3 Verschijningsvormen van cybercriminaliteit in enge zin

Jan-Jaap Oerlemans, Wytske van der Wagen & Marleen Weulen Kranenbarg*

3.1 Inleiding

Zoals in hoofdstuk 1 en 2 naar voren kwam, kent cybercriminaliteit veel verschillende verschijningsvormen. In dit hoofdstuk beschrijven wij de belangrijkste verschijningsvormen van cybercriminaliteit in enge zin en gaan na hoe deze gedragingen strafbaar zijn gesteld in het Wetboek van Strafrecht (Sr), waarna we ditzelfde doen in hoofdstuk 4 voor gedigitaliseerde vormen van criminaliteit.

In dit hoofdstuk bespreken we respectievelijk: hacken (computervredebreuk), malware, botnets en ddos-aanvallen. Bij de beschrijving van de verschillende verschijningsvormen wordt veelal gebruikgemaakt van casusmateriaal en/of geven we een beschrijving van (een deel van) het crime script (stappenplan van daders) om een duidelijk beeld te geven van hoe deze soms toch wel technisch complexe vormen van cybercriminaliteit in hun werk gaan. Daarnaast besteden we specifiek aandacht aan de rol van social engineering, het manipuleren van slachtoffers, omdat dit vaak een belangrijk onderdeel is van de modus operandi van cyberdaders. Aan het einde van het hoofdstuk gaan we nog in op toekomstige ontwikkelingen en presenteren we de studievragen en kernbegrippen met betrekking tot cybercriminaliteit in enge zin.

* Prof. mr. dr. J.J. Oerlemans is werkzaam als universitair docent Strafrecht bij het Instituut voor Strafrecht & Criminologie van de Universiteit Leiden. Daarnaast is hij bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht. Dr. W. van der Wagen is als criminoloog gespecialiseerd in cybercriminaliteit. Dr. M. Weulen Kranenbarg is werkzaam als universitair docent Criminologie bij de afdeling Criminologie van de Vrije Universiteit (VU) Amsterdam.

3.2 Strafbaarstelling van cybercriminaliteit in enge zin

Bij cybercriminaliteit in enge zin gaat het om strafbare gedragingen waarbij computers en netwerken zowel het doelwit als middel zijn van criminaliteit. Het gaat hier om gedragingen die de integriteit, beschikbaarheid of exclusiviteit van gegevens in computers aantasten (Commissie-Franken, 1987). De beschikbaarheid heeft betrekking op de opslag, verwerking en overdracht van gegevens. Een ddos-aanval bijvoorbeeld, die een website platlegt (zie paragraaf 3.4), tast de beschikbaarheid van gegevens aan. De integriteit van gegevens heeft betrekking op de juistheid en correctheid van gegevens en programma's. Als een computer wordt gehackt en vervolgens bijvoorbeeld rekeninggegevens in een document worden aangepast, dan tast dit de integriteit van gegevens op een computersysteem aan. De exclusiviteit van gegevens heeft betrekking op het aspect dat onbevoegden geen kennis kunnen nemen van vertrouwelijke gegevens. Ook kan daarbij worden gedacht aan een gehackt computersysteem waarvan vervolgens vertrouwelijke gegevens worden gekopieerd en 'op straat komen te liggen'.

In het kader van de strafbaarstelling van de verschillende delicten die in dit hoofdstuk aan bod komen, is het belangrijk om te bespreken waarom er is gekozen voor nieuwe strafbepalingen voor cybercriminaliteit in enge zin. Omdat de bescherming van de exclusiviteit, vertrouwelijkheid en integriteit van gegevens centraal staat bij deze strafbaarstellingen, had de wetgever ervoor kunnen kiezen de bestaande strafbaarstellingen ten aanzien van *goederen*, ook toepasbaar te laten zijn voor computercriminaliteit die ziet op *gegevens*. Daar heeft hij echter niet voor gekozen. Volgens de Commissie-Franken (1991) konden gegevens namelijk niet als goederen worden aangemerkt, omdat zij op belangrijke punten van elkaar verschillen. Anders dan goederen zijn gegevens het product van geestelijke (en niet van fysieke) arbeid. Bovendien zijn zij 'multipel' (dat wil zeggen te kopiëren), terwijl goederen uniek zijn. Hierdoor kunnen diverse strafbaar gestelde gedragingen, zoals het 'wegnemen' van een goed bij diefstal, wél met goederen worden verricht, maar *niet* met gegevens.

Deze verschillen verklaren waarom er nieuwe bepalingen in het Wetboek van Strafrecht zijn geïntroduceerd of waarom sommige bestaande bepalingen zijn gewijzigd of aangevuld om deze ook toepasbaar te maken in het digitale domein. Ook de plaats en nummering van de strafbaarstellingen van cybercriminaliteit in het Wetboek van Stafrecht valt door dit principe te verklaren. Denk bijvoorbeeld aan het klassieke delict 'zaakbeschadiging' in artikel 350

Sr. Een persoon kan een computer op de grond gooien en die daarmee beschadigen en voldoen aan deze strafbaarstelling. Het is ook mogelijk op afstand in te breken in een computer en slechts een enkel bestand te wijzigen, waardoor de computer of het bestand niet meer werkt. Speciaal voor deze gedraging is een artikel voor gegevensbeschadiging (art. 350a Sr) in het Wetboek van Strafrecht geïntroduceerd. Inmiddels zijn op deze manier na een drietal 'Wetten computercriminaliteit' (zie hoofdstuk 2 voor de geschiedenis rondom het ontstaan van deze wetten) het wegnemen, vernielen, afpersen met en helen van gegevens strafbaar gesteld, net zoals deze gedragingen ook met goederen strafbaar zijn (Kouwenberg, 2024).

Op het uitgangspunt dat gegevens geen goederen zijn, bestaat echter één belangrijke uitzondering. In het Runescape-arrest en navolgende arresten heeft de Hoge Raad bepaald dat gegevens die uniek en op geld waardeerbaar zijn, wél als goed kunnen worden aangemerkt en daarmee 'gestolen' kunnen worden (waarmee sprake kan zijn van diefstal zoals bedoeld in art. 310 Sr).[1]

3.3 Hacken (computervredebreuk)

In de literatuur, vooral in de wat oudere studies, wordt 'hacken' of 'hacking' vaak omschreven als 'een apparaat of machine iets laten doen waarvoor het van origine niet is bedoeld of ontworpen' en 'het oplossen van technische problemen of obstakels' (Steinmetz, 2015a). In deze (originele) betekenissen van hacken, die terug te voeren zijn naar de jaren zestig en zeventig, staat vooral het *creatieve* en *innovatieve* gebruik van technologie (in de ruime zin van het woord dus niet alleen ICT) centraal, een aspect dat ook onderdeel is van de hackerscultuur (Jelsma, 2017).[2] Dergelijke definities van hacken worden bijvoorbeeld nog steeds in zogenoemde 'hackerspaces' gehanteerd: fysieke ontmoetingsplaatsen waar hackers (dus in de ruime zin van het woord) bijeenkomen om met hardware, elektronica en software te knutselen. Dat kan ook gaan om analoge activiteiten als lockpicking of soldeersessies. Het gaat hier dan niet om strafbaar gedrag, bijvoorbeeld omdat de hacker zelf eigenaar is van het apparaat of het systeem. Hoewel er in de media vooral over crimineel hacken wordt gesproken, bestaan er dus ook niet-criminele

1 In het *Runescape*-arrest (HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251) ging het om een virtueel amulet en een masker (die een financiële waarde vertegenwoordigden) die in een spel werden gestolen van een ander personage in het spel.

2 In de oudere studies over het hackerfenomeen is veel aandacht voor de hackerscultuur en de veranderende definitie van hacking (zie bijvoorbeeld Levy, 1984; Taylor, 1999).

varianten van hacken, waar ethisch hacken ook een voorbeeld van is (zie verder paragraaf 3.2.2). De hackersgemeenschap is daarmee dus ook een heterogene groep (zie bijvoorbeeld Althoff et al., 2019; Steinmetz, 2015a). In dit boek focussen we voornamelijk op de strafbare vorm van hacking, oftewel computervredebreuk.

Het delict computervredebreuk (hacken of 'hacking') is een van de meest voorkomende vormen van cybercriminaliteit in enge zin. In de Veiligheidsmonitor 2023 beschrijft het Centraal Bureau voor de Statistiek (CBS) dat in 2023 zes procent van de bevolking slachtoffer is geweest van hacken.[3] Het plegen van computervredebreuk kan op veel verschillende manieren. Bernaards et al. (2012) onderscheiden bijvoorbeeld vier veelvoorkomende manieren om computervredebreuk te plegen, die ook nu nog vaak worden gebruikt.

Ten eerste kan iemand zich de toegang tot een computer of netwerk verschaffen door middel van een slimme list, zoals door middel van social engineering-technieken (zie paragraaf 3.6) waarmee een dader inloggegevens kan bemachtigen en deze kan misbruiken. Denk bijvoorbeeld aan een dader die een slachtoffer een phishing e-mail (zie ook hoofdstuk 4) stuurt waarin het slachtoffer ervan wordt overtuigd om zijn of haar werkinloggevens in te vullen op een phishing website. De dader kan deze inloggegevens vervolgens gebruiken om in te loggen op het netwerk van de werkgever van het slachtoffer.

Ten tweede kunnen daders gebruikmaken van eerder gestolen inloggegevens die op het internet worden aangeboden. Dergelijke gegevens kunnen op veel verschillende manieren zijn gestolen, bijvoorbeeld door grootschalige phishing, maar ook door diefstal van bijvoorbeeld klantgegevens bij bedrijven. Wanneer de inloggegevens niet goed versleuteld zijn opgeslagen in een database en deze database wordt gestolen, dan kunnen deze gegevens worden verhandeld op online criminele marktplaatsen (Madarie et al., 2019; Madarie et al., 2023). Daders kunnen vervolgens deze combinaties van gebruikersnamen en wachtwoorden op verschillende accounts, computersystemen en netwerken uitproberen, omdat veel mensen op verschillende plekken hetzelfde wachtwoord gebruiken.

3 Daarbij moet worden opgemerkt dat veel mensen vaak niet doorhebben dat hun computer is gehackt. Hetzelfde geldt voor de delicten malware en botnets (zie ook hoofdstuk 7). De omvang van daderschap en slachtofferschap van cybercriminaliteit wordt nader besproken in hoofdstuk 5 en 7.

