raeven	ministerie van Veiligheid en Justitie

-/-

BIJLAGE C: LIJST VAN AFKORTINGEN/GLOSSARIUM VAN TERMEN

LIJST VAN ACRONIEMEN, AFKORTINGEN EN TERMEN	NEDERLANDS OF ACRONIEM IN ORIGINELE TAAL	NEDERLANDS OF ACRONIEM IN ORIGINELE TAAL	ENGELS
ACM	*ACM*		Autoriteit Consument & Markt
AIRS	*AIRS*	*Afdeling Internationale Rechtshulp in Strafzaken*	Office for International Legal Assistance in Criminal Matters
AIVD	*AIVD*		Openbaar Ministerie, Algemene Inlichtingen- en Veiligheidsdienst
CBS	*CBS*		Centraal Bureau voor de Statistiek
CBP	*CBP*	*College Bescherming Persoonsgegevens*	The Dutch Data Protection Agency
CSBN	*CSBN*		Cyber Security Beeld Nederland
Sv	*Sv*	*Wetboek van Strafvordering*	Dutch Code of Criminal Procedure
DefCERT	*DefCERT*		Defense CERT
DNB	*DNB*		De Nederlandsche Bank
FIOD	*FIOD*	*Fiscale inlichtingen- en opsporingsdienst*	Fiscal Information and Investigation Service
GovCert	*GovCert*		Computer Emergency Response Team van de Nederlandse overheid

IGCI	*IGCI*		Interpol Global Complex for Innovation
ISP	*ISP*		Internetdienstaanbieders
ITOM	*ITOM*		Illegale handel op onlinemarktplaatsen
NCC	*NCC*		Nationaal Crisiscentrum
NCSC	*NCSC*		Nationaal Cyber Security Centrum
NCTV	*NCTV*		Nationaal Coördinator Terrorismebestrijding en Veiligheid
THTC	*THTC*		Team High Tech Crime
NFI	*NFI*		Nederlands Forensisch Instituut
NRN	*NRN*		Nationaal Respons Netwerk
NVB	*NVB*	*Nederlandse Vereniging van Banken*	Dutch Banking Association
Kmar	*Kmar*		Koninklijke Nederlandse Marechaussee
SSR	*SSR*	*Studiecentrum Rechtspleging*	Training and study centre for the judiciary
Wbp	*Wbp*	*Wet bescherming persoonsgegevens*	The Dutch Data Protection Act
Wpg	*Wpg*	Wet politiegegevens	the Police Data Act
WWN	*WWN*		Watch and Warning Network

BIJLAGE D: NEDERLANDS WETBOEK VAN STRAFRECHT EN CYBERCRIMINALITEIT

Illegal access to information system = computervredebreuk		
Art. 2 Cybercrimeverdrag	Art. 3 EU-Richtlijn 2013/40	Art. 138ab, lid 1, Wetboek van Strafrecht
Gebruikte definitie	Hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan is schuldig aan computervredebreuk: Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven: a. door het doorbreken van een beveiliging, b. door een technische ingreep, c. met behulp van valse signalen of een valse sleutel, of d. door het aannemen van een valse hoedanigheid.	
Opzet of roekeloosheid	-/-	
Verzwarende/verzachtende omstandigheden	Verzwarende omstandigheid= 1. Indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt. 2. Computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens: a. met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk; b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.	
Minimum/maximumstraf	Max: gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (kan worden verhoogd tot twee jaar) Max: verzw. 1/2: gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Illegal system interference = stoornis in een geautomatiseerd werk veroorzaken		
Art. 5 Cybercrimeverdrag	Art. 4 EU-Richtlijn 2013/40	Art. 138b, art. 350a Wetboek van Strafrecht, en art. I, lid G, conceptvoorstel voor nationale uitvoeringsrichtlijn
Gebruikte definitie	(138b) Hij die opzettelijk en wederrechtelijk de toegang tot en het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden (350a) 1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt G, conceptvoorstel voor nationale uitvoeringsrichtlijn Na artikel 350b worden twee artikelen ingevoegd, luidende: (Artikel 350c) 1. Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens of stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst, ontstaat. 2. Artikel 138b, tweede en derde lid, is van overeenkomstige toepassing.	
Opzet of roekeloosheid	- opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	Verzwarende omstandigheid= 1. Hij die het feit, bedoeld in het eerste lid, pleegt na wederrechtelijk te zijn binnengedrongen en ernstige schade met betrekking tot die gegevens veroorzaakt 2. die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten Verzachtende omstandigheid= Degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken	

