Cybercrime en gedigitaliseerde criminaliteit

Inleiding

Er is een heel scala aan actoren actief in cyberspace die een dreiging vormen voor de cybersecurity. Dat zijn onder meer beroepscriminelen, statelijke actoren, terroristen, hacktivisten en cybervandalen. De groeiende dreiging voor de cybersecurity van Nederland wordt volgens het *Cybersecuritybeeld Nederland 2016* van het Nationaal Cyber Security Centrum vooral veroorzaakt door beroepscriminelen en statelijke actoren. Dit hoofdstuk richt zich voornamelijk op de groeiende dreiging die uitgaat van beroepscriminelen die zich bezighouden met cybercrime en gedigitaliseerde criminaliteit. Criminaliteit gepleegd door statelijke actoren, terroristen, hacktivisten en cybervandalen komt slechts zijdelings aan bod, omdat deze niet tot het domein van georganiseerde criminaliteit behoort. Voor het domein van terrorisme en spionage zijn er rapportages van de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de Algemene Inlichtingen- en Veiligheidsdienst en het Nationaal Cyber Security Centrum die voorzien in de kennis- en informatiebehoefte.

De groeiende interesse van beroepscriminelen voor cybercrime en digitalisering van commune delicten (gedigitaliseerde criminaliteit) past in de algemene tendens van toenemende digitalisering in de samenleving. Geavanceerde digitale mogelijkheden zijn voor iedereen toegankelijk en te gebruiken zonder veel voorkennis. Rode draad binnen deze mogelijkheden zijn de steeds betere encryptietechnieken, die zorgen voor een steeds betere beveiliging (cybersecurity) van zowel legale als illegale handelingen en activiteiten. Aan criminelen bieden ze de kans anoniem te opereren en zich af te schermen voor opsporingsactiviteiten.

De basis voor dit hoofdstuk vormt het (vertrouwelijke) rapport *Cybercrime en gedigitaliseerde criminaliteit. Nationaal dreigingsbeeld 2017.* De auteurs van het onderzoeksrapport zijn Kristiaan Schuppers, Nikita Rombouts, Peter Zinn en Hielke Praamstra, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.

Er wordt in het onderzoek onderscheid gemaakt tussen cybercrime en gedigitaliseerde criminaliteit. Bij cybercrime gaat het om criminaliteit waarbij informatie- en communicatietechnologie (ICT) zowel het middel als het doelwit is. Cybercrime kent technieken en middelen enerzijds en verschijningsvormen anderzijds. Bij technieken en middelen gaat het om hacken, malware, botnets, DDoS-aanvallen en *social engineering.* Bij verschijningsvormen gaat het om het doel waarmee de technieken en middelen worden ingezet, zoals verstoring van ICT, afpersing, diefstal van datasets met persoonsgegevens en fraude met betaalmiddelen.

Sommige varianten van cybercrime worden hightechcrime genoemd, hoofdzakelijk vanwege het innovatieve en ondermijnende karakter. Tot deze hightechcrimevarianten van cybercrime behoren aanvallen op vitale infrastructuren, aanvallen op het financiële stelsel, bedrijfsspionage en hacktivisme. Hoewel deze varianten deels niet tot het domein van de georganiseerde criminaliteit behoren, wijden wij er in dit hoofdstuk wel aandacht aan vanwege hun innovatieve karakter en mogelijke implicaties voor cybercrime en gedigitaliseerde criminaliteit.
Bij gedigitaliseerde criminaliteit is ICT een middel om (traditionele vormen van) criminaliteit te plegen. ICT kan een rol spelen in elk van de fasen van het criminele proces, bij zowel de voorbereiding als de uitvoering als de afronding. Zo kunnen de sociale media dienen als ontmoetingsplaats, het darkweb als handelsplaats en kan witwassen plaatsvinden met behulp van bitcoins. Digitale technologie vergroot de reikwijdte van criminelen en biedt goede mogelijkheden om criminele activiteiten af te schermen voor opsporing en justitie.

In de praktijk is het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit niet zo strikt. Er is sprake van een steeds sterkere verweving tussen cybercrime, gedigitaliseerde criminaliteit en traditionele vormen van criminaliteit. Binnen het domein van georganiseerde criminaliteit is het gebruik van digitale technologie in al haar facetten eerder een thema-overstijgende werkwijze dan dat er sprake is van nieuwe digitale vormen van georganiseerde criminaliteit.

In dit hoofdstuk wordt een beeld gegeven van de ontwikkelingen die de afgelopen jaren bij cybercrime en gedigitaliseerde criminaliteit hebben plaatsgevonden en van de invloed die deze ontwikkelingen hebben gehad op de (daders van) georganiseerde criminaliteit. Daarnaast worden verwachtingen geformuleerd voor de komende jaren: wat te verwachten ontwikkelingen op het gebied van ICT zijn, hoe die zich verhouden tot de georganiseerde criminaliteit en welke mogelijke gevolgen dat heeft voor de Nederlandse samenleving.

Ontwikkelingen van cybercrime en gedigitaliseerde criminaliteit

De huidige tijd kenmerkt zich door de snelle opeenvolgende ontwikkelingen van digitale technologie, ontwikkelingen die invloed hebben op de hele samenleving, het criminele deel incluis. In het Nationaal dreigingsbeeld van 2004 werd de invloed van deze nieuwe ontwikkelingen op de georganiseerde criminaliteit vooralsnog beperkt geacht. De nieuwe mogelijkheden werden destijds voornamelijk gebruikt om te communiceren. Wel werd verwacht dat criminele samenwerkingsverbanden in toenemende mate gebruik zouden gaan maken van de mogelijkheden op dit vlak, bijvoorbeeld om afgeschermd te communiceren. De ontwikkelingen bleken sneller te gaan dan destijds verwacht werd. In het NDB2008 speelde bij meerdere onderwerpen internet al een belangrijke rol en niet uitsluitend als communicatiemiddel. Onderwerpen die voorbijkwamen, waren onder andere virtuele seks, witwassen en de verkoop van kweekbenodigdheden voor hennepkwekerijen via internet.

De verwachting in 2008 was dat de digitalisering van het criminele bedrijf gelijke tred zou houden met de digitalisering in de samenleving. Die verwachting is tot op heden bewaarheid. In het NDB2012 werd de digitale technologie als alomtegenwoordig beschouwd en voor het huidige NDB geldt hetzelfde, met de toevoeging dat digitale technieken tegenwoordig geraffineerder en professioneler gebruikt worden dan voorheen.

Cybercrime

Afpersing

Cybercrime wordt steeds agressiever en ook wordt steeds directer de confrontatie aangegaan met slachtoffers. Het gaat dan vooral om afpersing waarbij de computer van een slachtoffer versleuteld wordt door *ransomware.* Daardoor kan het slachtoffer niet meer bij zijn persoonlijke gegevens. Het slachtoffer wordt gevraagd te betalen voor de sleutel om weer toegang te krijgen tot zijn informatie. Slachtoffers worden op slinkse wijze verleid om bijvoorbeeld te klikken op besmette hyperlinks op internetpagina's of in mailtjes. Sinds 2013 worden zowel particulieren als bedrijven in toenemende mate slachtoffer van ransomware. Ransomware wordt over het algemeen ongericht verspreid maar soms ook gericht naar specifieke bedrijven.

Vooral het midden- en kleinbedrijf (MKB) en (semi)overheidsorganisaties zijn kwetsbaar, omdat hun ICT niet altijd up-to-date is en vaak slecht beveiligd. Zo zijn ziekenhuizen in de Verenigde Staten en Duitsland slachtoffer geworden van afpersing via ransomware. Bij Nederlandse ziekenhuizen is dit – voor zover bekend – nog niet voorgekomen, maar het wordt door experts wel mogelijk geacht dat ook zij hiermee geconfronteerd zullen worden. De aangiftebereidheid bij bedrijven is laag, omdat bedrijven weinig vertrouwen hebben in de wijze waarop de aangiften door de politie worden opgepakt. Bovendien zijn ze bang voor reputatieverlies. Door de geringe aangiftebereidheid ontbreekt een goed zicht op de omvang van aanvallen met ransomware.