Ten derde kunnen daders gebruikmaken van zogenoemde '*brute force attacks*',[4] waarbij ze veel rekenkracht van een computer gebruiken om een wachtwoord te kraken door heel veel verschillende mogelijke wachtwoorden te proberen. Dit is vooral succesvol wanneer een computersysteem niet is beschermd tegen dergelijke aanvallen en wanneer gebruikers zwakke (korte) wachtwoorden gebruiken. In sommige gevallen is het niet eens nodig om een 'brute force attack' te gebruiken, als er gebruik wordt gemaakt van wachtwoorden die heel makkelijk te raden zijn. Een voorbeeld van een zwak wachtwoord is bijvoorbeeld het wachtwoord van de Amerikaanse president Trump op Twitter dat al na zeven pogingen werd geraden door een Nederlandse ethisch hacker: 'maga2020!'.[5]

Ten vierde kunnen daders toegang krijgen tot een computersysteem of netwerk door gebruik te maken van (bekende) kwetsbaarheden in deze systemen. Vaak wordt hierbij misgebruik gemaakt van computersystemen die verouderde software gebruiken. In deze software zitten dan bekende kwetsbaarheden die nog niet door een update verholpen zijn. Daders maken dan gebruik van bekende manieren waarop er door middel van deze kwetsbaarheden kan worden ingebroken. Er kan echter ook misbruik worden gemaakt van zogenoemde *zero-day* aanvallen. Er is dan een bekende kwetsbaarheid in een systeem, waarvoor nog geen update beschikbaar is (zie bijvoorbeeld Deshpande et al., 2023).

Het plegen van computervredebreuk is niet altijd 'high tech'. Zelfs het aanpassen van een URL (het adres van een webpagina) om toegang te krijgen tot niet-toegankelijk bedoelde delen van een website, kan leiden tot computervredebreuk. In 2012 was het bijvoorbeeld mogelijk de kersttoespraak van toenmalige koningin Beatrix vroegtijdig te lezen door het jaartal in een URL te wijzigen. Dat bleek destijds uit onderstaande tweet:

> '@annejan88: BREAKING: Zojuist kersttoespraak van morgen gevonden met beetje datum ophogen in url. Echt bizar. http://vruc.ht/kersttoespraak-2012...'[6]

4 Dit refereert aan een programma dat geautomatiseerd wachtwoorden kan kraken door tal van combinaties van tekens uit te proberen. Hoe ingewikkelder en langer het wachtwoord, hoe langer het duurt om het te kraken.

5 Maga2020 verwijst naar de slogan van de campagne van Trump: 'Make America Great Again', zie 'Nederlander hackt opnieuw Twitteraccount van president Trump', *NOS*, 22 oktober 2020.

6 'RVD onderzoekt uitlekken kersttoespraak Beatrix', *Elsevier*, 25 december 2012.

In dit geval heeft het Openbaar Ministerie besloten niet te vervolgen voor computervredebreuk of een ander misdrijf, waarschijnlijk omdat de gedraging niet ernstig genoeg werd bevonden in verhouding tot de gevolgen die vervolging van het feit met zich mee zou brengen.

Computervredebreuk kan een zelfstandig delict zijn, maar wordt ook vaak in het kader van andere cyberdelicten gepleegd zoals diefstal van gegevens, botnets en malwareverspreiding en ingezet bij gedigitaliseerde vormen van criminaliteit. Er ontstaat dan vaak een keten van delicten die overgaat van cybercriminaliteit in enge zin naar gedigitaliseerde criminaliteit. Voorbeelden van dit laatste zijn het hacken van accounts van bedrijven (webshops) met als doel geld afhandig te maken van klanten (bijv. door een ander rekeningnummer door te geven) of het hacken van consumentenaccounts met als doel om op hun naam goederen te bestellen en op een ander adres af te laten leveren (Boekhoorn, 2020; Roks & Monshouwer, 2020). In hoofdstuk 4 komt ook de casus 'Veroordeling voor handel op RaidForums aan bod', waarbij de verdachte door middel van hacking gegevens heeft gestolen en deze vervolgens te koop aanbood.

3.3.1 Strafbaarstelling

Hacken is strafbaar gesteld in artikel 138ab Sr (computervredebreuk) als het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk. Deze gedraging is strafbaar gesteld als misdrijf. Op computervredebreuk staat een maximale gevangenisstraf van twee jaar of een geldboete. Als na een 'hack' (het 'binnendringen') gegevens worden overgenomen, is sprake van een strafverzwarende omstandigheid (art. 138ab lid 2 Sr). Ook het gebruikmaken van de computerkracht van de gehackte computers of van reeds gehackte computers als tussencomputer ('proxy') waarvandaan computercriminaliteit wordt gepleegd, kan tot een strafverzwaring leiden (art. 138ab lid 3 Sr).

Het bestanddeel 'opzet' in de delictsomschrijving betekent kortgezegd dat een persoon 'willens en wetens' een gedraging uitvoert. Het bestanddeel 'wederrechtelijk' betekent kortgezegd 'in strijd met het recht'. In de context van computervredebreuk gaat het er bijvoorbeeld om dat een persoon geen toestemming heeft gekregen van de eigenaar van een apparaat om dit te hacken. Daar tegenover staan personen die hacken *met* toestemming. Zij worden ook wel 'ethische hackers' genoemd (zie paragraaf 3.2.2). Deze hackers worden bijvoorbeeld door bedrijven ingehuurd om de beveiliging van hun systemen te testen door computers te 'hacken' om het bedrijf of de instelling vervolgens

van een beveiligingsadvies te voorzien. Personen die bij een bedrijf werkzaam zijn en dergelijke testen uitvoeren, worden ook wel 'penetratietesters' of *pentesters* genoemd. Het hacken gebeurt dan binnen de overeenkomst met de opdrachtgever en is dan niet strafbaar, omdat de wederrechtelijkheid ontbreekt.[7]

Het object waarop de strafbaarstelling ziet, is een 'geautomatiseerd werk'. De term geautomatiseerd werk is het strafrechtelijke begrip voor een computer. De definitie van een geautomatiseerd werk staat in artikel 80sexies Sr. Het gaat kortgezegd om een apparaat of een netwerk van apparaten, waarbij een programma op het apparaat computergegevens verwerkt. Doorgaans betreft het apparaat waarop wordt binnengedrongen een server, PC, laptop of smartphone. De definitie moet breed worden opgevat: ook apparaten die onderdeel uitmaken van een netwerk, zoals een slimme lamp, zijn een geautomatiseerd werk.[8] Het is belangrijk dat in de tenlastelegging staat op welk geautomatiseerd werk is binnengedrongen. Dat is doorgaans een server van bijvoorbeeld een socialemediadienst of een webshop in een datacentrum. Als daarin staat dat op een 'account' wordt binnengedrongen, dan leidt dit in de praktijk tot vrijspraak, omdat 'een account' in juridische zin niet als 'een geautomatiseerd werk' kwalificeert.[9]

Voor computervredebreuk in artikel 138ab Sr is ook vereist dat wordt *binnengedrongen* in een geautomatiseerd werk. Voor de betekenis van deze term wordt aangesloten bij de invulling van het bestanddeel 'binnendringen' bij het delict huisvredebreuk (art. 138 Sr). Als bijvoorbeeld andermans inloggegevens worden gebruikt om in te loggen op een account van het slachtoffer, is sprake van het opzettelijk en wederrechtelijk binnendringen door middel van een 'valse sleutel' in artikel 138ab Sr.[10]

Om van computervredebreuk te kunnen spreken moet dus daadwerkelijk sprake zijn van binnendringen. Een poortscan, waarbij wordt gekeken met welke poorten computers in een netwerk communiceren, is *geen* computervredebreuk.[11] Hackers voeren vaak een poortscan uit in de verkenningsfase ('*reconnaissance*') voordat een systeem wordt gehackt, om te kijken op welke

7 De 'wederrechtelijkheid' van de gedraging vervalt vanwege de toestemming om te hacken zoals dat in de overeenkomst staat.

8 Zie *Kamerstukken II* 2015/16, 34373, nr. 3.

9 Zie bijvoorbeeld Hof Den Haag 22 september 2020, ECLI:NL:GHDHA:2020:2005.

10 Rb. Midden-Nederland 19 november 2020, ECLI:NL:RBMNE:2020:5038, r.o. 5.3.

11 HR 9 april 2019, ECLI:NL:HR:2019:560.

manier een computer kwetsbaar is. Het is bij het delict computervredebreuk niet vereist dat het geautomatiseerd werk in kwestie is beveiligd en een beveiliging wordt doorbroken.

Casus: het Politiemol-arrest

In het zogenoemde Politiemol-arrest legt de Hoge Raad uit dat ook sprake kan zijn van computervredebreuk in de situatie dat een opsporingsambtenaar met een (eigen) gebruikersnaam en wachtwoord een politiesysteem bevraagt zonder dat daarvoor in de uitoefening van zijn politietaak enige aanleiding bestaat.[12]

De opsporingsambtenaar in kwestie had in de periode van 1 januari 2012 tot en met 29 september 2015 door middel van zijn eigen gebruikersnaam en wachtwoord voor de applicatie 'Blue View' zichzelf toegang verschaft tot de servers van de politie en de Belastingdienst.[13] Vervolgens had hij vertrouwelijke informatie uit de applicatie Blue View gehaald, deze op een USB-stick gezet, en doorgegeven aan niet-bevoegde personen. Bij elke export van de gegevens werd de betrokkene gewaarschuwd dat het 'oneigenlijk gebruik dan wel misbruik van de gegevens ten strengste is verboden', net als 'het verstrekken van de gegevens aan niet-geautoriseerde derden'. Na het lezen van de waarschuwing moest de gebruiker op OK drukken. In dat geval is sprake van computervredebreuk gepleegd met behulp van een 'valse sleutel'.

Er is veel kritiek gekomen op dit arrest. Deze kritiek is hoofdzakelijk dat nu wel heel eenvoudig sprake kan zijn van het delict computervredebreuk, zelfs als een eigen gebruikersnaam en inlognaam wordt gebruikt, maar toegang wordt verschaft tot meer gegevens dan waarvoor toestemming is (Berndsen & Visser, 2022). Met de implementatie van de Wet computercriminaliteit III in maart 2019 is verder het opzettelijk en wederrechtelijk overnemen van niet-openbare opgeslagen gegevens in een computer strafbaar gesteld (art. 138c Sr). In een zaak als het

12 HR 30 november 2021, ECLI:NL:HR:2021:1691.

13 Blue View is een indexsysteem, waarmee data vindbaar zijn uit diverse politiesystemen, zoals 'Summ-it', 'Luris' en 'FIU', afkomstig van bijna alle opsporingsinstanties in Nederland (zoals de Kmar, FIOD, enz.).