Minimum/maximumstraf	Max: bij stoornis) = gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (kan worden verhoogd tot twee jaar) Bij veranderen, wissen enz.: gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. Max: verzw. 1/2: gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie Verzachtende omstandigheid = is niet strafrechtelijk aansprakelijk
Veelpleging/recidive	Zie algemene regels
Aanzetten, medeplichtigheid en poging	Zie algemene regels en huidig art. 139d, lid 2 Hij die: a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft; met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c wordt gepleegd, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie. G, conceptvoorstel voor nationale uitvoeringsrichtlijn (Artikel 350d) hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 350a, eerste lid, of 350c wordt gepleegd: a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

<table>
<tr><td colspan="3">Illegal data interference = opzettelijk vernielen, verstoren of onbruikbaar maken van computers of computernetwerken</td></tr>
<tr><td>Art. 4 Cybercrimeverdrag</td><td>Art. 5 EU-Richtlijn 2013/40</td><td>Art. 350a Nederlands Wetboek van Strafrecht (NB hoe zit het met 350b???)</td></tr>
<tr><td>Gebruikte definitie</td><td colspan="2">(350a)
1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt
(350b)
1 Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt,
2 Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt,
G, conceptvoorstel voor nationale uitvoeringsrichtlijn
Na artikel 350b worden twee artikelen ingevoegd, luidende:
(Artikel 350c)
1. Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens of stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst, ontstaat.
2. Artikel 138b, tweede en derde lid, is van overeenkomstige toepassing.</td></tr>
<tr><td>Opzet of roekeloosheid</td><td colspan="2">- opzet wordt vermoed in artikel 350a
- nalatigheid wordt vermoed in artikel 350b</td></tr>
<tr><td>Verzwarende/verzachtende omstandigheden</td><td colspan="2">Verzwarende omstandigheid=
1. Hij die het feit, bedoeld in het eerste lid, pleegt na wederrechtelijk te zijn binnengedrongen en ernstige schade met betrekking tot die gegevens veroorzaakt
2. die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten.
Verzachtende omstandigheid=
Degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken</td></tr>
</table>

Minimum/maximumstraf	350a Max: gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie Max: verzw. 1/2: gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie Verzachtende omstandigheid = is niet strafrechtelijk aansprakelijk 350b Max: gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie
Veelpleging/recidive	Zie algemene regels
Aanzetten, medeplichtigheid en poging	Zie algemene regels en artikel 350a, lid 3 Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

