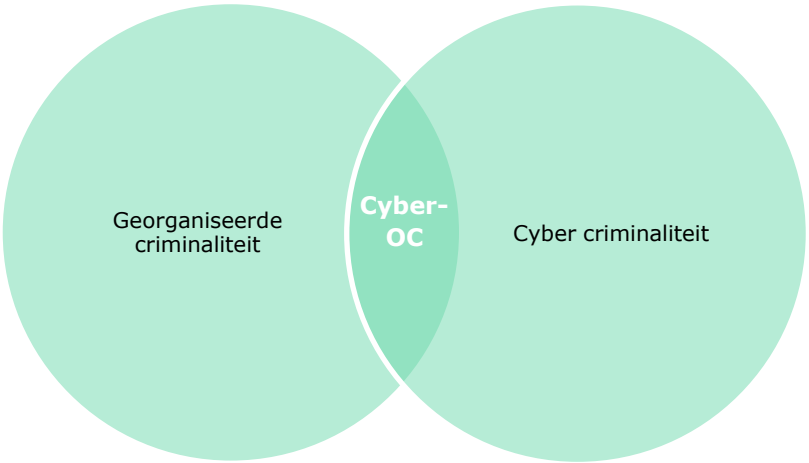
Samenvatting

Georganiseerde Cybercrime in Nederland
Empirische bevindingen en implicaties voor de rechtshandhaving

Doel van het onderzoek

De toename van cybercriminaliteit en de verhoogde kwetsbaarheid om hier slachtoffer van te worden, is een zorg binnen de samenleving, van de rechtshandhaving en van beleidsmakers. Over de aard en de organisatie van deze criminaliteit is echter nog niet veel informatie beschikbaar. Dit onderzoek richt zich op de vraag hoe criminele samenwerkingsverbanden op, via en tegen het internet te werk gaan. We hebben ons daarbij gericht op kenmerken van de verdachten, hun organisatorische structuren en modus operandi. We hebben ook gekeken naar de manier waarop (georganiseerde) cybercriminaliteit wordt opgespoord en op de kansen en knelpunten die hierbij bestaan. Met de term 'cyber-OC' ofwel 'Cyber Organised Crime' (zie ook Bulanova-Hristova et al., 2016) doelen we op de overlap tussen de georganiseerde criminaliteit en cybercrime, met andere woorden, de *link* tussen en het samengaan van cybercrime en georganiseerde criminaliteit.



Andere doelstellingen van het onderzoek waren het verkennen van de volgende vragen: In hoeverre biedt het internet nieuwe 'windows of opportunity' voor illegale activiteiten en voor het vinden en benaderen van nieuwe slachtoffers?; In hoeverre heeft het internet geleid tot structurele veranderingen in de georganiseerde criminaliteit?

Onderzoeksmethoden: politiedossiers en interviews

Om de onderzoeksvragen te beantwoorden, zijn verschillende onderzoeksmethoden gebruikt. Er is een analyse gemaakt van politiedossiers van opsporingsonderzoeken naar georganiseerde cybercriminaliteit. Wij hebben hiervoor elf afgeronde opsporingsonderzoeken geselecteerd. De verdachten in deze zaken waren actief in ver-

schilende vormen van cybercriminaliteit: het verspreiden van malware, hacking, het runnen van botnets, phishing, misbruik van het bankwezen, het (digitaal) witwassen van geld en illegale online handel. Bijna alle zaken (tien) zijn inmiddels voor de rechter geweest en hebben geleid tot veroordelingen. Het opsporingsonderzoek van de onderzochte zaken heeft gelopen tussen 2009 en 2014. De politiedossiers van de elf opsporingsonderzoeken bevatten gegevens over in totaal 107 verdachten.
Naast de studie van politiedossiers, interviewden we twaalf functionarissen van politie en justitie om informatie te verzamelen. Dit betroffen officieren van justitie, politieagenten van de opsporingsteams, en vertegenwoordigers van de *Electronic Crimes Task Force* en van Europol. De gegevens zijn verzameld in het kader van een internationaal onderzoeksproject gefinancierd door de Europese Commissie (voor de eerdere publicatie op basis van deze data zie Bulanova-Hristova et al., 2016).[43]