Politiemol-arrest kan de officier van justitie tegenwoordig ook voor dit delict vervolgen.

3.3.2 Ethisch hacken

Naast de eerdergenoemde pentesters zijn er ook hackers die computersystemen en netwerksystemen testen op hun veiligheid zonder toestemming van de eigenaar. Daarbij is het niet hun doel om misbruik te maken van deze systemen en die gegevens die erop staan, maar om aan te tonen waar kwetsbaarheden in de beveiliging zitten en zo bij te dragen aan de verbetering van deze beveiliging. Deze 'ethische hackers' hebben vaak een sterk ontwikkeld moreel besef en zijn gemotiveerd om systemen veiliger te maken (Noordegraaf & Weulen Kranenbarg, 2023; Spronk & Weulen Kranenbarg, 2020). Ze dienen hiermee een hoger maatschappelijk doel en proberen de samenleving een helpende hand te bieden (Van 't Hof, 2015).

Als er geen sprake is van toestemming, dan kan de gedraging strafbaar zijn en kan worden besloten over te gaan tot vervolging. Rechtbanken beoordelen in dat geval of de gedraging *proportioneel* is geweest (is niet vaker dan nodig computervredebreuk gepleegd, zijn niet meer gegevens ingezien of gedownload dan nodig is om het beveiligingsprobleem aan te kaarten, heeft de hacker de organisatie de mogelijkheid geboden om het probleem te verhelpen voordat dit openbaar werd?) en *subsidiair* is (waren er minder vergaande manieren voorhanden om hetzelfde beveiligingsprobleem aan te kaarten?).

Casus: ethisch hacken van ledenadministratie?

Een 45-jarige verdachte deed in een strafzaak in 2018 een beroep op de rechtvaardigingsgrond van het algemeen belang bij het hacken van de ledenadministratie van een stichting.[14] De website van de stichting was slecht beveiligd, want door het opvragen van het bekende 'robot.txt-bestand' van de webserver waren 80.000 donateursgegevens beschikbaar. In de gegevensset waren ook NAW-gegevens (naam, adres, woonplaats), bankrekeningnummers, e-mailadressen en opmerkingen over

14 Rb. Den Haag 30 augustus 2018, ECLI:NL:RBDHA:2018:10451.

het betaalgedrag van donateurs te vinden. De verdachte heeft deze informatie direct gedeeld met de media.

De rechtbank overweegt dat de verdachte willens en wetens de beveiliging van de website omzeilde en de gegevens heeft opgevraagd door een geldig ID in te voeren. De rechtbank vindt dat de verdachte niet proportioneel heeft gehandeld door de hele database binnen te halen (in plaats van slechts enkele records) en door meteen naar de media te stappen in plaats van naar de betrokken stichting zelf. De rechtbank houdt wel rekening met de persoonlijkheid van de dader en de omstandigheden waaronder het feit is begaan. De verdachte had geen kwade bedoelingen, heeft de gegevens uit de database niet voor eigen gewin gebruikt en diende een maatschappelijk belang. De verdachte is daarop veroordeeld voor computervredebreuk, maar kreeg geen straf opgelegd.

Coordinated Vulnerability Disclosure-richtlijn

Om hackers te stimuleren om binnen de juridische ruimte kwetsbaarheden in systemen aan te tonen en die te melden bij de betrokkene en om vervolging te voorkomen heeft het Nationaal Cyber Security Centrum een richtlijn opgesteld: de 'Leidraad Coordinated Vulnerability Disclosure' (NCSC, 2013; 2018; Van der Ham & Terra, 2023). Nederland loopt hiermee al sinds 2013 voorop in het stimuleren van ethisch hacken (destijds Responsible Disclosure genoemd) en inmiddels gebeurt dit ook in andere landen zoals de Verenigde Staten (zie The National Law Review, 2022 en in de internationale standaard ISO/IEC/TR 5895:2022).[15]

Het doel van de richtlijn is bij te dragen aan de veiligheid van ICT-systemen door ethische hackers hun kennis over kwetsbaarheden te laten delen met de eigenaren van ICT-systemen. De eigenaren kunnen dan de kwetsbaarheden verhelpen voordat deze actief worden misbruikt door derden. Hierna wordt in de regel de kwetsbaarheid openbaar gemaakt, zodat ook anderen gebruik kunnen maken van deze kennis om hun systemen beter te beveiligen. In de Leidraad staat omschreven dat de organisatie en melder kunnen overeenkomen dat er geen aangifte wordt gedaan (van in de eerste plaats computervredebreuk), zolang de melder binnen de randvoorwaarden van het beleid van het bedrijf of de instelling opereert. Om deze randvoorwaarden duidelijk

15 Zie iso.org/standard/81807.html.

te maken kunnen bedrijven een CVD-beleidstekst op hun webpagina zetten, waarin ze de randvoorwaarden en contactgegevens kunnen vermelden.[16] Het Openbaar Ministerie zegt daarnaast toe dat het in zijn beslissing tot het al dan niet instellen van strafrechtelijk onderzoek meeweegt of het 'Coordinated Vulnerability Disclosure'-beleid is nagekomen.

Vanuit een rationelekeuzeperspectief (zie ook hoofdstuk 10) is het relevant om te benadrukken dat dit beleid nog in ontwikkeling is en dat er belangrijke voor- en nadelen kleven aan het melden van ICT-kwetsbaarheden (Van der Ham & Terra, 2023; Weulen Kranenbarg et al., 2018a). Zo blijken jonge ethische hackers uit angst voor vervolging of frustratie over de communicatie met ICT-eigenaren lang niet altijd melding te maken van kwetsbaarheden die zij vinden (Noordegraaf & Weulen Kranenbarg, 2023; Spronk & Weulen Kranenbarg, 2020; Van der Wagen et al., 2019; zie ook hoofdstuk 5 en 10).

3.4 Malware

Malware is een verzamelnaam voor verschillende typen kwaadaardige software, zoals virussen, wormen en Trojaanse paarden. Een virus verwijst naar kwaadaardige software die computersystemen infecteert. Kenmerkend is dat het (in tegenstelling tot een worm) een handeling vereist van de computergebruiker, zoals het openen van een e-mailbijlage met de malware. Een worm, daarentegen, is kwaadaardige software die *zichzelf* verspreidt binnen een netwerk van computers. Een Trojaans paard (de naam heeft haar oorsprong in de Griekse mythologie) is een onschuldig lijkend programma of bestand dat malware bevat, zoals een e-mailbijlage met een Word-document met een onschuldig lijkende bestandsnaam zoals een factuur. Zodra dit bestand wordt geopend of extra opties ('macro's') in een Office-document worden geactiveerd, raakt het systeem geïnfecteerd (Holt et al., 2015).[17]

Vroeger werd een strikt onderscheid gemaakt tussen virussen, wormen en Trojaanse paarden, maar tegenwoordig heeft kwaadaardige software vaak kenmerken van al deze typen: de kwaadaardige software wordt geactiveerd na het klikken op een link naar een website of het openen van een e-mailbijlage (een virus), kan zichzelf verspreiden op andere computers (kenmerkend voor wormen), en doet zich vaak voor als onschuldig lijkend programma

16 Zie de voorbeeldtekst op https://responsibledisclosure.nl/.

17 Zie ook bijvoorbeeld Rb. Rotterdam 19 maart 2020, ECLI:NL:RBROT:2020:2395, *Computerrecht* 2020/88, m.nt. J.J. Oerlemans (Rubella Macro malware).

(Trojaans paard). Daarom wordt tegenwoordig meestal de verzamelterm 'kwaadaardige software' (in het Engels *malicious software*) gebruikt, kortweg 'malware' (Koops & Oerlemans, 2019a).

Malware bevat vaak vele functionaliteiten die een cybercrimineel van dienst kunnen zijn. Denk daarbij bijvoorbeeld aan het plaatsen van een achterdeurtje (*back door*) om toegang te krijgen tot een computer of andere kwaadaardige software te downloaden, het maken van *screenshots*, het aanzetten van een microfoon of camera, of het overnemen of wijzigen van gegevens (Bernaards et al., 2012).[18] Een ander voorbeeld is het registreren van toetsaanslagen waarmee hackers bijvoorbeeld inlognamen en wachtwoorden kunnen afvangen om daarmee later een beveiliging te doorbreken.

Er zijn veel soorten malware met een of meer van deze functionaliteiten in omloop. We bespreken achtereenvolgens *info-stealers*, *ransomware* en *banking malware*. De eerste twee soorten komen volgens Europol (2017, 2018; 2020; 2021) het frequentst voor. Daarnaast is banking malware lange tijd een hardnekkig probleem geweest, maar komt dit mede door de maatregelen van banken steeds minder vaak voor.

3.4.1 Info-stealers

De eerste veelvoorkomende vorm van malware zijn info-stealers. Deze zijn gericht op het kopiëren van gegevens op een geïnfecteerd computersysteem. Het gaat dan vaak om waardevolle gegevens, zoals inlognamen, wachtwoorden en persoonsgegevens die zijn ingevoerd in webbrowsers. Het gebruik van dergelijke info-stealers is het begin van een keten van delicten, waarbij daders de gestolen gegevens gebruiken om vervolgens bijvoorbeeld oplichting te plegen of aankopen te doen op naam van het slachtoffer.

Casus: Operatie Cookie Monster

Op 5 april 2023 werd tijdens de internationale politieoperatie 'Cookie Monster' de online handelsplaats 'Genesis Market' opgerold. De FBI, Europol en – onder andere – de Nederlandse politie werkten samen in dat onderzoek dat leidde tot doorzoekingen in zeventien landen wereld-

18 Het afluisteren of onderscheppen van communicatieverkeer met malware is overigens strafbaar op grond van, onder andere, art. 139c Sr.

wijd. Op Genesis Market werden miljoenen gebruikersprofielen van slachtoffers verkocht, waaronder van ongeveer 50.000 Nederlanders.

De website Genesis Market verkocht gebruikersprofielen met bijbehorende zogenoemde *fingerprints* van de slachtoffers. Fingerprints zijn kenmerkende gegevens van de apparaten waar personen gebruik van maken. Genesis Market bevatte een unieke digitale vingerafdruk van een geïnfecteerde computer (een *bot*), inclusief afgevangen inlognamen en wachtwoorden, browsergegevens en cookies, die door middel van malware van het type info-stealer verkregen waren van nietsvermoedende slachtoffers. Met behulp van de aangekochte gegevens kon een koper (de dader) inloggen op bijvoorbeeld een account van een slachtoffer bij een webwinkel en vervolgens malafide bestellingen doen als zijnde het slachtoffer, al dan niet met de aan het account van het slachtoffer gekoppelde betalingsdiensten. Ook kon met de gegevens de digitale identiteit van een geïnfecteerde computer nauwkeurig worden nagebootst. Door gebruik te maken van deze digitale identiteit konden antifraudesystemen bij websites worden misleid en leek het voor deze websites alsof de originele gebruiker inlogt. Op deze manier kon de gebruiker die de bot had aangeschaft misbruik maken van de gegevens die op de geïnfecteerde computer waren aangetroffen. Zolang een computer met malware geïnfecteerd was, werden ook eventuele wijzigingen van wachtwoorden doorgegeven aan Genesis Market.