Illegal interception of computerdata = onrechtmatige onderschepping / gegevensdiefstal		
Art. 3 Cybercrimeverdrag	Art. 6 EU-Richtlijn 2013/40	Art. 139c en 139d Nederlands Wetboek van Strafrecht
Gebruikte definitie	(139c) Hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk. Geen aansprakelijkheid in de volgende gevallen: • door middel van een radio-ontvangapparaat ontvangen gegevens • door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting • ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de Inlichtingen- en veiligheidsdiensten 2002. (139d, eerste lid) Hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn	
Opzet of roekeloosheid	opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	-/-	
Minimum/maximumstraf	Max: gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (kan worden verhoogd tot twee jaar)	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Misuse of devices = instrumenten voor het plegen van strafbare feiten / voorbereidingshandelingen onderschepping		
Art. 6 Cybercrimeverdrag	Art. 7 EU-Richtlijn 2013/40	Art. 139d Wetboek van Strafrecht
Gebruikte definitie	(139d, tweede lid) Hij die: a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft;	
Opzet of roekeloosheid	opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	Hij die het genoemde misdrijf heeft gepleegd (1) met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c wordt gepleegd (2) met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138b, tweede of derde lid, wordt gepleegd,	
Minimum/maximumstraf	Max: gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (kan worden verhoogd tot twee jaar) Verzw. 1: zelfde straf als in artikel 138ab, eerste lid, 138b of 139c =; gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie Verzw. 2: wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Computer-related production, distribution or possession of child pornography = kinderporno		
Art. 9 Cybercrimeverdrag	Art. 5 EU-Richtlijn 2011/92	Art. 240b Wetboek van Strafrecht
Gebruikte definitie	Degene die een afbeelding - of een gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezet heeft of zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft	
Opzet of roekeloosheid	-/-	
Verzwarende/verzachtende omstandigheden	Verzwarende omstandigheid= Degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of een gewoonte maakt (1	
Minimum/maximumstraf	Max: gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie Max: verzw. 1: gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Computer-related solicitation or grooming of children = grooming / kinderlokken on line		
Art. 23 Verdrag van Lanzarote	Art. 6 EU-Richtlijn 2011/92	Art. 248e Wetboek van Strafrecht
Gebruikte definitie	Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een persoon van wie hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van zestien jaren nog niet heeft bereikt, een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met die persoon te plegen of een afbeelding van een seksuele gedraging waarbij de persoon is betrokken, te vervaardigen, indien hij enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting	
Opzet of roekeloosheid	-/-	
Verzwarende/verzachtende omstandigheden	-/-	
Minimum/maximumstraf	Max: gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Computer-related fraud or forgery = computergerelateerde fraude en oplichting		
Art. 7, 8 Cybercrimeverdrag		Artikelen 326/225 (phishing, fraude op online marktplaatsen, voorschotfraude, “clickfraude"), 232 (skimmen), 310 (diefstal van virtuele goederen) 317/318/285 (verduistering, / afpersing), 334 (marktmanipulatie), 139e (heling) van het Wetboek van Strafrecht
Gebruikte definitie	(326) Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een schuld; (232) • Hij die opzettelijk een betaalpas, waardekaart, enige andere voor het publiek beschikbare kaart of een voor het publiek beschikbare drager van identiteitsgegevens, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, • Hij die opzettelijk gebruik maakt van de valse of vervalste pas of kaart als ware deze echt en onvervalst, dan wel opzettelijk zodanige pas of kaart voorhanden heeft, ontvangt, zich verschaft, vervoert, verkoopt of overdraagt, terwijl hij weet of redelijkerwijs moet vermoeden dat de pas of kaart bestemd is voor zodanig gebruik (310) Hij die enig goed dat geheel of ten dele aan een ander toebehoort wegneemt, met het oogmerk het zich wederrechtelijk toe te eigenen	
Opzet of roekeloosheid	opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	(326) Indien het feit wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken	
Minimum/maximumstraf	Max: (326) gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie Verzw.: de op het feit gestelde gevangenisstraf wordt met een derde verhoogd (232) gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie (310) gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Controlling or sending spam = spam		
Art. 7, 8 Cybercrimeverdrag		art. 11, lid 7 Wet Telecommunicatie)
Gebruikte definitie	NB strafbaarstelling Tw opzoeken (contact met OPTA???)	
Opzet of roekeloosheid	opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	(225) Indien het feit wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken	
Minimum/maximumstraf	Max: (225) gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie Verzw.: de op het feit gestelde gevangenisstraf wordt met een derde verhoogd .	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	

Computer-related identity fraud = identiteitsfraude		
Art. 7, 8 Cybercrimeverdrag		Artikelen 326/225 (phishing, fraude op onlinemarktplaatsen, voorschotfraude, “click”-fraude
Gebruikte definitie	(225) • Hij die een geschrift dat bestemd is om tot bewijs van enig feit te dienen, valselijk opmaakt of vervalst, met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken • Hij die opzettelijk gebruik maakt van het valse of vervalste geschrift als ware het echt en onvervalst, dan wel opzettelijk zodanig geschrift aflevert of voorhanden heeft, terwijl hij weet of redelijkerwijs moet vermoeden dat dit geschrift bestemd is voor zodanig gebruik (326) Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een schuld; Er is geen specifiek artikel over identiteitsfraude door het gebruiken van de legitimatiebewijzen van iemand anders. In die gevallen wordt artikel 326 gebruikt.	
Opzet of roekeloosheid	opzet wordt vermoed	
Verzwarende/verzachtende omstandigheden	(225) Indien het feit wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken	
Minimum/maximumstraf	Max: (225) gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie Verzw.: de op het feit gestelde gevangenisstraf wordt met een derde verhoogd .	
Veelpleging/recidive	Zie algemene regels	
Aanzetten, medeplichtigheid en poging	Zie algemene regels	