Resultaten: de traditionele groepen en nieuwe allianties

In de geanalyseerde zaken zien we enerzijds traditionele criminele groepen die betrokken raken bij cybercrime om hun (traditionele) criminele activiteiten efficiënter of geavanceerder uit te voeren. Het gaat dan bijvoorbeeld om de online verkoop van drugs, of om het gebruik van het internet of encryptie bij hun 'interne' communicatie. Anderzijds zien we nieuwe groepen die specifieke cyber-gerelateerde criminele activiteiten ontwikkelen. Het gaat hier dus in feite om nieuwe vormen van criminaliteit, zoals DDoS-aanvallen, het verspreiden van malware en ransomware.

Nieuwe mogelijkheden: nieuwe ideeën, nieuwe slachtoffers

Ontwikkelingen op het gebied van internet en informatie- en communicatie technologieën zorgen voor nieuwe vormen en uitvoeringsmogelijkheden van criminaliteit. Het gaat dan bijvoorbeeld om anonimiteit, crime-as-a-service en de mogelijkheid om fora te gebruiken. Daarnaast zorgen deze ontwikkelingen voor nieuwe manieren om slachtoffers te bereiken; voor meer efficiëntie in de uitvoering; en voor een vergroting van de financiële opbrengst van criminaliteit. Deze ontwikkelingen zorgen ervoor dat criminaliteit waarbij coördinatie van verschillende activiteiten is vereist, in feite eenvoudiger en toegankelijker lijkt te zijn geworden voor grotere groepen mensen. Dit leidt, afgezien van veranderingen in de modus operandi en de veranderingen in de toegang tot slachtoffers, tot (1) nieuwe spelers in het veld, (2) nieuwe vormen van samenwerking en (3) nieuwe economische structuren.

1 Nieuwe faciliteerders

Een voorbeeld van nieuwe spelers zijn faciliteerders die bewust of onbewust en gewild of ongewild criminaliteit faciliteren. Zij bestaan onder meer uit technisch geschoolde mensen, en (legitieme) bedrijven (private partijen), zoals hosting providers, online reclamebureaus/advertentiebedrijven, webshops, koeriersbedrijven (postbedrijven) en telecommunicatiebedrijven. Daarnaast komen we faciliteerders tegen die helpen om zaken af te schermen, zoals dekmantel-ondernemingen, *bitcoin* handelaren en *money mules*. Deze faciliteerders zijn niet dezelfde partijen als partijen die actief zijn in offline georganiseerde misdaad. Deze nieuwe spelers bieden nieuwe mogelijkheden voor de aanpak en preventie van cybercrime en voor het

[43] EU Project: Bulanova-Hristova et al. (2016) (HOME/2012/ISEC/AG/4000004382).

betrekken van deze partijen, bijvoorbeeld binnen publiek-private samenwerkingsverbanden.

2 Samenwerking en organisatie

De manier waarop verdachten met elkaar samenwerken is voor een deel vergelijkbaar met andere vormen van georganiseerde misdaad. De overeenkomsten zijn:

- *Dynamische netwerken*: criminele samenwerkingsverbanden zijn veranderlijk qua samenstelling.
- *Gebaseerd op sociale relaties*: criminele samenwerkingsverbanden zijn gebaseerd op familiebanden, vriendschappen en andere offline en online relaties.