In Nederland werden zeventien verdachten aangehouden. De rechtbank Den Haag veroordeelde bijvoorbeeld een verdachte tot twee jaar gevangenisstraf (waarvan acht maanden voorwaardelijk) voor het verwerven en voorhanden hebben van niet-openbare gegevens (heling van gegevens (art. 139g Sr)), identiteitsfraude (art. 231b Sr) en computervredebreuk (art. 138ab Sr).[19] De verdachte kocht 1029 bots op Genesis Market. Na het verkrijgen van de bots zijn de gegevens gebruikt door bij verschillende webshops – zoals Bol.com en Mediamarkt.nl – op de accounts van anderen in te loggen en (veelal) luxeproducten te bestellen onder hun naam en op hun kosten. Hij is hierbij volgens de rechtbank 'op listige en bedrieglijke wijze' te werk gegaan: hij liet de bestellingen afleveren op een ander adres dan die van zijn slachtoffers

19 Rb. Den Haag 19 september 2023, ECLI:NL:RBDHA:2023:14140.

en logde meteen na het plaatsen van de bestellingen in op de e-mailaccounts van de slachtoffers om de bevestigingsmail van zijn zojuist geplaatste bestelling te verwijderen.

3.4.2 Ransomware

De tweede veelvoorkomende vorm van malware is ransomware. Ransomware, ook wel 'gijzelsoftware' genoemd, is malware die bestanden op een computer onbruikbaar maakt door deze te versleutelen. Het slachtoffer (vaak een bedrijf) moet losgeld betalen om de bestanden weer te (laten) ontsleutelen. Na betaling, meestal in de *cryptocurrency bitcoin*, kunnen slachtoffers weer toegang krijgen tot de bestanden met een toegestuurde sleutel (Oerlemans et al., 2016; Van der Wagen & Pieters, 2020).

Net als bij veel andere offline en online delicten wordt bij het uitvoeren van een ransomwareaanval een reeks stappen gevolgd, ook wel het *crime script* genoemd: van de ontwikkeling en/of aankoop van de ransomware zelf, het verkrijgen van toegang, infectie, encryptie, afpersing, cash-in, tot witwassen en cash-out. Matthijsse et al. (2023) geven in hun beschrijving van het crime script van ransomware inzicht in het achterliggende ecosysteem dat ransomware faciliteert. Zij laten zien hoe daders elkaar vaak ontmoeten op ondergrondse forums. Dadergroepen zijn ofwel autonoom en doen alles zelf of besteden delen van het crime script uit. Veel aanvallers verkrijgen bijvoorbeeld niet langer zelf toegang, maar kopen toegang tot systemen van anderen (*initial access brokers*). Bovendien is het gebruikelijk geworden dat aanvallers gegevens exfiltreren (dat wil zeggen het overhevelen van gegevens van het slachtoffernetwerk naar de dader), voordat de systemen worden versleuteld. Hiermee worden slachtoffers nog verder onder druk gezet om te betalen, omdat wordt gedreigd met het openbaar maken van deze gegevens. Ook komt het voor dat klanten van een bedrijf worden gebeld of dat bestuursleden en hun familie met geweld worden bedreigd (Cybersecuritybeeld Nederland, 2023). Het crime script laat ook zien hoe de opbrengsten van het losgeld niet alleen worden gebruikt om daders in het netwerk en samenwerkingspartners te betalen, maar ook om te herinvesteren in de ransomwarecampagne, bijvoorbeeld om te betalen voor hostingdiensten of licenties om van hacking tools of malware gebruik te kunnen maken.

Europol wijst al jaren achtereen ransomware aan als de 'nummer 1' populairste malware onder cybercriminelen (Europol, 2017, 2018, 2019, 2020 en 2021). Daarnaast levert het ook steeds meer schade op, aangezien het bedrijf ChainAlysis in 2016 het totaal aan ransomwarebetalingen inschatte op 24 miljoen dollar en dat in 2023 al is opgelopen naar meer dan een miljard dollar (ChainAlysis, 2024). Wat hier mogelijk ook mee samenhangt, is dat ransomware op dit moment vooral veel voorkomt onder bedrijven. Naast het betalen van het losgeld bestaat de schade zeker bij bedrijven natuurlijk ook uit het opnieuw opbouwen van de ICT-infrastructuur (als niet wordt betaald of alsnog na betaling), het verlies van productiviteit door onbruikbare computersystemen, het inhuren van cybersecuritybedrijven, het verlies van gegevens (als ook gegevens worden gekopieerd), eventuele reputatieschade als de aanval publiekelijk bekend wordt en de niet in geld uit te drukken emotionele impact die ransomwareaanvallen met zich meebrengen (Button et al., 2021). Het 'succes' van ransomware valt te verklaren door het feit dat personen en organisaties al snel bereid zijn te betalen voor gegevens die niet meer toegankelijk zijn. In het verleden ging het bijvoorbeeld om familiefoto's of vakantiefoto's van particulieren die waren versleuteld. Steeds vaker worden echter grote instellingen (zoals gemeenten) of bedrijven aangevallen, waarbij de gehele administratie en back-ups worden versleuteld. Daarbij kunnen daders in één keer veel meer losgeld vragen. Ook is ransomware door de jaren heen steeds geavanceerder geworden. Waar het aanvankelijk nog volledig afhankelijk was van *social engineering* (manipulatie/deceptie, zie ook paragraaf 3.4) om slachtoffers over te halen te betalen (de bestanden waren in theorie nog wel zonder sleutel te ontsleutelen), is het sinds de komst van *cryptolocker* voor slachtoffers onmogelijk om zonder de sleutel weer toegang te krijgen tot hun gegevens en moet men wel echt kiezen tussen twee kwaden: geld betalen of alle gegevens verliezen (Van der Wagen & Pieters, 2020).

Europol signaleert dat de aanvallen met ransomware in de periode 2015-2020 bovendien gerichter, winstgevender en schadelijker zijn geworden (Europol, 2019). De aanval op de computers van de Universiteit Maastricht rond Kerstmis 2019 was zo'n gerichte aanval en leidde tot uitval van alle computers van studenten en medewerkers, met versleuteling van onderzoeksgegevens, persoonsgegevens van studenten en docenten, en de universiteitsadministratie. De universiteit koos ervoor om 200.000 euro aan losgeld te betalen om meer schade te voorkomen. Gijzelbedragen van meer dan één miljoen euro in bitcoin komen helaas ook voor. De universiteit van Maastricht kwam er uiteindelijk nog niet zo slecht van af, want in 2022 kwam de politie een deel van het losgeld in cryptovaluta op het spoor die flink in waarde gestegen

waren.[20] De universiteit kreeg het losgeld volledig (of zelfs met winst) terug. Dit is uiteraard een zeldzaamheid, want de meeste bedrijven zien helaas niets van het betaalde geld terug.

Nederland kent tot nu toe slechts drie (gepubliceerde) veroordelingen voor ransomware in twee verschillende zaken.[21] Het schaarse aantal veroordelingen is voornamelijk te verklaren door jurisdictieproblemen die zich voordoen wanneer de daders van cybercriminaliteit zich in het buitenland bevinden, wat bij ransomware gepleegd door georganiseerde groepen vaak lijkt voor te komen (Martin & Whelan, 2023; zie verder hoofdstuk 9 over digitale opsporing). Wel heeft de Nederlandse politie deelgenomen in enkele internationale operaties om ransomware te bestrijden. Naar aanleiding van deze operaties is enkele keren de ICT-infrastructuur van ransomwaregroepen ontmanteld en de administratie op deze computers in beslag genomen, zijn virtuele valuta in beslag genomen en enkele personen gearresteerd.[22]

3.4.3 Banking malware

Een derde vorm van malware die een aantal jaren regelmatig voorkwam, ook in Nederland, betreft banking malware (Leukfeldt et al., 2017c). Bij banking malware proberen cybercriminelen banktransacties af te vangen en worden transacties op het internet (semi)automatisch doorgesluisd naar tussenrekeningen. In dit kader maken daders vaak gebruik van zogenoemde *injects*, code die als het ware in de browser wordt 'geïnjecteerd' en de gebruiker een nagemaakte bankpagina toont (Van der Wagen & Bernaards, 2018). Een andere mogelijkheid is het gebruik van zogenoemde Remote Access Tools (RAT), een veelgebruikte tool (ook door hackers) die het mogelijk maakt om computers op afstand over te nemen en de inloggegevens te verkrijgen. Een voorbeeld hiervan was een zaak uit 2017, waarbij het crime script er als volgt uitzag:

20 Zie bijvoorbeeld: 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld', *NOS.nl*, 2 januari 2020.

21 Zie Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6152 en Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153. Zie ook Rb. Amsterdam 3 november 2023, ECLI:NL:RBAMS:2023:6967.

22 Zie, o.a. Europol, 'Five arrested for spreading ransomware throughout Europe and US', 20 december 2017 (met betrekking tot 'CTB-Locker'); 'International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war', 28 november 2023 (met betrekking tot HIVE en Dharma ransomware); 'Law enforcement disrupt world's biggest ransomware operation', 20 februari 2024 (met betrekking tot LockBit).