Behalve ransomware worden ook DDoS-aanvallen gebruikt voor afpersingsdoeleinden. Door het gebruik van DDoS wordt een website onbereikbaar. Vooral websites waar transacties worden gedaan zijn slachtoffer, zoals webshops, financiële websites en websites van de reisbranche.

Fraude

Uit de onderzoeken naar horizontale fraude blijkt dat de digitale ontwikkelingen gretig omarmd zijn bij het plegen van fraude (zie ook deel 2, Fraude en witwassen). Bij meerdere verschijningsvormen van horizontale fraude spelen een of meer cybercrime-elementen een duidelijke rol: fraude met internetbankieren, fraude met creditcardgegevens, fraude met online handel, factuurfraude en CEO-fraude. De cybercrime-elementen waar het om gaat, zijn het gebruik van malware en hacking. Ook de werkwijzen phishing en social engineering spelen bij deze fraudevormen een rol.

Bij fraude met internetbankieren werd in 2012 vooral gebruikgemaakt van *banking malware* waarbij de directe communicatie tussen bank en klant vervangen werd door een communicatie tussen klant-crimineel-bank, het zogenoemde *man-in-the-middle*-principe. Dat is sinds die tijd flink afgenomen, omdat de geautomatiseerde detectie van malware bij banken sterk is verbeterd. Tegenwoordig wordt vooral phishing (zonder malware) gebruikt. Mensen worden er via een mail toe verleid naar een bepaalde website te gaan, waar naar hun inloggegevens wordt gevraagd. Ook dat is de laatste jaren afgenomen. Volgens experts is dat te danken aan een betere detectie en opsporing van netwerken van moneymules (geldezels). Deze verbetering is mede gerealiseerd dankzij de Electronic Crime Taskforce, een samenwerkingsverband van de vier grote banken van Nederland, International Card Services BV (ICS), het Openbaar Ministerie en de politie om digitale bancaire criminaliteit te bestrijden.

Bij fraude met creditcardgegevens is er volgens Europol in de meeste lidstaten van de Europese Unie sprake van een verschuiving van zogenoemde *card-presentfraude* naar zogenoemde *card-not-presentfraude.* Digitaal zijn er grote hoeveelheden betaalkaartgegevens beschikbaar door onder andere datalekken, deels als gevolg van *data stealing malware* en social engineering. Deze vorm van fraude speelt slechts een kleine rol in Nederland. Er wordt in ons land relatief weinig met creditcards betaald en veel meer met het beter beveiligde iDEAL.

Bij fraude met online handel zijn meer technisch complexe cybercrime-elementen terug te vinden dan vier jaar geleden. Zo is het namaken van webwinkels de afgelopen jaren professioneler geworden en zijn nepwebwinkels niet of nauwelijks van echte te onderscheiden. De makers van de valse websites zorgen – op naam van een katvanger – voor een inschrijving bij de Kamer van Koophandel, een kantoorpand, een telefoonnummer (met telefoniste) en een bestaand adres. De valse websites zijn lastig uit de lucht te krijgen, doordat ze veelal in Azië en Amerika (Panama) worden gehost. Ook zijn er voorbeelden waarbij hotmail- en Gmailaccounts gehackt zijn om marktplaatsaccounts te achterhalen. Zo'n account wordt dan gebruikt om te adverteren met een webwinkel die ofwel *fake* is ofwel ook gehackt. Op dit moment lijkt er sprake van een verschuiving van frauduleuze verkopen via bekende online handelsplaatsen en nepwebwinkels naar frauduleuze verkopen via sociale media. Er worden bijvoorbeeld goederen aangeboden via Facebook.

Ook bij CEO-fraude en factuurfraude worden weleens technisch complexere cybercrime-elementen aangetroffen. Alleen is niet duidelijk of het hier een nieuwe ontwikkeling betreft. Bij CEO-fraude wordt een persoon of een afdeling van een bedrijf zogenaamd door de CEO van dat bedrijf benaderd om een fors bedrag over te maken naar een bepaalde bankrekening. Hiervoor wordt een bedrijf weleens gehackt om informatie te krijgen die bruikbaar is voor het plegen van de fraude. Bij factuurfraude wordt soms een man-in-the-middle-werkwijze gehanteerd om tussen de leverancier en afnemer in te komen en een factuur met gewijzigd rekeningnummer te versturen ten gunste van de crimineel.

Diefstal van persoonsgegevens

In de context van cybercrime gaat het bij de diefstal van persoonsgegevens om diefstal van digitale datasets met persoonsgegevens na bijvoorbeeld het hacken van servers. Voor deze vorm van diefstal kunnen verschillende beweegredenen zijn. Zo kunnen de gegevens worden gestolen vanuit financiële motieven (doorverkopen van gegevens of afpersen) of vanuit ideologische motieven. Zogenoemde *whitehat*-hackers testen vanuit nobele motieven de beveiliging van servers door te proberen deze te hacken.

In 2014 telden vooral de Verenigde Staten meerdere voorbeelden van grootschalige datalekken van persoonlijke gegevens van klanten bij webwinkels, grote winkelketens en banken en van cliënten van ziektekostenverzekeraars en medische instellingen. Vanwege de grootschaligheid wordt 2014 wel Year of the Mega Breaches genoemd. Ook daarna zijn er in het buitenland grootschalige datalekken geweest; in de databases waaruit gelekt werd, stonden ook gegevens van Nederlanders. In Nederland hebben – voor zover bekend – dergelijke grote hacks niet plaatsgevonden.
In 2015 zijn er buiten Nederland enkele grote hacks geweest. Zo was er een hack op het Amerikaanse Office of Personnel Management (OPM), waarvan de gegevens zouden kunnen worden misbruikt voor contraspionage en het onder druk zetten of chanteren van overheidsmedewerkers. Ook was er een hack op Ashley Madison, een online datingsite, waarin werd geëist dat de website zou worden opgeheven.
In Nederland zijn er hacks geweest op speelgoedfabrikant V-tech en huishoudketen Brabantia, maar de achterliggende motieven zijn onbekend. Sinds 2016 bestaat in Nederland de verplichting datalekken te melden bij de Autoriteit Persoonsgegevens. Op 15 december 2016 stond de teller op bijna 5500 meldingen. De datalekken die bekend zijn geworden, zijn volgens de Autoriteit Persoonsgegevens vooral het gevolg van slordigheid en niet van crimineel handelen. Het betreft onder andere zoekgeraakte usb-sticks, verkeerd verstuurde mailtjes, niet-afgesloten bureauladen en documenten die in de prullenbak belandden in plaats van vernietigd te worden.

Verstoring, vernieling, sabotage

In dit tekstblok gaat het om de gevallen waarin het daadwerkelijk de intentie is om ICT te verstoren of te vernielen en niet om partijen af te persen voor geld. Afpersing is hierboven afzonderlijk behandeld.
Er kunnen diverse motieven zijn om de ICT te willen verstoren of vernielen en een ander zo schade toe te brengen: baldadigheid, wraak, concurrentie of ideologische motieven. De daders (en motieven) van dergelijke aanvallen blijven meestal onbekend.
De meest voorkomende vormen zijn DDoS-aanvallen en *defacements*. DDoS staat voor 'distributed denial-of-service' en houdt in dat een computerserver of website van een bedrijf of instelling wordt aangevallen door meerdere besmette computers (oftewel een botnet), waardoor de website of server plat komt te liggen en klanten en gebruikers er niets meer mee kunnen.

DDoS-aanvallen zijn een wijdverspreid probleem en worden wel de meest gedemocratiseerde vorm van cybercrime genoemd. Voor een geringe prijs kunnen DDoS-aanvallen worden ingekocht via zogenoemde *booter services.* De meeste aanvallen vinden plaats tussen jongeren onderling, maar ook volwassenen en bedrijven maken zich er schuldig aan. *Defacement* of *defacen* is het aanpassen van webpagina's, vaak met als doel een politieke of ideologische boodschap achter te laten. In sommige gevallen zijn er ernstiger vormen van sabotage, waarbij gegevens worden gewist en er informatie verloren gaat.