Er zijn ook aspecten van de georganiseerde cybercriminaliteit die enigszins verschillen van andere vormen van georganiseerde misdaad:

- *Anonimiteit in cyberspace*: online activiteiten kunnen anoniem worden uitgevoerd, en offline contact tussen 'partners in crime' is niet perse nodig om online (criminele) activiteiten te plegen. Dit maakt samenwerking minder risicovol en verandert de rol van vertrouwen binnen de criminele samenwerking.
- *Crime as a service*: bepaalde taken kunnen online worden gekocht als diensten, wat de organisatie van cybercrime een nieuwe of andere dimensie geeft. ICT-geschoolde mensen kunnen hun diensten verkopen aan anderen die online of offline actief zijn. Binnen deze 'samenwerking', ondernemen verschillende individuen specifieke activiteiten en er is geen echte noodzaak om offline contact met elkaar te hebben.
- *De rol van fora*: online fora waar wordt gecommuniceerd over cybercriminaliteit lijken te fungeren als ontmoetingsplaatsen en als communicatiekanalen voor het delen en verkrijgen van informatie en het leggen van contacten met betrekking tot criminele activiteiten (op het internet). Ze bevorderen de samenwerking tussen de verdachten en leiden tot de vorming van nieuwe samenwerkingen tussen verdachten die actief zijn op deze fora. Op deze manier kunnen verdachten online relaties opbouwen, samenwerken en communiceren zonder elkaar offline te hoeven ontmoeten. Deze kanalen worden gebruikt voor de verkoop en het delen van kennis, software, scripts, goederen, producten en ruw materiaal. Het feit dat online communicatiediensten encryptie gebruiken en de gebruiker vaak anoniem kan blijven door het gebruik van anonimiserings-software, blijkt een belangrijke motivatie te zijn om deze fora te gebruiken in plaats van meer traditionele communicatiekanalen.

Ketenstructuren: verdeelde verantwoordelijkheden en de rol van vertrouwen

Verder lijken nieuwere groepen binnen cybercriminaliteit, in tegenstelling tot de meer traditionele georganiseerde misdaad groepen, te verschillen als het gaat om hun lange termijn perspectief binnen de samenwerking. Hoewel individuen wel een lange termijn perspectief hebben ten aanzien van hun eigen activiteiten, zijn de nieuwe samenwerkingsverbanden vaak minder stabiel en kennen zij in mindere mate een lange termijn perspectief ten aanzien van het gezamenlijk uitvoeren van illegale activiteiten. Anders dan bij traditionele georganiseerde criminaliteit waar vertrouwen tussen samenwerkende verdachten een belangrijke rol speelt, lijkt het bij online samenwerkingsverbanden minder noodzakelijk te zijn om een stabiele groep te vormen. De kwaliteit van iemands kennis en kunde speelt een belangrijkere rol. De anonimiteit van online samenwerking, maakt deze samenwerking minder riskant, waardoor het opbouwen van vertrouwen tussen verdachten binnen deze cyber-OC-groepen minder belangrijk is. Binnen deze lossere netwerken kan samenwerking tussen verdachten de vorm hebben van een keten, waarbinnen mensen die betrokken zijn bij verschillende activiteiten aan elkaar gekoppeld zijn,

en waarvan de verschillende activiteiten samen een strafbaar feit opleveren. In deze keten-achtige samenwerkingen, werken verdachten wel met elkaar samen, maar zijn zij slechts verantwoordelijk voor één onderdeel van de criminele activiteit. Als gevolg hiervan kunnen verdachten betrokken zijn bij georganiseerde criminaliteit, zonder precies te weten van welke misdaden hun activiteiten onderdeel uitmaken. Binnen deze keten-achtige structuren heeft elke verdachte in zekere zin macht, en elke verdachte heeft een bepaalde rol, maar tegelijkertijd lijkt iedereen of juist niemand verantwoordelijk te zijn voor de misdaad als geheel. Dit lijkt een nieuw kenmerk van georganiseerde criminaliteit op het terrein van cybercrime, wat een verandering zou betekenen voor de inhoud van het concept georganiseerde criminaliteit. In zo'n ketenstructuur kunnen de verschillende spelers voor zichzelf bezig zijn en individuele doelen hebben. Samen bereiken ze een georganiseerde vorm van criminaliteit, niet zozeer van bovenaf georganiseerd maar veeleer bottom-up ontstaan. Op deze manier lijken zowel de criminele activiteiten als de groepen van samenwerkende personen min of meer op toevallige wijze te ontstaan en bepaalde vormen aan te nemen.