> 'Eenmaal geïnfecteerd (met de malware njRAT) meldden de besmette computers zich aan op het beheerderspaneel dat op de computer van de verdachte geïnstalleerd was. Op dat moment was het voor de verdachte of zijn mededader(s) mogelijk om mee te kijken op het computerscherm van het slachtoffer en kon de verdachte of zijn mededader(s) ook de controle over de muis en het toetsenbord overnemen. Ook hield de RAT bij welke toetsaanslagen er allemaal op het toetsenbord van de besmette computer werden gemaakt. Op deze wijze verkregen de verdachte en zijn mededader(s) wachtwoorden en andere inloggegevens waarmee zij konden inloggen op de [bank]-internetbankieromgevingen van bedrijven.
>
> Vervolgens veranderden de verdachte en zijn mededader(s) de bankrekeningnummers met betrekking tot betaalopdrachten in het kader van o.a. loonuitbetalingen, die in de [bank]-internetbankieromgeving klaarstonden om te worden verwerkt. Door het veranderen van de bankrekeningnummers zorgden zij ervoor dat de gelden niet op de bankrekeningen van de rechthebbenden terechtkwamen, maar op de bankrekeningen van geldezels (ook wel money mules of katvangers genoemd), die door de verdachte en zijn mededader(s) waren geworven. Daarna werd geld door de verdachte en zijn mededader(s) vanaf die bankrekeningen opgenomen en gecasht.'[23]

Door nieuwe maatregelen van banken (zoals tweefactorauthenticatie) komt banking malware niet meer in dezelfde mate voor. Toch weten cybercriminelen deze maatregelen soms wel te omzeilen. Zo wordt bankingmalware bijvoorbeeld steeds vaker via malafide apps verspreid, waarbij geautomatiseerd geld van bankrekeningen kan worden afgeschreven.[24]

Kortom, malware komt in verschillende hoedanigheden voor (in deze paragraaf zijn slechts enkele belangrijke voorbeelden besproken) en richt veel schade aan. Het zal in de toekomst nog wel een hardnekkig probleem blijven, onder andere omdat virusscanners de nieuwste malwarevarianten vaak niet kunnen detecteren en de ontwikkelingen lastig bij te benen zijn.[25] Daarnaast is het gebruik van AI een zorgelijke ontwikkeling in het kader van malware. AI kan een rol spelen bij het maken van malware, maar er ook voor zorgen dat het lastiger detecteerbaar is (zie ook hoofdstuk 2).

---

23 Zie Rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m.nt. J.J. Oerlemans en Hof Den Haag 30 maart 2021, ECLI:NL:GHDHA:2021:587).

24 'Nederlandse bank-apps doelwit van volautomatische Android-malware', *Security.nl*, 10 maart 2023.

25 'Malware-markt wordt nog steeds onderschat', *Computable.nl*, 29 augustus 2008.

3.4.4 Strafbaarstelling

Het opzettelijk en wederrechtelijk installeren van malware op een geautomatiseerd werk is strafbaar als computervredebreuk (daarbij kan bijvoorbeeld sprake zijn van binnendringen met een 'technische ingreep' als bedoeld in art. 138ab lid 1 Sr). Het installeren van malware is ook strafbaar gesteld als het delict 'gegevensaantasting'. Dat is het opzettelijk en wederrechtelijk toevoegen van gegevens aan een computer in artikel 350a lid 1 Sr. Als het geautomatiseerde werk door de malware onbruikbaar wordt, is doorgaans ook artikel 350c Sr van toepassing. Naast deze bepalingen die gaan over het gebruik van malware op specifieke systemen, is ook het verspreiden van malware strafbaar gesteld in artikel 350a lid 3 Sr. Het voorhanden hebben van malware met het oogmerk computervredebreuk te plegen is verder nog strafbaar gesteld in artikel 139d lid 2 sub a Sr.

Na de implementatie van de EU-richtlijn over aanvallen op informatiesystemen in 2013[26] is het artikel voor ddos-aanvallen (zie paragraaf 3.6) in artikel 138b Sr ingrijpend gewijzigd en zijn er daarnaast voor verschillende vormen van computercriminaliteit strafverzwaringen doorgevoerd. Als een computerdelict, zoals gegevensaantasting (art. 350a Sr) en de ontoegankelijkheidsmaking van gegevens (350a Sr) wordt gepleegd 'met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen' (kortgezegd: het delict wordt gepleegd om er geld aan te verdienen) dan geldt een hogere gevangenisstraf van ten hoogste drie jaar of een geldboete van de vierde categorie. Als deze delicten 'ernstige schade veroorzaken', geldt een strafverzwaring naar een maximale gevangenisstraf van vijf jaar of een geldboete van de vierde categorie. Van het gebruik van malware ter uitvoering van terroristische misdrijven, zoals bedoeld in artikel 138b Sr, is in Nederland tot nu toe nog geen sprake geweest.

26 Richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ.

Casus: CoinVault

Figuur 3.1 Screenshot van CoinVault-ransomware

Bovenstaand figuur is een screenshot van een computer die besmet is met CoinVault-ransomware. Net als bij veel andere ransomware is een bericht te zien waarin staat dat de computerbestanden van het slachtoffer zijn versleuteld. De bestanden kunnen slechts worden ontsleuteld als een bedrag in bitcoins wordt overgemaakt naar de daders. Met de sleutel kunnen slachtoffers de bestanden op een computer ontsleutelen. Een timer loopt af om te laten zien hoeveel tijd de slachtoffers nog hebben om het bedrag van een halve bitcoin (destijds 164,64 euro) te betalen. Bij CoinVault bestond ook de mogelijkheid om één bestand als test gratis te laten ontsleutelen en bevatte het informatiescherm een knop met meer informatie over hoe de betaling met bitcoin moet plaatsvinden. Voor de dader is dit een strategie om slachtoffers aan te moedigen te betalen, waarmee het 'businessmodel' dus meer kans van slagen heeft.

In de 'CoinVault'-zaak zijn twee Nederlandse jongemannen (ze waren broers) veroordeeld voor afpersing met gijzelsoftware. CoinVault was een van de vroegere vormen van ransomware en richtte zich vooral op de bestanden op individuele Windows PC's. Uit mediaberichten over de zaak blijkt dat de verdachten de malware als trojan hebben verspreid. In dit geval was de malware verstopt in populaire commerciële software

en 'sleutelgeneratoren' voor games, die werden aangeboden in nieuwsgroepen op internet. Nadat duizenden computers waren besmet activeerden de verdachten de cryptoware en eisten ze ongeveer 250 euro in bitcoin van hun slachtoffers. De daders hadden de ransomware zelf vervaardigd en maakten gebruik van het anonimiseringsnetwerk 'Tor' (zie hoofdstuk 4). In een enkel geval was dit echter niet geactiveerd en verwees het IP-adres terug naar de houder van het internetabonnement (deze stond op naam en het adres van het ouderlijk huis van de verdachten). Dat leidde tot de arrestatie van de verdachten in een klein dorp bij Amersfoort.[27]

In deze zaak had de officier van justitie computervredebreuk (art. 138ab Sr), gegevensaantasting (art. 350a Sr) en afpersing (art. 317 Sr) ten laste gelegd. De daders kregen in deze zaak 240 uur taakstraf en een voorwaardelijke gevangenisstraf van twee jaar opgelegd. Ook moesten zij aan verschillende mensen een schadevergoeding betalen. Dat is een relatief milde straf gezien de ernst van de gedraging en de maximale gevangenisstraf van negen jaar voor het delict afpersing (art. 317 lid 2 Sr). Ook de rechtbank overweegt in het vonnis dat er sprake is van 'zeer ernstige feiten en dat eigenlijk een forse gevangenisstraf op zijn plaats is'. Maar omdat het proces vertraging had opgelopen (er waren bijna drie jaar verstreken sinds hun aanhouding), en vanwege het feit dat zij volledig hadden meegewerkt aan het politieonderzoek en het beperken van de (digitale) schade, een blanco strafblad hadden en ook geen nieuwe strafbare feiten hadden gepleegd, legde de rechtbank geen onvoorwaardelijke gevangenisstraf op.[28]

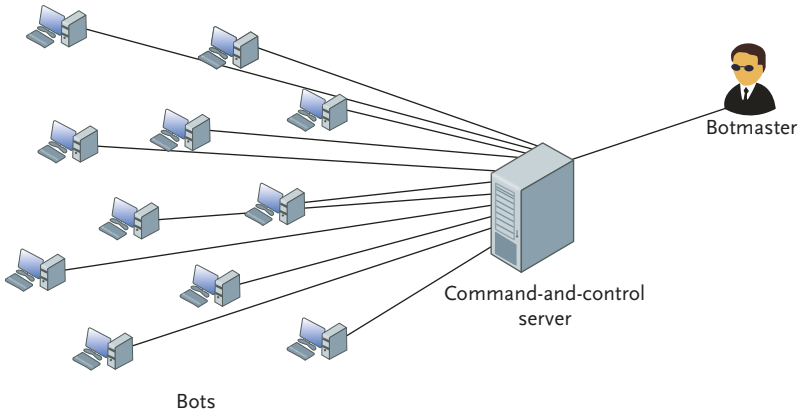
3.5 Botnet

Een botnet is een netwerk van met malware geïnfecteerde computers dat door een of meer beheerders (ook wel botherder of botmaster genoemd) wordt

27 Zie voor enige achtergrond over de verdachten: T. Kreling, 'Het begon als kick, maar liep volstrekt uit de hand: broers voor de rechter voor afpersen met gijzelingssoftware', *Volkskrant.nl*, 12 juli 2018.

28 Zie uitgebreid Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, m.nt. J.J. Oerlemans (*CoinVault*-zaak).

aangestuurd (Bernaards et al., 2012, p. 45). Hoe een eenvoudig (centraal aangestuurd) botnet eruitziet, is weergegeven in figuur 3.2.



Figuur 3.2 Eenvoudig model van een botnet (bron: Plohmann et al., 2011)

Zoals ook al beschreven met betrekking tot malware kunnen computers op verschillende manieren besmet raken en onderdeel worden van een botnet. Dit kan bijvoorbeeld via het openen van een kwaadaardige bijlage in een e-mail, maar ook via websites die je bezoekt.

Hieronder zetten Van der Wagen en Bernaards (2018, p. 59-60) uiteen hoe het crime script eruitziet van botherders die gebruikmaken van dergelijke zogenoemde *exploit kits*:

'Om (computer)systemen te compromitteren en zo zijn of haar botnet op te bouwen kan de herder gebruikmaken van een exploit kit. Dergelijke kits draaien op een website en scannen de (computer)systemen van websitebezoekers op kwetsbaarheden om die uit te buiten. Voor de beheerder van een exploit kit is het uiteraard van belang dat er daadwerkelijk bezoekers op de website afkomen waar de exploit kit op draait. Het verkeer naar een website met een exploit kit wordt ook wel *traffic* genoemd, een specialisme dat verzorgd wordt door *traffickers*. Traffic wordt onder meer gegenereerd door *malvertising*: hierbij laat de trafficker een advertentie verspreiden onder bezoekers van een (legitieme) website. De advertentie leidt de gebruiker vervolgens naar een malafide

website waar de exploit kit het omgeleide (computer)systeem opwacht. Een exploit kit beheerder wil vaak specifieke traffic hebben zodat de kit vanuit zijn perspectief de meeste kans op succes heeft. Afhankelijk van het soort exploit kit is hij bijvoorbeeld vooral geïnteresseerd in traffic van (computer)systemen met een specifieke *user agent* (kenmerken van het betreffende systeem), waaruit blijkt dat gebruiker mogelijk een besturingssysteem heeft met kwetsbaarheden die door de exploit kit kunnen worden uitgebuit. Een uiteindelijk succesvol geïnfecteerd (computer)systeem wordt ook wel een *install* of *load* genoemd.'