Hightechcrime

Aanvallen op vitale infrastructuren

Een infrastructuur is vitaal als producten, diensten en de onderliggende processen van essentieel belang zijn voor het dagelijkse leven van de meeste mensen. De vitale producten waar het om gaat, zijn onder meer olievoorziening, productie, transport en distributie van gas en elektriciteit, drinkwatervoorziening, waterbeheer en toegang tot internet en datadiensten. Verstoring van deze producten en processen kan (zeer) ernstige economische, fysieke en sociaal-maatschappelijke gevolgen hebben die leiden tot maatschappelijke ontwrichting. In Nederland is dat tot op heden niet gebeurd. Wel zijn er voorbeelden in het buitenland, zoals een cyberaanval op het Oekraïense elektriciteitsnet in 2015 waarbij 225.000 huishoudens enkele uren zonder stroom kwamen te zitten.

Organisaties in Nederland die verantwoordelijk zijn voor vitale processen en producten hebben evenals andere organisaties last van cyberaanvallen. De meeste aanvallen blijken niet specifiek gericht te zijn tegen de vitale processen. De meestgebruikte digitale instrumenten bij deze aanvallen zijn malware, phishing en ransomware. De vitale processen zijn kwetsbaar voor aanvallen, doordat vaak verouderde procescontrolesystemen worden gebruikt die niet geüpdatet worden maar wel van buitenaf, via internet, toegankelijk zijn. Hiervoor is de laatste jaren meer aandacht en dat heeft geleid tot extra beveiligingsmaatregelen. Daardoor zullen eenvoudige hacks waarschijnlijk minder vaak voorkomen. Desalniettemin blijven vitale processen kwetsbaar voor geavanceerde aanvallen. Er zijn actoren die over de middelen en vaardigheden beschikken om dergelijke aanvallen op vitale infrastructuren uit te voeren. In hoeverre die actoren ook motieven hebben om dit de komende jaren in Nederland te doen, is afhankelijk van internationale politieke en andere ontwikkelingen.

Aanvallen op banken

Bij aanvallen op banken spelen verschillende motieven een rol: het verkrijgen van informatie, ontwrichting van het financiële stelsel en financieel gewin. Zowel criminelen als statelijke actoren kunnen aanvallen (laten) uitvoeren om informatie te verkrijgen. Het doel van statelijke actoren kan bijvoorbeeld zijn invloed uit te kunnen oefenen op of wanorde te kweken in het financiële stelsel van andere landen. Criminelen vallen banken vooral aan om veel geld te verdienen.

Er zijn wereldwijd diverse aanvallen op banken geweest waarbij grote hoeveelheden geld zijn buitgemaakt. Het meest tot de verbeelding sprekende voorbeeld is dat van de criminele groep die in 2014-2015 met behulp van de zogenoemde *Carnabak malware* over de hele wereld meer dan honderd banken heeft aangevallen en tussen de 500 miljoen en 1 miljard US dollar heeft buitgemaakt. De aanvallen waren goed voorbereid en social engineering speelde een belangrijke rol. De aanvallers gebruikten ook de Society for Worldwide Interbank Financial Telecommunication (SWIFT) om grote geldbedragen over te schrijven naar hun eigen rekeningen. SWIFT is een internationaal communicatiesysteem waar wereldwijd ruim negenduizend banken en andere financiële spelers gebruik van maken. In 2015 en 2016 zijn twee banken aangevallen met gebruikmaking van SWIFT. Daarbij werden grote geldbedragen gestolen. Slachtoffers waren de centrale bank van Bangladesh en een commerciële bank in Vietnam.
Er zijn voor zover bekend geen Nederlandse banken slachtoffer geworden van dergelijke grote aanvallen. Maar door deze aanvallen werden zij zich er wel van bewust dat deze ook in Nederland zouden kunnen plaatsvinden. Het is een serieus risico, waarmee banken nu meer rekening houden dan voorheen in de scenario's die ze ontwikkelen om voorbereid te zijn op aanvallen van criminelen.

In Nederland is vooralsnog alleen sprake van pogingen om banksystemen binnen te dringen. Daarbij lijkt het deels te gaan om schijnaanvallen om de beveiliging te testen. De toegenomen maatregelen aan de kant van de banken vragen om grotere investeringen van cybercriminelen. Deze criminelen gaan zich daarom steeds beter organiseren en zich steeds beter voorbereiden om de aanvallen op banken zo effectief mogelijk uit te kunnen voeren. De verwachting is dat daardoor de opbrengst (en dus het verlies voor de banken) per aanval groter wordt. Wat het risico vergroot, is het feit dat de financiële keten als gevolg van de invoering van de nieuwe EU-richtlijn Payment Service Directive2 uit steeds meer partijen bestaat die een deel van het betalingsverkeer overnemen, alle met hun eigen systemen en kwetsbaarheden. Daardoor hebben banken steeds minder controle over de verschillende onderdelen in de keten.

Bedrijfsspionage

Staten, bedrijven en criminelen houden zich bezig met bedrijfsspionage. In de praktijk is het soms lastig onderscheid te maken tussen de verschillende actoren. Zowel statelijke actoren als bedrijven maken voor bedrijfsspionage gebruik van de diensten van beroepscriminelen en criminele middelen (malware).

Spionage door bedrijven bij andere bedrijven of wetenschappelijke instituten heeft doorgaans als doel het verbeteren van de eigen concurrentie- en kennispositie. Bij multinationals gaat het vaak om diefstal van intellectueel eigendom. Dergelijke aanvallen worden zelden openbaar gemaakt. Er zijn enkele Amerikaanse gevallen van vooral bedrijfsmatige spionage bekend geworden. Zo heeft een Amerikaanse aanbieder van linnengoed toegegeven een server van een concurrent te hebben gehackt om zicht te krijgen op diens klanten

en die vervolgens te benaderen. Ook bekende een scout van een Amerikaans baseballteam dat hij een database (met onder andere contract-informatie) van een rivaliserend team had gehackt. Uit gelekte documenten van de gecompromitteerde datingsite Ashley Madison bleek dat de leiding daarvan zich in het verleden toegang had verschaft tot de klantendatabase van een concurrerende datingsite. In 2015 meldden de Nederlandse media dat Chinese hackers chipfabrikant ASML gehackt hadden en informatie hadden gestolen.

Er is nauwelijks zicht op bedrijfsspionage en eventuele ontwikkelingen op dit terrein. Wel kan worden gesteld dat de belangen en potentiële opbrengsten van bedrijfsspionage groot zijn en dat deze vorm van spionage in Nederland voorkomt. Bewustwording en maatregelen blijven achter op de dreiging die volgens experts van dit fenomeen uitgaat. Als dat niet verandert, is de verwachting dat bedrijfsspionage zich de komende jaren ook in Nederland vaker zal voordoen, met nadelige gevolgen voor de concurrentiepositie van ons land.

Hacktivisme

De term *hacktivisme* is een samentrekking van de woorden 'hacking' en (politiek) 'activisme'. Hacktivisme onderscheidt zich van reguliere cybercrime in het motief. Hacktivisten acteren vanuit een politieke of anderszins idealistische overtuiging en ze gebruiken daarvoor drie methoden: (1) verstoren en ontoegankelijk maken van websites, bijvoorbeeld door DDoS-aanvallen, (2) verspreiden van een (ideologische) boodschap, bijvoorbeeld door defacements, en (3) informatie stelen en openbaar maken, bijvoorbeeld door hacking.

De meerderheid van de aanvallen is klein en heeft een beperkte impact. Een DDoS-aanval of defacement kan relatief snel worden opgelost. Er mogen dan weinig grote hacktivistische aanvallen zijn, één enkele aanval kan een grote impact hebben. Voorbeelden hiervan zijn de NSA-*databreach* van Edward Snowden in 2013 en de Panamapapers-hack in 2016. Deze *highprofile*-aanvallen hebben consequenties die jaren kunnen voortduren. Ze zijn eenvoudig uit te voeren, en het lage beveiligingsniveau van de ICT bij veel bedrijven voedt de verwachting dat dergelijke aanvallen steeds meer gemeengoed zullen worden.

Gedigitaliseerde criminaliteit

Bij gedigitaliseerde criminaliteit is ICT een middel om (traditionele vormen van) criminaliteit te plegen. ICT kan een rol spelen in alle fasen van het criminele proces: bij de voorbereiding, de uitvoering en de afronding.