Deze ontwikkelingen maken dat cyber-OC zowel kan worden gepleegd op basis van onderlinge afspraken tussen verdachten (die elkaar kennen en samenwerken aan een bepaald project, op basis van een bepaalde verdeling van taken) of juist in de vorm van de hierboven geschetste ketenstructuur, dus zonder duidelijke coördinatie. Er bestaat dus diversiteit waardoor het moeilijk kan zijn om criminaliteit aan specifieke criminele groepen of organisaties toe te wijzen en om te voorspellen hoe criminaliteitsvormen zich ontwikkelen.

3 Nieuwe economische structuren

Het gebruik van cryptocurrencies om geld te versturen of om geld wit te wassen via het internet hebben geleid tot het ontstaan van nieuwe economische structuren. Deze nieuwe vormen van ondergronds bankieren vormen structuren die moeilijk te controleren zijn. Het is interessant om na te gaan in hoeverre regels, meldingssystemen en controlerende instanties op het gebied van ongebruikelijke transacties ook gelden en gebruikt kunnen worden voor cryptocurrencies.

De opsporing van georganiseerde cybercriminaliteit

Het speciale cybercrime team van de Nederlandse Politie – het Team High Tech Crime – is de afgelopen jaren hard gegroeid. Dit betekent dat capaciteit en expertise is vrijgemaakt en gereserveerd voor de opsporing van cybercrime zaken. Cybercrime neemt echter toe en de politie is genoodzaakt om prioriteiten te stellen bij het signaleren en opsporen van zaken.

Bijzondere opsporingsbevoegdheden

Het brede scala aan geavanceerde technische mogelijkheden om anoniem te handelen op het internet, maken dat bijzondere opsporingsbevoegdheden worden ingezet om de identiteit van verdachten te kunnen achterhalen. Deze opsporingsbevoegdheden worden zowel online als offline toegepast. Het nieuwe wetsvoorstel Computercriminaliteit III biedt de politie nieuwe onderzoeksinstrumenten, en creëert mogelijkheden om de toegang tot informatie te krijgen voordat de informatie gecodeerd wordt.

Informatiepositie op internet
Om grip te krijgen op traditionele georganiseerde criminele groepen, beschikt de Nederlandse politie over een speciale eenheid, de Criminele Inlichtingen Eenheid (CIE). Rechercheurs van de CIE kunnen undercover samenwerken met mensen in een criminele groep en op deze manier informatie vergaren over criminele activiteiten. Deze informatie wordt vaak gebruikt als een startpunt voor een strafrechtelijk onderzoek. Een soortgelijke eenheid voor de online criminele wereld bestaat echter nog niet. Als gevolg daarvan heeft het Team High Tech Crime nog geen vergelijkbare informatiepositie in de internetgemeenschap. Verschillende geïnterviewden zijn van mening dat de ontwikkeling van een dergelijke informatiepositie in de toekomst waardevol zou zijn in de strijd tegen cybercriminaliteit.

Internationale samenwerking
Aangezien een verdachte op het internet zich overal ter wereld kan bevinden, vergt het identificeren, lokaliseren, arresteren en uiteindelijk veroordelen van verdachten vaak een intensieve internationale samenwerking. Onze geïnterviewden zijn positief over de faciliterende rol van Europol bij internationale samenwerking, al lijkt het succes van Joint Investigation Teams sterk afhankelijk van de capaciteit en prioriteiten in de samenwerkende landen. Binnen politie onderzoeken die niet de formele status van een JIT hebben, zijn rechtshulpverzoeken nodig om hulp of informatie te krijgen uit andere jurisdicties. Door verschillende prioriteiten, ingewikkeld papierwerk of procedures, worden deze verzoeken vaak behandeld met een tempo dat onverenigbaar is met de snelheid van het internet. Het overwinnen van dit soort problemen zou winst kunnen opleveren in de opsporing van (georganiseerde) cybercrime.