De botherder stuurt via een server – de *command-and-control-server* genoemd – de geïnfecteerde computers aan en verhuurt doorgaans delen van het botnet aan derden om er geld mee te verdienen (Van der Wagen & Pieters, 2015). De geïnfecteerde computers worden ook wel 'zombiecomputers' genoemd, omdat zij onder controle staan van de botherder. Er bestaan ook botnets die niet zozeer centraal aangestuurd worden, maar een zogenoemde *peer-to-peer* infrastructuur hebben (Gao et al., 2022). In dat geval wordt geen gebruik gemaakt van een command-and-control-server (waarbij de botherder rechtstreeks commando's geeft aan de bots in het netwerk), maar geven de bots als het ware commando's aan elkaar (het principe van *self-propagation of commands*). Deze botnets hebben een complexere infrastructuur en zijn dan ook lastiger om te detecteren en te ontmantelen. Ook bestaan er botnets die zowel centraal als peer-to-peer zijn opgebouwd, ook wel een hybride infrastructuur genoemd (Plohmann et al., 2011; Wagenaar, 2012). Al deze infrastructuren hebben hun eigen kwetsbaarheden (zie Gao et al., 2022). Om deze reden maken cybercriminelen de laatste jaren ook gebruik van zogenoemde *internet of things (IoT) devices* (apparaten verbonden met het internet, zie ook paragraaf 3.8) om hun acties te verhullen (Tanabe et al., 2020).

Botnets worden ook wel de 'werkpaarden van cybercriminelen' (Oerlemans et al., 2016) of het 'Zwitserse zakmes van cybercriminaliteit' (Bernaards et al., 2012) genoemd, omdat ze op veel verschillende manieren gebruikt kunnen worden om (crimineel) geld te verdienen. Daarbij kan worden gedacht aan het vergaren van persoonsgegevens (zoals we ook al in de casus Cookie Monster zagen), het beheren van met ransomware geïnfecteerde computers, het installeren van banking malware, en het beheren van virtueel geld dat door geïnfecteerde computers wordt gecreëerd door bijvoorbeeld *mining malware* (Wagenaar, 2012). Mining malware maakt gebruik van de verwerkingskracht

van computers om via berekeningen nieuw virtueel geld te maken (zie hoofdstuk 4 over virtuele valuta) (Pastrana & Suarez-Tangil, 2019; Tekiner et al., 2021). Botnets worden tot slot ook vaak gebruikt om ddos-aanvallen mee uit te voeren, een vorm van cybercriminaliteit waarop in de volgende paragraaf verder wordt ingegaan.

Botnets lijken derhalve een goede illustratie van het geautomatiseerde karakter van cybercriminaliteit in enge zin, zoals besproken in hoofdstuk 2. Aan de ene kant vinden veel processen geautomatiseerd plaats (denk aan het besmetten van computers) en aan de andere kant kunnen botnets, zoals bijvoorbeeld bij ddos-aanvallen, fungeren als *force multiplier*. Van der Wagen & Pieters (2015) spreken in dit kader over het hybride of 'cyborgachtige' karakter van botnets waarmee ze bedoelen dat zowel mens als machine het botnet creëert als in standhoudt. Ze focusten in hun onderzoek op de verweving en interactie tussen menselijke en technische entiteiten in het Bredolab[29] botnet en beschrijven dat dit botnet alleen succesvol ontmanteld kon worden door zowel de botherder te arresteren, de infrastructuur offline te halen, als de individuele besmettingen op te heffen. Dit principe geldt voor vrijwel alle botnets: als niet alle drie de elementen gestopt worden, blijft het botnet bestaan of kan als het weer 'tot leven komen'. Dit laatste was bijvoorbeeld het geval bij het Conficker botnet. Hoewel een grootschalige internationale politieactie dit botnet en zijn controlesysteem had uitgeschakeld, bleef het steeds opnieuw opduiken.[30] Dit had ermee te maken dat er nog veel geïnfecteerde bots in omloop waren (Van der Wagen & Bernaards, 2018). In hoofdstuk 8 wordt nader ingegaan op het cyborg crime-perspectief dat voortvloeide uit deze botnetstudie.

3.5.1 Strafbaarstelling

Voor de ingebruikname van een botnet, of het nu om een centraal aangestuurd of peer-to-peer botnet gaat, moet computervredebreuk worden gepleegd. De Hoge Raad heeft in het Toxbot-arrest in 2011 nog eens duidelijk gemaakt dat bij het gebruik van een botnet sprake is van een gekwalificeerde vorm van computervredebreuk (art. 138ab lid 3 sub b Sr) als door de verdachte

29 Zie A. Kadiev, 'End of the line for the Bredolab Botnet', *Securelist.com*, 20 december 2010 en de Graaf et al. (2013).

30 'Miljoenen nieuwe ip-adressen onderdeel van twee botnets', *Security.nl*, 29 oktober 2018.

voor het creëren van een botnet ook computers geïnfecteerd worden met malware (Oerlemans & Koops, 2011).[31]

Als gevolg van de eerdergenoemde EU-richtlijn over aanvallen op informatiesystemen[32] is het creëren van een botnet van geïnfecteerde computers strafbaar gesteld met maximaal drie jaar gevangenisstraf.[33]

3.6 Ddos-aanval

Bij een ddos-aanval bezoeken vele computers tegelijk een andere computer, zoals een server van een website, waarna deze webserver overbelast raakt. Ddos-aanvallen zijn populair bij doorgewinterde cybercriminelen, maar bijvoorbeeld ook bij tieners die zich vervelen of geen examen op een computer willen maken op een bepaalde datum en tieners die het hun tegenspelers lastig willen maken bij het gamen.[34] Cybercriminelen die uit zijn op financieel gewin, maken er bijvoorbeeld gebruik van als vorm van afpersing bij webwinkels, cryptowisselkantoren en online gokwebsites (Europol, 2021).[35] Dit soort websites moeten voor hun inkomsten online blijven en zijn vaak bereid daarvoor geld te betalen. De eerder besproken hacktivisten leggen bepaalde websites plat vanuit ideologische of politieke beweegredenen (zie ook hoofdstuk 2 en hoofdstuk 5).

Het plegen van ddos-aanvallen betreft een vorm van cybercriminaliteit die volgens het NCSC de laatste jaren steeds vaker in Nederland voorkomt (NCSC, 2020).[36] Een ddos-aanval kan grote gevolgen hebben. In de afgelopen jaren is in Nederland het online betalingsverkeer van banken regelmatig onbereikbaar geweest en zijn belangrijke of populaire internetdiensten zoals de Belastingdienst en X (voorheen: Twitter) door de aanvallen korte tijd offline gegaan.

31 HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 (*Toxbot*-arrest).

32 Richtlijn 2013/40/EU van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ.

33 Art. 138b lid 2 Sr.

34 Zie bijvoorbeeld 'DDoS-aanvallen Comenius Leeuwarden voorbij: twee leerlingen verveelden zich', *Omrop Fryslan.nl*, 26 maart 2021.

35 Zie bijvoorbeeld O. Yoachimik & J. Pacheco, 'DDoS threat report for 2023 Q3', *The Cloudfare Blog*, 26 oktober 2023, T. Litchfield, 'Diablo 4 and other Battle.net games are back online after brutal weekend DDoS attack', *PCgamer.com*, 25 juni 2023 en 'Cybercriminals are using bots to deploy DDoS attacks on gambling sites', *Help Net Security*, 19 augustus 2022.

36 'Toename aan intensiviteit en aantal DDoS aanvallen', *NCSC.nl*, 4 september 2020.

Bij deze vorm van cybercriminaliteit zien we duidelijk het in hoofdstuk 2 besproken principe van force multiplier terug; een enkele dader kan met slechts enkele muisklikken veel impact genereren. Ddos-aanvallen gaan ook vaak gepaard met andere vormen van cybercriminaliteit zoals botnets (die helpen om de aanval mee uit te voeren) (Overvest & Straathof, 2015) of phishing waarbij de aanvaller bijvoorbeeld gebruikmaakt van de omstandigheden (in dit geval een ddos-aanval) om een phishing campagne uit te voeren (Junger et al., 2021).

Casus: Webstresser.org

Figuur 3.3 Screenshot van de website webstresser.org, die na de internationale politieactie ontoegankelijk is gemaakt

In april 2018 werd de populaire 'ddos-dienst' (in het Engels *booter* of *stresser*) Webstresser.org bij een internationale politieoperatie offline gehaald.[37] Met de operatie kreeg de politie gegevens van ruim 151.000 gebruikers van deze website in handen.

37 'Nederlandse politie haalt ddos-dienst webstresser.org offline', *Tweakers.net*, 25 april 2018.

Volgens de politie maakten ook veel jongeren gebruik van de website. Het uitvoeren van een korte ddos-aanval was al mogelijk voor slechts 15 euro.[38] Door deze laagdrempelige manier om ddos-aanvallen uit te voeren zijn bijvoorbeeld ook computerexamens op scholen verstoord. In deze casus was een botnet onderdeel van het cybercriminele verdienmodel en dus het middel om de ddos-aanvallen uit te voeren (Santanna et al., 2015).

De operatie heeft niet geleid tot veroordelingen in Nederland. Dit had er mogelijk mee te maken dat een belangrijke doelstelling van de politie was om zo snel mogelijk de technologie uit te schakelen die de ddos-aanvallen mogelijk maakte. Dit deed men door de servers achter de website inactief en onbereikbaar te maken.[39] Daarna werd pas gekeken naar de beheerders van de ddos-dienst en hun klanten (Van der Wagen & Bernaards, 2018). De politie meldt dat politieagenten wel gesprekken met de gebruikers hebben gevoerd over hun strafbare gedragingen (een *knock-and-talk* actie). Het doel hiervan is ook dat betrokkenen zich realiseren dat zij niet zo anoniem zijn als ze mogelijk dachten.[40] Bij cybercriminaliteit en zeker ook bij ddos-aanvallen zien we vaker dat de politie inzet op dergelijke verstoring of preventie, in plaats van opsporing en vervolging (zie ook hoofdstuk 10). Meer recent is er bijvoorbeeld een gerichte advertentiecampagne geweest, waarmee de politie jongeren die tijdens het gamen een ddos-aanval wilden uitvoeren (en hiernaar zochten via Google) waarschuwde voor de negatieve gevolgen hiervan (Moneva et al., 2022; 2023; Moneva & Leukfeldt, 2023). De effectiviteit hiervan is echter wel lastig aan te tonen (zie ook hoofdstuk 10).