Bij de productie van en handel in cannabis en synthetische drugs speelt internet een rol in de voorbereiding. Het gaat hierbij vooral om het uitwisselen van kennis en informatie over bijvoorbeeld nieuwe productiemethoden of recepten voor nieuwe synthetische drugs. Wat betreft vermogensmisdrijven is er anekdotische informatie dat Google Earth gebruikt wordt voor doelwitselectie en voorverkenning bij woninginbraken en voertuigdiefstal. Sociale media worden gebruikt om afspraken te maken over straatroven, overvallen of woninginbraken.

Bij verschillende vormen van vermogenscriminaliteit worden digitale technologieën gebruikt bij de uitvoering. De opvallendste ontwikkeling is zichtbaar bij de diefstal van auto's: daarbij worden steeds vaker laptops gebruikt voor het uitlezen van sleutels en het uitschakelen van het alarm en de startonderbreker. Bij winkeldiefstallen worden stoorzenders gebruikt om detectiepoorten buiten werking te stellen. Bij zware overvallen en liquidaties wordt gebruikgemaakt van BlackBerry's met PGP (Pretty Good Privacy), een manier om afgeschermd te communiceren.

Digitalisering in de transportsector en in de Nederlandse havengebieden heeft ertoe geleid dat criminelen hun toevlucht zoeken tot nieuwe methoden om het logistieke proces te manipuleren. Dat is onder andere geconstateerd bij de cocaïnehandel en -smokkel en bij ladingdiefstal. Vroeger werden bijvoorbeeld vrachtbrieven en containerinformatie 'analoog' gestolen uit chauffeurscafés of verkocht door havenmedewerkers. Tegenwoordig is deze informatie steeds vaker alleen digitaal beschikbaar. Dat betekent dat criminelen toegang moeten krijgen tot de digitale systemen, hetzij door hacken hetzij door het omkopen van kantoorpersoneel of opsporingsambtenaren. Social engineering is hierbij een mogelijkheid voor criminelen om contacten te leggen. Langs deze weg kunnen ICT'ers bij havenbedrijven bijvoorbeeld benaderd worden via LinkedIn of Facebook.
Bedrijven in de transportsector maken steeds vaker gebruik van digitale vrachtuitwisselingssystemen. Deze systemen zijn niet altijd goed beveiligd. Er zijn tot nu toe enkele ladingdiefstallen gepleegd waarbij ze zijn misbruikt. Er zijn nog geen gevallen bekend waarbij ze zijn gehackt. Dit alles zal mogelijk veranderen als criminelen hun digitale vaardigheden verder ontwikkelen.

Slachtoffers van mensenhandel, kinderporno en diverse vormen van horizontale fraude (fraude met betaalmiddelen, fraude op online marktplaatsen, voorschotfraude en acquisitiefraude) worden benaderd en gerekruteerd via internet en sociale media. Katvangers worden gerekruteerd via online advertenties en sociale media, soms met een sollicitatiegesprek waaruit niet blijkt dat ze zullen gaan meewerken aan criminele activiteiten.

Identiteitsfraude is vaak een stap bij de uitvoering van andere (fraude)delicten en komt voor bij veel vormen van georganiseerde criminaliteit. Het betreft vooral het gebruik van valse namen, het gebruik van andermans rekeningnummer en de inzet van katvangers bij onder andere gebruikmaking van rechtspersonen. Als gevolg van de digitale ontwikkelingen nemen de mogelijkheden om identiteitsfraude te plegen toe. Veel mensen hebben online meerdere gebruikersprofielen. Al die accounts kunnen worden misbruikt. Dat steeds meer zaken op afstand geregeld worden, zonder dat iemand in persoon hoeft te verschijnen, vergroot de mogelijkheden voor identiteitsfraude eveneens. Identiteitsverificatie wordt hierdoor immers lastiger. Dit speelt bijvoorbeeld bij het aanvragen van financiële producten zoals verzekeringen, hypotheken en betaalrekeningen.

Ook bij de productie van illegale goederen worden digitale technologieën gebruikt. Zo worden met inkjetprinters valse eurobiljetten gemaakt en kunnen 3D-printers producten namaken (merkfraude) en vuurwapens fabriceren. In hoeverre dat de komende jaren daadwerkelijk zal gebeuren, is moeilijk in te schatten. Naar verwachting is er vanwege de lage productiekosten voorlopig voldoende aanbod van regulier geproduceerde namaakproducten.

De handel in illegale goederen en diensten op internet neemt toe, zowel op het darkweb als op het reguliere internet. Het betreft veelal de handel in drugs (voornamelijk synthetische drugs en cannabis), nagemaakte goederen of namaakgoederen, illegale vuurwapens, gestolen waar, vals geld, gestolen creditcardgegevens of kinderporno, mensenhandel of mensensmokkel. Bij deze handel wordt vaak gebruikgemaakt van cryptocurrency's, in het bijzonder van bitcoins. De versleutelingstechniek achter cryptocurrency's wordt blockchaintechnologie genoemd. Deze technologie controleert de echtheid van een virtuele munt en biedt koper en verkoper de mogelijkheid op een vertrouwde manier transacties te verrichten zonder tussenkomst van een derde vertrouwde partij.

De groeiende populariteit van het darkweb bij criminelen is vooral te danken aan de mogelijkheden die het biedt om anoniem te blijven. Het darkweb is onderdeel van het deepweb. Het deepweb is het deel van het internet dat niet door zoekmachines zoals Google geïndexeerd kan worden; hieronder vallen bijvoorbeeld ook intranetsites van reguliere bedrijven. Het darkweb bestaat uit darknets, netwerken waarbij communicatie in vertrouwen plaatsvindt. Het oorspronkelijke doel van het darkweb was het garanderen van vrijheid van meningsuiting voor hen die te maken hebben met censuur. TOR is het bekendste voorbeeld van een darknet. Andere voorbeelden zijn Freenet en Invisible Internet Project (I2P). TOR en andere darknets worden niet alleen gebruikt om censuur te vermijden, er worden ook criminele activiteiten op ontplooid. TOR lijkt daarbij volgens onderzoek van Europol vooralsnog verkozen te worden boven andere ondergrondse platforms en marktplaatsen. Dat wordt bevestigd in onderzoek van Van Remunt en Van Wilsem uit 2016. Volgens dat onderzoek groeit de populariteit van het TOR-netwerk nog steeds evenals de omvang van de geldtransacties die er plaatsvinden. Het gaat daarbij vooral om drugshandel. De mogelijkheid bestaat dat de drugshandel zich verplaatst van de fysieke wereld naar het digitale domein. Experts zijn het niet eens over de vraag in hoeverre en op welke termijn dat daadwerkelijk zal gebeuren. Aan de ene kant werkt het darkweb drempelverlagend en kan daar op een veilige en afgeschermde manier worden gehandeld, aan de andere kant wordt aangevoerd dat drugs en ook andere goederen in Nederland ook zonder darkweb gemakkelijk te verkrijgen zijn.

De technologische ontwikkelingen staan ondertussen niet stil. Volgens de rapportage van Trend Micro uit 2015 (Ciancaglini et al.) zullen criminelen meer investeren in het darkweb om nog anoniemer te kunnen communiceren en onvindbaar en ongrijpbaar te blijven voor opsporingsinstanties. Daarnaast worden er nieuwe gedecentraliseerde marktplaatsen verwacht die gebaseerd zijn op de blockchaintechnologie.

Ook bestaat het vermoeden dat er nog geavanceerdere diensten zullen komen die het traceren van cryptocurrency's en met name bitcoins (nog) moeilijker maken.

Het gebruik van cryptocurrency's wordt in toenemende mate gesignaleerd in witwasonderzoeken. Het zijn vooral bitcoins die de afgelopen jaren in beslag zijn genomen. Transacties met bitcoins kunnen relatief anoniem zijn, vooral wanneer gebruik wordt gemaakt van bitcoinmixers en (malafide) bitcoinexchangers om het virtuele geld om te zetten in traditionele betaalmiddelen. De afgelopen jaren is ook gebleken dat *payment service providers* (PSP's) gebruikt of zelfs opgezet worden om geld wit te wassen. Een PSP is een online-betaaldienstverlener die de betalingen bij zowel online als offline winkeliers kan afhandelen. Een PSP spaart vaak verschillende transacties op, waardoor het voor de bank moeilijker is een controle uit te voeren op verdachte transacties. Een PSP zelf blijkt hiertoe vaak ook niet in staat. Zo kan een PSP onbedoeld criminelen helpen bij het verhullen van de herkomst van geld.

Bij veel van de genoemde digitale ontwikkelingen gaat het om de afschermingsmogelijkheden door geavanceerde encryptietechnologieën waarmee financiële transacties, communicatie, identiteit en andere gegevens worden verhuld. Daarvoor worden ook bonafide diensten gebruikt zoals Dropbox, Pinterest, WhatsApp en Google docs. Deze diensten zijn aantrekkelijk, omdat verkeer van en naar deze diensten vaak standaard versleuteld wordt verstuurd en omdat communicatie met deze diensten op zichzelf niet verdacht is.

Jammers en opspoorapparatuur zijn offensieve methoden waarmee opnameapparatuur en bakens kunnen worden verstoord. Met opspoorapparatuur kunnen onder andere voertuigen en goederen worden 'gesweept', gecontroleerd op afluisterapparatuur. In verschillende deelonderzoeken voor dit dreigingsbeeld is dat geconstateerd. Bij kraken op geldautomaten sweepen daders hun voertuigen op bakens en bij heling zoeken ze op deze wijze naar track-and-tracetechnologie in gestolen partijen goederen om deze vervolgens onschadelijk te maken. Hennepplantages en drugslabs worden (tegen de politie en criminelen) beveiligd met behulp van digitale camera's, bewegingsmelders, opnameapparatuur en alarmsystemen.

Invloed op aard en omvang van criminaliteit

Bij meerdere criminele verschijnselen heeft de digitalisering invloed op de aard van de criminaliteit. Zo lijkt als gevolg van de digitale ontwikkelingen de ernst van enkele delicten toe te nemen, zien we soms nieuwe typen daders of dadergroepen en slachtoffers, en zijn er gevolgen voor de wijze waarop het logistieke proces georganiseerd is. In sommige gevallen leidt de digitalisering tot verandering in de criminele samenwerking. En bij enkele criminaliteitsvormen zien we door de digitale ontwikkelingen een toename in de omvang.

Door de geavanceerde afschermingsmogelijkheden die de digitale ontwikkelingen bieden, is het zicht op verschillende criminele verschijnselen minder geworden. Met een afnemend zicht kan de ernst van deze delicten toenemen. Dit komt sterk naar voren bij kinderpornografie: er lijkt tegenwoordig minder schroom te bestaan om ook de ernstiger vormen van misbruik te delen.
Ook fenomenen als sexting (het digitaal verspreiden of delen van seksueel getinte foto's) en *livestreaming* of 'live distant child abuse' nemen toe door deze digitale ontwikkelingen. Hierdoor worden meer – soms zeer jonge –kinderen slachtoffer van *sextortion* of seksueel misbruik. Sextortion is afpersing op internet met door sexting verkregen afbeeldingen of filmpjes. Vooral door sexting lopen Nederlandse kinderen een verhoogd risico slachtoffer te worden van sextortion of cyberpesten.

Doordat vooral jongeren zeer actief zijn op internet en er weinig moeite mee hebben om gevoelig (beeld)materiaal te delen, wordt een bredere groep jongeren kwetsbaar voor kinderporno en mensenhandel. Niet alleen het profiel van (potentiële) slachtoffers is aan veranderingen onderhevig, ook het profiel van afnemers verandert. Bij het aanschaffen van illegale of gestolen goederen of het inhuren van illegale diensten zijn het vooral online handelsplaatsen die drempelverlagend werken. Waren voorheen connecties nodig met criminelen, in de fysieke wereld, nu zijn die niet meer nodig.

Afgaand op (een weliswaar beperkt aantal) opsporingsonderzoeken kunnen we ons een beeld vormen van daders achter cybercrime. Afhankelijk van het type delict zien we verschillende soorten daders. Bij delicten waar financieel gewin centraal staat, zoals bij afpersing, verschillende fraudevormen en criminele activiteiten op de illegale markten, zijn het overwegend beroepscriminelen die de dienst uitmaken. Beroepscriminelen zijn agressiever en gaan sneller de directe confrontatie met slachtoffers aan dan andere categorieën daders, die met andere vormen van cybercrime geassocieerd worden, zoals hacktivisten, statelijke actoren en cybervandalen.
Over de wijze waarop daders met elkaar samenwerken, is weinig empirisch materiaal beschikbaar. In de samenwerking worden verschillende rollen onderscheiden: kernleden die het proces aansturen, facilitatoren, moneymules, programmeurs, techneuten, hackers, fraudeurs, (criminele) hosters en financieel ondersteuners. Soms wordt door dadergroepen samengewerkt langs hiërarchische lijnen en soms wordt samengewerkt in losse, tijdelijke, internationaal opererende samenwerkingsverbanden.

Bij sommige delicten verandert de criminele samenwerking als gevolg van de digitale ontwikkelingen. Dit is bijvoorbeeld het geval bij autodiefstal. De gebruikte digitale beveiligingsmethoden vereisen specialistische kennis en materiaal. De investering in kennis en materiaal is voor individuele daders te kostbaar; dadergroepen hebben meer financiële armslag. Bij kinderpornografie is er als gevolg van de groei van het internet en de toegenomen geavanceerde mogelijkheden meer dan voorheen sprake van clustering van gebruikers

in internationale kinderpornonetwerken. Deze clusters houden zich bezig met livestreaming van kindermisbruik of met chantage met seksueel beeldmateriaal.
In een aantal gevallen is gebleken dat er nieuwe daders en dadergroepen actief zijn geworden. Er zijn bijvoorbeeld particuliere, zelfstandig werkende producenten van synthetische drugs aangetroffen die hun producten uitsluitend via het darkweb verkopen. Overigens zijn er op het darkweb naast nieuwkomers ook veel oudgedienden te vinden: veel verkopers van drugs op het darkweb waren voorheen straatdealer.

De verplaatsing van de handel naar het darkweb kan gevolgen hebben voor de wijze waarop het logistieke proces georganiseerd is. Zo zou in veel gevallen de tussenhandel kunnen verdwijnen, omdat directe handel tussen producent en gebruiker makkelijker is geworden. Bij drugshandel waarbij een beroep moet worden gedaan op grootschalige internationale netwerken, zoals bij de handel in cocaïne en heroïne, ligt dit volgens de onderzoekers minder voor de hand. De kopers op het darkweb lijken in dit geval juist vaker de tussenhandelaars te zijn.

Aansluitend heeft de handel op het darkweb gevolgen voor de wijze waarop de illegale goederen worden vervoerd. Hoewel de smokkelwaar nog grotendeels in grotere partijen via de lucht, het water en de weg wordt getransporteerd, is er door de handel op *darkmarkets* een toename van het vervoer van kleinere partijen via post-, pakket- of koeriersdiensten.

De verplaatsing van handel naar internet betekent een sterkere marktwerking, waarin de klant een sterkere positie heeft. Daardoor krijgt hij betere waar voor zijn geld en verminderen de schadelijke gevolgen van drugs die via internet zijn aangeschaft. Drugsgebruikers wisselen op internet meer informatie uit over de kwaliteit van geleverde drugs en verantwoord drugsgebruik. Ook worden er drugstests aangeboden.
Uit het deelproject over mensensmokkel blijkt dat er door communicatie via sociale media een meer open markt ontstaat. Zo is er een betere informatie-uitwisseling over de geleverde diensten van mensensmokkelaars. Ook zijn irreguliere migranten door de informatie-uitwisseling in toenemende mate in staat zelfstandig te reizen. Wellicht wordt de rol van mensensmokkelaars daardoor minder groot. Een mogelijke keerzijde van de genoemde ontwikkeling is dat irreguliere migratie laagdrempeliger wordt.