3.6.1 Strafbaarstelling

Met de implementatie van de Wet computercriminaliteit II in 2006 zijn ddos-aanvallen strafbaar gesteld in artikel 138b Sr, namelijk als volgt:

38 N. Klaassen, 'Pssst, wil je een cyberaanval uitvoeren? Dat kost 15 euro', *AD.nl*, 31 januari 2019.

39 Uiteindelijk werd wel een harde klap uitgedeeld, maar het effect was tijdelijk, want de markt voor *booters* veranderde er niet structureel door (zie verder Collier et al., 2019).

40 'Politie en justitie gaan wereldwijd achter de gebruikers van "DDoS-for-hire websites" aan', *Politie.nl*, 28 januari 2019.

het opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden.

Op het delict staat een maximale gevangenisstraf van twee jaar of een geldboete van de vierde categorie.[41] Met de zelfstandige strafbaarstelling van ddos-aanvallen wordt duidelijk gemaakt dat de integriteit en beschikbaarheid van gegevens op computers en computersystemen van groot maatschappelijk belang zijn (Koops & Oerlemans, 2019a).

Als de aanval 'aanzienlijke schade' met zich meebrengt of is gericht op een 'vitale infrastructuur', is tevens een strafverzwaring van toepassing (art. 138b lid 3 Sr). Hiervan was bijvoorbeeld sprake bij de aanval met de 'NotPetya'-malware, die tot gevolg had dat de Tweede Maasvlakte een week lang niet kon worden gebruikt.[42] Van 'cyberterrorisme' is tot dusver geen sprake geweest in Nederland, maar ook voor die omstandigheid biedt artikel 138b Sr een strafverzwaring (zie lid 4 en 5). Een ddos-aanval op websites zoals die van de Belastingdienst, Overheid.nl of banken is ten slotte ook strafbaar als een aanval op een 'dienst van algemene nutte', met een maximale gevangenisstraf van zes jaar of een geldboete van de vijfde categorie (art. 161sexies Sr).[43]

3.7 De rol van social engineering bij cybercriminaliteit

In dit hoofdstuk zijn bij verschillende verschijningsvormen van cybercriminaliteit diverse crime scripts aan bod gekomen om de stappen die daders moeten maken beter te begrijpen. Op het moment van schrijven wordt er, zeker in Nederland, veel onderzoek gedaan naar de crime scripts (of onderdelen daarvan) van uiteenlopende vormen van cybercriminaliteit (zowel in enge zin zoals besproken in dit hoofdstuk als in ruime zin (gedigitaliseerde criminaliteit) zoals besproken in het volgende hoofdstuk). Daarbij gaat het bijvoorbeeld om onderzoek naar hacking, phishing, ransomware en het delen van seksueel materiaal van minderjarigen op forums (Loggen & Leukfeldt, 2022; Matthijsse et al., 2023; Moneva et al., 2024; Van der Bruggen & Blok-

41 Zie bijvoorbeeld Rb. Den Haag 7 maart 2019, ECLI:NL:RBDHA:2019:2116, *Computerrecht* 2019/93, m.nt. J.J. Oerlemans (*Mirai*-zaak).

42 T. Kreling & H. Modderkolk, 'Gijzelingssoftware legt al drie dagen een Rotterdamse haven plat – De schade in beeld', *Volkskrant.nl*, 30 juni 2017.

43 Zie bijvoorbeeld Rb. Den Haag 14 maart 2005, ECLI:NL:RBSGR:2005:AT0249 en Rb. Zeeland-West-Brabant 2 september 2014, ECLI:NL:RBZWB:2014:6659. Een ddos-aanval is ook strafbaar op grond van artikel 350c Sr.

land, 2021). Crime scripts maken niet alleen de modus operandi inzichtelijk, maar bieden ook waardevolle inzichten voor passende preventieve interventies, doorgaans gericht op het opwerpen van barrières in het criminele proces (zie ook hoofdstuk 10). Wanneer naar de verschillende crime scripts wordt gekeken, valt op dat er bij veel verschillende vormen van cybercriminaliteit in enge zin (en ook wel bij gedigitaliseerde vormen die in het volgende hoofdstuk worden besproken) niet alleen misbruik wordt gemaakt van technische kwetsbaarheden, maar ook van de mens als zwakke schakel. In dit kader wordt vaak gesproken van de term social engineering. In deze paragraaf gaan we hier nader op in.

Bij social engineering probeert een dader een slachtoffer zo te manipuleren dat hij of zij de social engineer toegang geeft tot een systeem of tot bepaalde informatie (Mitnick & Simon, 2002; Steinmetz et al., 2021). Op basis van interviews met professionele (dus niet criminele) social engineers beschrijven Steinmetz et al. (2021) het proces van social engineering in verschillende fases. Deze beschrijving gaat vooral over intensieve social engineering, waarbij daders vaak niet alleen digitaal maar ook fysiek contact leggen met hun slachtoffers om zo bijvoorbeeld (de systemen van) een goed beveiligd bedrijf binnen te komen.

In de *planning* fase doen daders onderzoek naar hun eigen situatie en dat van het potentiële slachtoffer. Met deze informatie kunnen ze de manipulatie zo goed mogelijk plannen en opzetten. Ze proberen hierbij zo specifiek mogelijk aan te sluiten bij de situatie van het slachtoffer en hierbij ook rekening te houden met hun eigen kenmerken. Zo proberen ze uit te zoeken op welk moment een slachtoffer het best bereikbaar is of op welk moment in de week een slachtoffer het zo druk heeft dat hij of zij wellicht minder goed oplet (en makkelijker een e-mailbijlage met malware zal openen). Ook kan het zijn dat ze binnen een bedrijf dat ze willen binnendringen bijvoorbeeld op zoek gaan naar iemand met wie ze verwachten makkelijk een connectie te kunnen maken, bijvoorbeeld omdat die persoon dezelfde achtergrond of hetzelfde geslacht heeft als zijzelf.

In de *proximity* fase proberen ze vervolgens onderdeel te worden van de sociale omgeving van het slachtoffer. Ze leggen contact en proberen, met behulp van de informatie uit de eerste fase, een band op te bouwen. Hiermee proberen ze te bereiken dat het slachtoffer hen gaat vertrouwen en dat er een gevoel van saamhorigheid ontstaat.

Vervolgens proberen ze in de *activation* fase het slachtoffer daadwerkelijk zo ver te krijgen dat hij of zij hun de toegang tot ICT-systemen of informatie geeft die ze nodig hebben. Hierbij gebruiken ze verschillende overtuigingstechnieken. Ze kunnen iemand bijvoorbeeld eerst zelf iets geven of ergens mee helpen, waardoor die persoon daarna de neiging heeft om iets terug te doen.

Als laatste is het in de *concealment* fase nog belangrijk om te voorkomen dat iemand gaat twijfelen. Ten eerste kan een dader dit bereiken door zijn of haar rol heel goed te spelen en zo min mogelijk op te vallen. Het is dan ook belangrijk dat er in de planning fase een goede rol is uitgedacht, die niet te complex is en die makkelijk is aan te passen als dat nodig blijkt. Wanneer er twijfel ontstaat, moet de social engineer gelijk een antwoord op kritische vragen klaar hebben. Een tactiek die hierbij ook gebruikt wordt, is om snel toe te slaan en een slachtoffer te overladen met informatie waardoor hij of zij geen tijd heeft om er goed over na te denken.

Bovenstaande beschrijving van social engineering is behoorlijk intensief en hoewel dit proces ook heel snel zou kunnen verlopen is het aantal mensen dat met een dergelijke social engineering-aanval te maken krijgt waarschijnlijk klein. Iets waar wel vrijwel iedereen mee te maken krijgt is social engineering via phishing. De bekendste vorm van phishing is via e-mail, maar het vindt ook plaats via telefoon of WhatsApp (Van 't Hoff-de Goede & Leukfeldt, 2021), chatfuncties op platforms als Marktplaats (Rooyakkers & Weulen Kranenbarg, 2020), enzovoort. In de literatuur worden de tactieken die daders in deze phishingberichten gebruiken uitgelegd aan de hand van zes overtuigingsprincipes zoals beschreven door Cialdini (2009). Vaak gebruiken daders een combinatie van deze overtuigingsprincipes om mensen zover te krijgen dat ze malware uit e-mailbijlagen downloaden, gegevens afstaan, inloggen op phishingwebsites, producten kopen in *fake* webshops, geld overmaken, personen binnenlaten in hun beveiligde werkomgeving, enzovoort.

Het eerste principe, wederkerigheid, is hierboven ook al aan bod gekomen. Wanneer je mensen iets geeft of hen ergens mee helpt, zijn ze geneigd om iets terug te doen. Wanneer je bijvoorbeeld een buitendeur (die niet op slot zit) voor iemand openhoudt, heeft die persoon de neiging om de volgende deur voor jou open te houden (ook als die alleen met een toegangspas te openen is).

Het tweede principe is schaarste. Mensen hebben de neiging om sneller over te gaan tot actie als iets dat zij graag willen hebben schaars is. Daarom zetten daders hun slachtoffers vaak onder tijdsdruk. Aanbiedingen op fake webshops zijn vaak maar kort geldig of er is nog maar één artikel op voorraad.

Volgens het derde principe, autoriteit, hebben mensen de neiging zich te conformeren aan mensen of organisaties die autoriteit hebben. Daders doen zich dan ook vaak voor als een bekende webshop of bank en imiteren in hun e-mails zo veel mogelijk de manier waarop deze organisaties met hun klanten communiceren. Ze gebruiken zelfs gestolen gegevens (bijvoorbeeld gestolen door middel van hacking of malware) om bijvoorbeeld de laatste drie cijfers van een bankrekeningnummer te noemen, omdat veel organisaties dergelijke informatie gebruiken om te controleren of de persoon met wie ze contact hebben ook echt de eigenaar is van die bankrekening.

Ten vierde gebruiken daders het principe van consistentie. Als mensen eenmaal één keer ergens in mee zijn gegaan, zullen ze dat een volgende keer ook sneller doen. Zo zien we bijvoorbeeld bij datingfraude dat een dader eerst een klein bedrag vraagt. Wanneer het slachtoffer dit heeft overgemaakt wordt vervolgens steeds iets meer geld gevraagd. Vaak gaat een slachtoffer daar dan ook in mee.

Ten vijfde is het volgens het principe van sympathie belangrijk om vriendelijk en behulpzaam te zijn. Wanneer je aardig bent tegen je potentiële slachtoffer zal hij of zij sneller geneigd zijn om je te vertrouwen.