Het is niet bekend in hoeverre de omvang van de georganiseerde criminaliteit stijgt door de toegenomen digitale mogelijkheden om illegale goederen en diensten af te zetten en criminele handelingen af te schermen. Of en in welke mate er sprake is van ‘slechts’ een verschuiving van criminele handel van het fysieke domein naar het digitale domein, is evenmin bekend. Dit komt doordat er weinig zicht is op de omvang van de illegale handel op internet en in het bijzonder op het darkweb.

In een aantal gevallen is de criminaliteit ten gevolge van de digitalisering in omvang toegenomen. Dat zien we vooral bij sterk gedigitaliseerde criminaliteitsvormen als kinderporno-

grafie en online gokken. Internet en de geavanceerde afschermingsmogelijkheden werken bij kinderpornografie drempelverlagend. Steeds meer mensen krijgen toegang tot internet, en dat geldt dus ook voor verspreiders van kinderpornografie en misbruikers. De digitale ontwikkeling vergroot ook het risico van online gokken, vooral doordat deze ontwikkeling het mogelijk heeft gemaakt wereldwijd te gokken. Door de opkomst van mobiele platforms zijn goksites bovendien makkelijk bereikbaar. Ook de opkomst van *e-sports*, het in competitieverband spelen van computergames, vergroot het risico: ook op deze competities kan gewed worden.

Bij horizontale en verticale fraude is weliswaar sprake van een relatief hoge mate van digitalisering, maar voor de komende jaren wordt bij meerdere vormen hiervan geen grote verschuiving in aard en omvang verwacht. Zo is fraude met online handel een gedigitaliseerde vorm van fraude die al jaren veelvuldig voorkomt en is voorschotfraude een gedigitaliseerde vorm die al jaren wat minder voorkomt. Er zijn binnen het digitale domein ook remmende factoren waardoor er geen grote verschuivingen optreden, zoals naar voren komt bij fraude met betaalmiddelen, acquisitiefraude en hypotheekfraude. Er is software ontwikkeld om (deze) fraudes te herkennen, onder meer door het mogelijk te maken verschillende systemen aan elkaar te koppelen (big data).
Bij merkfraude wordt echter een toename verwacht. Door het internet is de drempel verlaagd om namaakartikelen aan te bieden. Bovendien lijkt het normbesef bij burgers, vooral binnen het digitale domein, af te nemen en zijn deze goederen dus makkelijker af te zetten. Handhavingscapaciteit schiet al snel tekort om alle (illegale) transacties via internet te volgen.

Er wordt een toename verwacht van het aanbod van synthetische drugs op het darkweb, waardoor het makkelijker wordt deze aan te schaffen. Heling – en daarmee (deels) ook de daaraan voorafgaande vormen van diefstal – gedijt door de digitalisering: door het internet groeit de afzetmarkt, consumenten vragen zich niet altijd af wat de herkomst van een goed is. Ten aanzien van mensenhandel wordt verwacht dat het rekruteringsproces door digitale ontwikkelingen een groter bereik heeft en dat het gebruik van online diensten om mensenhandel te faciliteren verder zal toenemen.

Tot slot nog enkele opmerkingen over de dienstverleners. Zij faciliteren het gebruik van digitale technologie op verschillende manieren. De belangrijkste actoren zijn *hostingproviders.* Nagenoeg elke vorm van digitale criminaliteit heeft hosting nodig, en Nederland heeft een goede digitale infrastructuur en veel grote hostingproviders. Malafide onderaannemers faciliteren bewust criminele activiteiten door voor relatief hoge prijzen volledig *bulletproof*, dat wil zeggen anonieme, hosting aan te bieden. Daardoor hebben hostingproviders geen zicht op de daadwerkelijke gebruikers van hun infrastructuur. Dit komt niet vaak meer voor, omdat de onderaannemer hierdoor zelf strafbaar wordt. Wel bieden malafide hostingproviders hosting aan waarbij het toezicht door de overheid op subtielere manieren wordt tegengewerkt.

Een bijzondere vorm van dienstverlening wordt *Crime-as-a-Service* (CaaS) genoemd. Dankzij deze dienstverlening kunnen criminelen, zonder over bijzondere digitale vaardigheden of grondige technische kennis te beschikken, gebruikmaken van digitale instrumenten om cybercrime te plegen en anoniem te opereren op het darkweb en internet: met CaaS kunnen ze DDoS-aanvallen uitvoeren, ransomware verspreiden en gebruikmaken van Remote Access Tools (RAT's), waarmee ze op afstand computers kunnen beheren. Er zijn kant-en-klare softwarepakketten te koop waarmee het mogelijk is diverse vormen van cybercrime te plegen. Een voorbeeld zijn de zogenoemde *exploit kits* die kwetsbaarheden in computerprogramma's detecteren en vervolgens malware installeren.

Verwachtingen en gevolgen

Verwachtingen

De belangrijkste verwachtingen omtrent de toekomstige ontwikkelingen van cybercrime en gedigitaliseerde criminaliteit zijn gerelateerd aan het toenemende belang van internet in de samenleving. Internet speelt een steeds grotere rol in de wijze waarop delen van de samenleving op allerlei terreinen met elkaar verbonden zijn, bijvoorbeeld in maatschappelijk, economisch en technologisch opzicht. Huidige trends zoals het *Internet of Things* (IoT), *cloudcomputing* en de snelle opmars van mobiele internettechnologie zullen de komende jaren doorzetten, en daarmee zal internet nog belangrijker worden.

Met IoT wordt bedoeld dat steeds meer 'dingen', zoals apparaten, infrastructuur en voertuigen, via het internet worden verbonden en gegevens met elkaar kunnen uitwisselen. De verwachting is dat het in 2020 om bijna 21 miljard 'dingen' gaat: koelkasten, thermostaten, auto's, medische apparaten et cetera. De beveiliging van deze apparaten is vaak niet in orde, doordat deze niet geüpdatet wordt. Dat biedt mogelijkheden om de apparaten te hacken.
Meerdere malen is het security-onderzoekers en hackers gelukt verschillende merken auto's te hacken. Dat stelde hen er onder andere toe in staat het stuur en de remmen over te nemen. Ook is in het recente verleden een groot botnet van apparaten die 'deel uitmaken' van het IoT, gebruikt voor grootschalige DDoS-aanvallen. Daarbij werd een bedrijf getroffen dat belangrijk is voor toegang tot onder andere Twitter, Netflix en Spotify, met als gevolg dat velen tijdelijk geen gebruik konden maken van deze populaire diensten.
In hoeverre voertuigen en andere 'dingen' die verbonden zijn met het internet gehackt en gebruikt zullen worden door criminelen hangt af van de mate waarin er een economisch verdienmodel van gemaakt kan worden. Hierbij kan gedacht worden aan 'dingen' waaraan financiële transacties gekoppeld zijn en/of 'dingen' met een hoog afbreukrisico, waarbij blokkering van de ICT fatale gevolgen heeft. Bij een hoog afbreukrisico is het doelwit wellicht vatbaar voor afpersing. Doelwit kunnen eigenaren en producenten van gehackte voertuigen zijn, maar ook bijvoorbeeld ziekenhuizen, zoals al is aangestipt.

Naast het IoT ontstaat de komende jaren ook een tendens waarbij mensen met het internet worden verbonden, bijvoorbeeld via implantaten. In dat verband wordt wel gesproken van het *Internet of People* (IoP). Een voorbeeld van zo'n 'menselijke connectie' met het internet is de pacemaker. In het IoP-tijdperk ontstaan in toenemende mate toepassingen die onze werkelijke wereld vermengen met een virtuele wereld en digitale informatie aan de werkelijke wereld toevoegen (*augmented* of *mixed reality*). Deze extra informatie kan worden getoond via een smartphone, tablet, *smart glasses* of *head-updisplay*. Volgens Europol kan dit het onderscheid tussen cyberaanvallen en fysieke aanvallen doen vervagen – met als gevolg fysiek letsel, maar mogelijk ook meer psychische schade.

De ontwikkelingen in de mobiele internettechnologie zijn de laatste jaren snel gegaan. Het smartphonebezit is toegenomen van 45 procent in 2011 naar 80 procent in 2015. Het merendeel van de smartphonefabrikanten gebruikt als besturingssysteem een eigen variant van Android; in 2016 had 80 procent van de verkochte smartphones Android als besturingssysteem. Omdat gebruikersgemak nogal eens de voorkeur krijgt boven beveiliging, actualiseren fabrikanten de besturingssystemen onvoldoende. Daardoor ontstaan beveiligingsrisico's. Criminelen spelen hierop in door in toenemende mate malafide apps te ontwikkelen, vooral op het vlak van *banking malware*. In 2015 maakte een grootschalig internationaal opsporingsonderzoek naar *mobile banking malware* duidelijk welke gelegenheid mobiele platforms bieden voor cybercrime. Bij dit onderzoek werd een belangrijk netwerk van cybercriminelen opgerold. Doordat ze de malware voortdurend aanpasten, wisten ze de beveiliging van de banken een aantal keren te omzeilen en een schade van minstens 2 miljoen euro te veroorzaken. Ze wasten het geld wit door middel van geldezels, die hun bankrekening tegen geringe betaling ter beschikking van de criminelen stelden. Minimaal 150 Nederlandse bedrijven en particulieren werden slachtoffer. Wereldwijd werden in totaal 60 verdachten aangehouden, van wie ongeveer 40 in Nederland. Ook een deel van de gebruikte infrastructuur stond in Nederland en werd ontmanteld.

Ondanks de toename van het smartphonebezit is het risico op malware op mobiele platforms relatief beperkt. Het verspreiden van malware op smartphones kost verhoudingsgewijs meer moeite en geld dan het verspreiden van malware op computers. Op traditionele computersystemen gebruiken mensen vaak één browser waarmee ze alle diensten raadplegen. Bij mobiele platforms gebeurt dit via afzonderlijke apps die allemaal verschillen qua ontwerp, protocollen en technieken. Om deze apps aan te vallen moet gerichte en dus dure malware worden ontwikkeld. Ook richt ransomware op smartphones waarschijnlijk minder schade aan dan op computers door de betere (automatische) back-upfuncties. Het aantal malafide apps zal door de toename van het smartphonebezit ongetwijfeld groeien, maar verwacht wordt dat computers voorlopig het belangrijkste doelwit blijven van cybercriminelen.

Een andere belangrijke ontwikkeling is cloudcomputing. De essentie hiervan is dat ICT-infrastructuren, platforms, softwarediensten en data niet langer lokaal op een eigen pc of server staan, maar via het internet worden gebruikt. Het beheer van de gegevens en de applicaties is uitbesteed aan een dienstverlener, en gegevens worden veelal verspreid over verschillende servers opgeslagen. Het werken in de cloud is een trend en zal naar verwachting de komende jaren toenemen. De cloud kent over het algemeen een goede beveiliging; in veel gevallen is hij beter beveiligd dan lokaal gebruikte computers van bijvoorbeeld kleine en middelgrote bedrijven. De toegangsbeveiliging is de laatste jaren verbeterd. Veel diensten in de cloud zijn overgegaan op een extra beveiligingslaag, de zogenoemde tweefactor-authenticatie. De komende jaren zullen meer diensten volgen. Desalniettemin blijven de toegang tot en de opslag van data bij clouddiensten risicovol, doordat deze beheerd worden door mensen. Die kunnen bedoeld of onbedoeld fouten maken in hun bedrijfsvoering, waardoor grote hoeveelheden data gestolen kunnen worden en in handen kunnen vallen van criminelen. Ook kan de cloud als instrument worden misbruikt bij het uitvoeren van cyberaanvallen. Bij misbruik van de cloud als instrument wordt de opslag- en rekencapaciteit ervan gebruikt voor het maken van botnets of voor het uitvoeren van grootschalige DDoS-aanvallen. Daarnaast kunnen clouddiensten een krachtig middel zijn voor de verspreiding van malware.
Als de cloud doelwit is van criminelen vanwege de schat aan informatie die hij herbergt, is het hun vaak te doen om het verkrijgen van financiële gegevens en identiteitsgegevens. Ze kunnen uit zijn op handel in data of op hacktivisme, maar ook op vernieling of verstoring door middel van DDoS-aanvallen of op afpersing door middel van ransomware en het dreigen met lekken van informatie.
Natuurlijk biedt de goede beveiliging van de cloud criminelen ook mogelijkheden om anoniem en niet-traceerbaar te communiceren. Daardoor is er steeds vaker geen aanwijsbare locatie waar de data zich bevinden – een uitdaging voor de opsporing, omdat de locatie zich dikwijls in het buitenland bevindt.
Transacties met cryptocurrency's (bitcoins) zijn openbaar en transparant, doordat ze direct tussen koper en verkoper plaatsvinden. Zoals eerder vermeld, is de technologie achter cryptocurrency's de blockchaintechnologie. Kort gezegd is een blockchain een openbaar en online register van transacties. Zo kan via de blockchain van de bitcoin nagegaan worden wie de eigenaar is en of de bitcoin niet twee keer wordt uitgegeven. Door het gebruik van geraffineerde online *mixtools* proberen criminelen de herkomst van bitcoins te verhullen. Vermoedelijk wordt het de komende jaren daardoor mogelijk bitcoins ontraceerbaar wit te wassen.

CaaS zal zich de komende jaren volgens het *Cybersecuritybeeld Nederland 2016* verder blijven ontwikkelen en professionaliseren. Cybercrime wordt niet alleen gefaciliteerd door aangeboden software en tools, er komen ook steeds meer handleidingen en zelfs helpdesks die criminelen kunnen raadplegen. Deze ontwikkelingen dragen bij aan een bredere beschikbaarheid van deze dienstverlening en dat zal het de komende jaren naar verwachting voor criminelen eenvoudiger maken om cybercrime en gedigitaliseerde criminaliteit te plegen.

Op het terrein van de cybersecurity werken veel publieke en private partijen samen om cybercrime tegen te gaan. Hun streven is de handen ineen te slaan en de Nederlandse samenleving weerbaarder te maken. Het Nationaal Cyber Security Centrum speelt daarin nu en de komende jaren een belangrijke rol. Digitale ontwikkelingen bieden ook kansen voor de opsporing, zoals slimme digitale camera's en digitale fraudedetectiesystemen, onder andere met de mogelijkheid verschillende systemen te koppelen (big data). Het gebruik van digitale technologieën door criminelen laat bovendien digitale sporen na die naar de daders kunnen leiden. De snelle opeenvolgende digitale ontwikkelingen maken het voor de opsporing noodzakelijk deze op de voet en adequaat te volgen.

Gevolgen

Het is niet bekend wat de totale omvang is van cybercriminaliteit in Nederland. Dat maakt het lastig om het geheel aan gevolgen voor de Nederlandse samenleving te beschrijven. Twee commerciële bedrijven, namelijk McAfee en Deloitte, hebben een poging gedaan en daaruit blijkt dat het (vermoedelijk) om aanzienlijke gevolgen gaat. De totale schade van cybercriminaliteit voor de Nederlandse economie schatten McAfee en Deloitte op respectievelijk 8,8 en 10 miljard euro, dat is om en nabij 1,5 procent van het bruto binnenlands product (bbp). In beide onderzoeken is gekeken naar zowel de directe als de indirecte kosten die het gevolg zijn van cybercriminaliteit. Directe kosten komen voort uit onder andere verlies van geld, verlies van waardevolle bedrijfsinformatie en onderbreking van de operationele continuïteit. Indirecte kosten komen voort uit de beveiligingsmaatregelen die getroffen worden tegen cybercriminaliteit en uit inbreuk op intellectueeleigendomsrechten.

Nederland heeft een relatief hoog geschat schadebedrag in vergelijking met andere landen. In het onderzoek van Deloitte wordt dat gerelativeerd: Nederland registreert in vergelijking met andere landen goed. De schade wordt door Deloitte verder genuanceerd als 'cost of doing business'. De digitalisering van onze samenleving brengt ook veel welvaart. In 2013 was het aandeel van de ICT-sector ruim 4 procent van het bbp. En de sector wordt steeds belangrijker voor de Nederlandse economie, met bovengemiddelde groeicijfers.