Als laatste het principe van conformiteit. Mensen zijn kuddedieren en doen graag dat wat andere mensen ook doen. Een fake webshop kan bijvoorbeeld suggereren dat een product heel populair is en al door heel veel andere klanten is gekocht, met goede reviews.

3.8 Toekomstige ontwikkelingen

De digitalisering van ons leven zet door en zal ook invloed blijven hebben op criminaliteit. Naar alle waarschijnlijkheid zullen bepaalde vormen van cybercriminaliteit in enge zin in de toekomst nog geavanceerder worden. Ook is het denkbaar dat nieuwe actoren op het toneel verschijnen en er nieuwe verschijningsvormen ontstaan. In deze paragraaf zetten wij de belangrijkste ontwikkelingen en de invloed daarvan op cybercriminaliteit in enge zin op

een rij. Sommige van deze ontwikkelingen zijn deels ook aan bod gekomen in hoofdstuk 2 en om die reden bespreken we ze hier beknopt.

3.8.1 Meer invloed van statelijke actoren

Zoals we zagen in hoofdstuk 2 maken statelijke actoren steeds vaker gebruik van de (cybercriminele) middelen die het cyberdomein biedt, bijvoorbeeld in het kader van oorlogsvoering. Het Nederlandse Nationale Cyber Security Centrum waarschuwt sinds 2018 zelfs dat er van statelijke actoren een grotere dreiging op het gebied van cybersecurity uitgaat dan van criminelen (NCSC, 2018).

Buitenlandse statelijke actoren voeren in Nederland voornamelijk economische spionage uit op Nederlandse 'topsectoren', zoals de hightechsector (bijvoorbeeld een chipmaker) en de agrarische sector (bijvoorbeeld bedrijven die zich bezighouden met de veredeling van zaden). In 2007 rapporteerde de Algemene Inlichtingen- en Veiligheidsdienst voor het eerst in een jaarverslag over 'digitale inbreuken op vitale Nederlandse ICT-netwerken die vanuit China werden geregisseerd'. De dienst waarschuwde vanaf 2013 tot en met 2024 steevast voor het gevaar van cyberspionage voor de nationale veiligheid van Nederland. Ook de Militaire Inlichtingen- en Veiligheidsdienst waarschuwt voor digitale spionage uit landen als China, Iran en Rusland op Nederland. Natuurlijk is het inbreken in computers door ambtenaren van een buitenlandse inlichtingen- of veiligheidsdienst ook strafbaar. De kans is echter klein dat voor deze delicten succesvol in Nederland kan worden vervolgd.

In 2024 werd het wetsvoorstel 'uitbreiding strafbaarstelling spionageactiviteiten' door de Tweede Kamer aangenomen.[44] Het voorstel voorziet in de invoering van een zelfstandige strafbaarstelling voor spionageactiviteiten. Daarbij valt te denken aan het onrechtmatig verzamelen van (gevoelige) informatie of objecten, sabotage, het interveniëren in (besluitvormings)processen of beïnvloeding van personen. Ook is het voorstel om enkele computerdelicten aan te passen, als die zijn gepleegd 'ten behoeve van een buitenlandse mogendheid'.

Ten slotte hebben Nederlandse inlichtingen- en veiligheidsdiensten door een wetswijziging in 2024 meer mogelijkheden om onderzoek te doen naar 'lan-

44 *Kamerstukken II* 2022/23, 36280, nr. 2 en *Kamerstukken I* 2023/24, 36280, nr. D.

den met een offensief cyberprogramma'.[45] Een offensief cyberprogramma is er onder meer op gericht om langs de digitale weg op heimelijke wijze de beschikking te krijgen over vertrouwelijke informatie, economische en technologische kennis of andere informatie van burgers of organisaties waarmee zij hun voordeel doen. Deze wet laat zien dat inlichtingen- en veiligheidsdiensten zich ook steeds meer in het domein begeven en zich met vormen van cybercriminaliteit bezighouden, die door staten worden uitgevoerd en de nationale veiligheid bedreigen.

3.8.2 Het Internet der Dingen

Een andere belangrijke hedendaagse ontwikkeling die ongetwijfeld ook in de nabije toekomst een steeds grotere rol gaat spelen, is het zogenoemde 'Internet der Dingen' (*Internet of Things*, kortweg IoT), waarbij apparaten door middel van sensoren gegevens verzamelen over hun omgeving, via een netwerk deze gegevens uitwisselen en (semi)autonome beslissingen nemen die van invloed zijn op de omgeving (Van Berkel et al., 2017). Daarbij kan bijvoorbeeld worden gedacht aan apparaten zoals internetcamera's, slimme auto's, slimme verkeerslichten (met sensoren zoals personentellers), slimme lampen of slimme planten (die het aangeven als ze water nodig hebben).

In de afgelopen jaren is al zichtbaar geworden dat veel IoT-objecten onvoldoende beveiligd zijn of dat mensen de standaardinstellingen en wachtwoorden niet wijzigen. Deze apparaten kunnen worden gehackt en vervolgens onderdeel worden van een botnet waarmee ddos-aanvallen worden uitgevoerd. In 2016 is bijvoorbeeld met honderdduizenden apparaten die onderdeel vormden van het Mirai-botnet een grote hosting provider aangevallen, waardoor populaire diensten voor miljoenen gebruikers zoals X (voorheen: Twitter), Netflix en CNN enige tijd ontoegankelijk waren.[46] Ook in Nederland is in 2019 een jongeman veroordeeld voor het gebruik van het Mirai-botnet en het uitvoeren van ddos-aanvallen.[47]

Serieuzere consequenties kunnen ontstaan wanneer in of aan het lichaam verbonden apparaten worden gehackt, zoals een insulinepomp of pacemaker.

45 Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen.

46 N. Woolf, 'DDoS attack that disrupted internet was largest of its kind in history, experts say', *Theguardian.com*, 16 oktober 2016.

47 Zie Rb. Den Haag 7 maart 2019, ECLI:NL:RBDHA:2019:2116, *Computerrecht* 2019/93, m.nt. J.J. Oerlemans.

In 2013 werd bijvoorbeeld bekend dat toenmalig vicepresident Dick Cheney uit de Verenigde Staten zijn pacemaker niet meer via een netwerk in verbinding liet staan, uit angst dat deze zou worden gehackt.[48] Langzamerhand ontstaat een 'Internet der Mensen' (*Internet of People*). In de toekomst zullen digitale technologieën steeds verder integreren met het menselijk lichaam. Deze apparaten op of in het menselijk lichaam zijn te kwalificeren als een geautomatiseerd werk. De delictsomschrijvingen voor gedragingen gericht op deze apparaten zijn dan ook goed toepasbaar op deze nieuwe verschijningsvormen van cybercriminaliteit. Wel hebben verschillende auteurs gepleit voor de invoering van een hogere maximale gevangenisstraf als in apparaten in het lichaam wordt binnengedrongen (Gasson & Koops, 2023; Oerlemans & Schermer, 2022). Dat zou recht doen aan de aantasting van lichamelijke integriteit van slachtoffers en de ernstige schade die daarmee gepaard kan gaan.

De laatste stap is dat al deze apparaten en mensen naadloos op elkaar aansluiten en met elkaar samenwerken waardoor er een 'Internet van Alles' (*Internet of Everything*) ontstaat. Het uitvoeren van ddos-aanvallen op netwerken of het infecteren van apparaten in netwerken kan dan zeer grote gevolgen hebben voor de economie, maar mogelijk ook voor de gezondheid van mensen, en kan de continuïteit van vitale diensten in gevaar brengen.

3.9 Tot besluit

In dit hoofdstuk zijn de belangrijkste verschijningsvormen van cybercriminaliteit in enge zin uitgelegd. U begrijpt op welke wijze deze misdrijven doorgaans worden gepleegd en op welke manier zij strafbaar zijn gesteld met eventuele strafverzwarende omstandigheden. Zoals we hebben gezien en ook zullen gaan zien in hoofdstuk 4, worden in de praktijk vaak verschillende delicten tegelijk (of in een keten) gepleegd en zijn meerdere wetsartikelen van toepassing die voor een deel ook in hoofdstuk 4 worden besproken. Het is bijvoorbeeld mogelijk oplichting te plegen nadat de financiële persoonsgegevens zijn overgenomen door computervredebreuk en het installeren van malware. Mogelijk worden zelfs de computers van meerdere slachtoffers aangestuurd via een botnet en werken de betrokkenen samen in een crimineel samenwerkingsverband.

48 L. Vaas, 'Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking', *Naked Security*, 22 oktober 2013.

3.10 Discussievragen

1. Zijn er offline equivalenten te bedenken voor de vormen van cybercriminaliteit die we in dit hoofdstuk behandeld hebben?
2. In hoeverre spelen de aspecten van (1) het wegvallen van barrières van tijd en ruimte, (2) automatisering en amplificatie, (3) innovatie en transformatie, (4) sociale en commerciële interconnectiviteit, (5) anonimiteit en plasticiteit van de identiteit, en (6) virtualisering en hybridisering (zie hoofdstuk 2) een rol bij hacken, malware, botnets en ddos-aanvallen?
3. Is het onderscheid tussen strafbaar hacken en ethisch hacken voldoende scherp?
4. Wat verklaart de plaats en strafbaarstellingen van cybercriminaliteit in het Wetboek van Strafrecht?
5. Welke voor- en nadelen kleven er voor hackers aan het melden van ICT-kwetsbaarheden door middel van Coordinated Vulnerability Disclosure?
6. Zijn de strafbaarstellingen voor cybercriminaliteit in enge zin voldoende ten aanzien van cyberaanvallen die gericht zijn op een vitale infrastructuur?
7. Zoek in uw mailbox een recente phishing e-mail; welke social engineering-technieken herkent u in deze e-mail?
8. In hoeverre zijn criminologen in staat om goed onderzoek te doen naar vormen van cybercriminaliteit in enge zin?
9. Hoe kunnen vormen van cybercriminaliteit in enge zin effectief aangepakt worden? En kan de politie dit wel alleen?
10. Wat vindt u na het lezen van dit hoofdstuk van de stelling: 'De wet loopt altijd achter'?

3.11 Kernbegrippen

- Banking malware
- Botnet
- Crime script
- Computervredebreuk
- Cyberspionage
- Ddos-aanval
- Ethisch hacken
- Exploit kit
- Hacking
- Info-stealers

- Identiteitsfraude
- Internet of Things
- Malware
- Overtuigingstechnieken
- Phishing
- Ransomware
- Remote access tool
- Social engineering