Cybercrime is een wijdverbreid probleem, dat qua aantallen slachtoffers volgens het Centraal Bureau voor de Statistiek (CBS) niet onderdoet voor vermogenscriminaliteit: in 2015 werden bij beide criminaliteitsvormen negentien slachtoffers geteld op elke honderd inwoners. De financiële schade voor burgers is in vergelijking met andere vormen van criminaliteit over het algemeen beperkt en wordt in veel gevallen (zoals bij fraude met internetbankieren en creditcardfraude) door de bank vergoed. De meeste schade komt volgens McAfee en Deloitte voor rekening van bedrijven en overheidsorganisaties. Slachtoffers kunnen ook last krijgen van psychische problemen, met soms fatale persoonlijke gevolgen, bijvoorbeeld als een slachtoffer zelfmoord pleegt. De ernst zal verschillen per type cybercrime. Bij een delict als afpersing is het risico op ernstige psychische schade groter dan bij fraude met internetbankieren.

Organisaties worden steeds vaker slachtoffer van cybercrime en het lijkt daarbij vaker te gaan om gerichte aanvallen. Volgens onderzoek van PwC uit 2014 is een op de vijf bedrijven in Nederland slachtoffer van cybercrime. Dat is minder dan bij andere vormen van economische criminaliteit, waar drie van de vier bedrijven slachtoffer worden. In dat onderzoek schatten respondenten ook de schade van cybercrime beduidend lager in dan die van andere vormen van economische criminaliteit. Recenter onderzoek van PwC uit 2016 in het Verenigd Koninkrijk heeft uitgewezen dat daar in vergelijking met 2014 een stijging is van het aantal bedrijven dat slachtoffer is geworden van cybercrime.[40] In Nederland is dat waarschijnlijk ook het geval.

Ook onderzoek van Veenstra, Zuurveen en Stol uit 2016 naar cybercrime bij bedrijven in het midden- en kleinbedrijf en bij zzp'ers geeft een wat genuanceerder beeld. Hoewel uit dit onderzoek naar voren komt dat bijna 30 procent van de onderzochte bedrijven en zzp'ers slachtoffer is geworden van een of meer vormen van cybercrime, rapporteert twee vijfde van de getroffenen dat zij geen schade hebben geleden. Bij de overige bedrijven is tijdverlies de meestgenoemde schadepost, gevolgd door financiële schade.

Hoewel middelgrote en kleine bedrijven volgens deskundigen kwetsbaar zijn, vanwege een relatief laag beveiligingsniveau in vergelijking met grotere bedrijven, blijkt dat niet direct uit eerdergenoemd onderzoek van PwC uit 2014. Uit dat onderzoek kwam naar voren dat de grootte van een organisatie niet van invloed is op de mate van slachtofferschap. Wel wordt vermoed dat middelgrote en kleine bedrijven en zzp'ers minder vaak aangifte doen dan grotere bedrijven.
Bij de overheid zijn vooral onderwijsinstellingen en zorginstellingen kwetsbaar vanwege de relatief zwakke ICT-voorzieningen. Scholen zijn vaak het doelwit van DDoS-aanvallen die door jongeren worden gepleegd; de schade van deze aanvallen bedraagt volgens berichten in de media miljoenen euro's. Ziekenhuizen zijn kwetsbaar vanwege het hoge afbreukrisico, mocht gedreigd worden het ziekenhuissysteem plat te leggen.

Conclusie

Internet en de bijbehorende digitale ontwikkelingen spelen een steeds grotere rol in de wijze waarop delen van de samenleving op allerlei terreinen met elkaar verbonden zijn. De afgelopen jaren volgden de ontwikkelingen elkaar snel op en de verwachting is dat dit de komende jaren niet anders zal zijn. De verbondenheid met internet in het dagelijks leven neemt de komende jaren verder toe. Bijna iedereen is in het bezit van een smartphone en maakt steeds meer gebruik van goed beveiligde diensten in de cloud en communiceert steeds anoniemer door sterk verbeterde encryptietechnieken. Deze diensten en technieken zijn voor iedereen toegankelijk en dragen bij aan een betere cybersecurity en een grotere weerbaarheid tegen cybercrime.

Dat heeft ook een andere kant: ook binnen het criminele domein zijn deze diensten en technieken laagdrempelig toegankelijk. Ze bieden criminelen goede afschermingsmogelijkheden, waarmee gegevens, identiteit, communicatie en financiële transacties succesvol kunnen worden verhuld voor opsporing en vervolging. Bovendien volgen veel personen en bedrijven de snelle digitale ontwikkelingen niet op de voet. Daardoor zijn ze kwetsbaar voor cybercrime en gedigitaliseerde criminaliteit. Dat biedt gelegenheden voor criminelen.

De digitale instrumenten en technieken die gebruikt worden bij cybercrime, worden in toenemende mate toegepast bij de traditionele vormen van georganiseerde criminaliteit die beschreven zijn in dit schrijven. De verweving tussen cybercrime en gedigitaliseerde criminaliteit wordt steeds sterker. Als deze ontwikkeling doorzet, zal er in de toekomst nauwelijks of geen onderscheid zijn tussen cybercrime en gedigitaliseerde criminaliteit. Het is dan een amalgaam van digitale middelen en vormen van criminaliteit om onder meer diefstal en frau-de te plegen, mensen af te persen, te smokkelen en te rekruteren, en drugs en wapens te verkopen.

Op alle criminele markten hebben de digitale ontwikkelingen invloed op de aard van de criminaliteit. Dat is te zien aan de manier waarop tegenwoordig wordt samengewerkt: bij internationale kinderpornonetwerken bijvoorbeeld ontstaan clusters, en er is meer samenwerking bij autodiefstal. Via internet wordt het voor criminelen makkelijker om (internationaal) samen te werken, in veel gevallen anoniem. De invloed van de digitale ontwikkelingen manifesteert zich ook in de toename van individuele producenten van synthetische drugs die als zzp'er hun producten via het darkweb verkopen. Ook de logistiek verandert als gevolg van de digitale ontwikkelingen. Zo neemt door het darkweb de straathandel af en krijgt wie op het web drugs heeft gekocht, ze met de (pakket)post toegestuurd. In enkele gevallen hebben de ontwikkelingen een stimulerend effect op het criminele verschijnsel. Dat is vooral het geval bij sterk gedigitaliseerde criminaliteitsvormen zoals kinderporno en online gokken.

Hoewel een strikt onderscheid tussen de gevolgen van cybercrime en gedigitaliseerde criminaliteit niet te maken is, staat wel vast dat de gevolgen van cybercrime een wijdverbreid probleem vormen, waarvan burgers, bedrijven en overheidsorganisaties slachtoffer worden. De totale schade voor de Nederlandse economie die uit cybercriminaliteit voortvloeit, wordt door McAfee en Deloitte geschat op 8 à 10 miljard euro en dat bedrag zal naar verwachting hoger worden. De ICT-sector en digitale ontwikkelingen, vooral die op het internet, worden volgens het CBS van steeds groter belang voor de Nederlandse economie. Niet alleen economisch, ook persoonlijk en maatschappelijk worden we steeds afhankelijker van het internet. Door deze grotere afhankelijkheid wordt ook de impact van cybercrime op de samenleving groter. De meeste schade komt volgens McAfee en Deloitte voor rekening van bedrijven en overheidsorganisaties. De financiële schade voor burgers is vooralsnog relatief beperkt. Psychische schade kan in individuele gevallen ernstige en soms fatale persoonlijke gevolgen hebben. Alleen al door de groter wordende verbinding met internet in

het dagelijks leven neemt het risico op slachtofferschap toe. Daarnaast worden de persoonlijke gevolgen mogelijk ernstiger, doordat meer (beroeps)criminelen laagdrempelig gebruik kunnen maken van digitale technologieën. Deze criminelen gaan eerder de directe confrontatie met slachtoffers aan dan hacktivisten en cybervandalen.

Kortom,

Binnen het domein van georganiseerde criminaliteit zijn cybercrime en gedigitali-seerde criminaliteit vooral thema-overstijgende werkwijzen die van invloed zijn op de aard en omvang van meerdere criminele verschijnselen en een grote (financiële) impact hebben op de Nederlandse samenleving, nu en in de komende jaren.

De wijdverspreide en groeiende invloed van de digitale ontwikkelingen op de georganiseerde criminaliteit vergroot de reikwijdte van criminelen en draagt bij aan de dreiging van georganiseerde criminaliteit in haar totaliteit.