Cyberdaders: uniek profiel, unieke aanpak?

Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin

Eindrapportage – December 2019

Dr. W. van der Wagen[1]

Dr. E.G van 't Zand-Kurtovic[2]

S.R. Matthijsse MSc[1]

Dr. T.F.C. Fischer[1]

Met medewerking van: Sophie Keizer en Nicole Alberts

[1] Erasmus Universiteit Rotterdam, Sectie Criminologie

[2] Universiteit Leiden, Instituut voor Strafrecht en Criminologie

COLOFON

Opdrachtgever

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Afdeling Externe Betrekkingen (EWB) Ministerie van Justitie en Veiligheid

Koningskade 4

2596 AA Den Haag

Onderzoekers

Dit onderzoek is uitgevoerd door de sectie Criminologie van de Erasmus Universiteit Rotterdam in samenwerking met de Universiteit Leiden. De betrokken onderzoekers waren: Wytske van der Wagen, Elina van ’t Zand, Sifra Matthijsse en Tamar Fischer, met medewerking van Sophie Keizer en Nicole Alberts.

Illustratie voorblad: https://tumblr.com

Inhoudsopgave

Samenvatting

Achtergrond en onderzoeksvragen

Er zijn verschillende indicaties dat hacken[3], het uitvoeren van DDoS-aanvallen[4], het verspreiden van ransomware[5] en andere vormen van cybercriminaliteit in enge zin[6] in omvang toenemen onder zowel jeugdigen als volwassenen. De wetenschappelijke kennis over deze dadergroep is tot op heden beperkt, anekdotisch, verouderd en versnipperd. In dit onderzoek is getracht op meer systematische wijze kennis over de kenmerken en profielen van jeugdige en volwassen daders van cybercriminaliteit in enge zin te genereren alsook inzichten te bieden in de vraag wat hierbij passende en effectieve interventies zijn. In dit onderzoek staat de volgende probleemstelling centraal:

"In hoeverre bestaan er verschillen qua profiel(en) van cyberdaders en daders van 'traditionele' criminaliteit, en in hoeverre en op welke wijze dienen (eventuele) verschillen gevolgen te hebben voor de aard van interventies voor cyberdaders?"

Methoden van onderzoek

In dit kwalitatieve onderzoek is gebruik gemaakt van een combinatie van onderzoeksmethoden. Ten eerste zijn twee systematische zoekopdrachten in de literatuur verricht: een gericht op kenmerken van cyberdaders en een gericht op interventies voor cyberdaders. De eerste zoekopdracht leverde 99 bronnen op over kenmerken van daders van cybercriminaliteit in enge zin, al dan niet in vergelijking met traditionele daders. De tweede zoekopdracht leverde 25 bronnen op over interventies gericht op cyberdaders in enge zin. Ten tweede zijn expertinterviews afgenomen (29 individuele interviews, 2 focusgroepen, 1 expertmeeting en 1 roundtable). In totaal zijn 52 experts gesproken, vanuit vrijwel alle samenwerkingspartners uit de veiligheidsketen (politie, Openbaar Ministerie, rechterlijke macht, advocatuur, (jeugd)reclassering, Raad voor de Kinderbescherming, Halt en zorgverleners) evenals experts uit het bedrijfsleven, onderzoekers en freelancers die zich met het thema cybercriminaliteit bezighouden. Ten derde zijn 14 volwassen daders geïnterviewd. Hiervan was het grootste deel veroordeeld voor een of meer cyberdelicten in enge zin (o.a. hacken, DDoS-aanvallen, virtuele diefstal[7]) en een kleiner deel was wel betrokken bij cyberdelicten, maar waren daarvoor niet gepakt. In de meeste gevallen was hacken het primaire delict. De justitiële interventies die de geïnterviewde daders opgelegd hebben gekregen betreffen voornamelijk taakstraffen, maar ook hebben sommige daders een (voorwaardelijke) gevangenisstraf, contactverbod, geldboete, schadevergoeding of elektronische detentie opgelegd gekregen. Vier daders hebben geen justitiële interventie opgelegd gekregen en twee daders waren ten tijde van het interview nog in afwachting van hun strafzaak.

[3] Dit verwijst naar het wederrechtelijk binnendringen in een computersysteem.
[4] Dit verwijst naar verstoren of platleggen van een systeem door middel van overbelasting.
[5] Dit verwijst naar kwaadaardige software (*malware*) die gebruikt kan worden om een systeem 'te gijzelen' c.q. te blokkeren opdat het slachtoffer losgeld moet betalen.
[6] Dit verwijst naar vormen van cybercriminaliteit waarbij ICT zowel het doelwit als het middel is.
[7] Dit verwijst naar het stelen van goederen in een virtueel spel.

Beperkingen van het onderzoek

Het onderzoek kent een aantal beperkingen. Ten eerste kent de gevonden literatuur haar beperkingen. Zo is er relatief veel literatuur gevonden over hackers (zij het wel veel verouderde literatuur en meestal kleine steekproeven), maar weinig over daders die betrokken zijn bij andere vormen van cybercriminaliteit in enge zin zoals DDoS aanvallen en ransomware. Tevens zijn er weinig (effect)studies gevonden waarin de toepassing van traditionele of cyber-gerelateerde interventies op cyberdaders is onderzocht, waardoor er dus weinig systematische kennis over interventies voor handen is. Ten tweede zijn bij de expertinterviews diverse respondenten betrokken die zelf nog maar met enkele cyberdaders ervaring hadden. De antwoorden van deze experts zijn dus bepaald door een klein aantal zaken en verder wellicht medebepaald door verhalen van collega's, beelden uit de media of het maatschappelijke debat. Ten derde vormen de geïnterviewde daders een specifieke groep (volwassen, meerderheid veroordeeld en met hacken als primair delict), waardoor minder focus ligt op andere dadertypen in dit onderzoek. Ten slotte zijn de uitkomsten afhankelijk van zelfrapportage door de daders. Het is mogelijk dat daders niet al hun delictgedrag rapporteerden, recente delicten verzwegen of juist hun delictcarrière 'succesvoller' afschilderden dan ze werkelijk waren.

Bevindingen

DEEL 1 Daderkenmerken

In het eerste deel van het rapport is stilgestaan bij de vraag wat de specifieke kenmerken zijn van cyberdaders en in hoeverre op basis daarvan verschillende daderprofielen te construeren zijn. De kenmerken zijn bovendien vergeleken met kenmerken van traditionele daders waardoor verschillen met deze daders konden worden beschreven. We onderscheiden (offline en online) criminogene (risicofactoren die een bijdrage leveren aan het delictgedrag) en protectieve (beschermende) factoren (factoren die delictgedrag kunnen voorkomen of afremmen). Bij de analyse van de dadergroep is gebruik gemaakt van verschillende algemene criminologische benaderingen zoals de differentiële-associatietheorie[8], neutralisatietechnieken[9] en de rationele keuzetheorie.[10] Ook zijn concepten toegepast die specifiek ontwikkeld zijn om online en technische aspecten van daderschap te duiden zoals het *online disinhibition effect*[11], *digital drift*[12] en *mastery*.[13]

Profielen

Gedurende het onderzoek bleek dat een eenvoudige clustering of profilering op grond van het wel of niet aanwezig zijn van bepaalde kenmerken geen realistisch beeld oplevert. Bij de daders zijn verschillende kenmerken en factoren (persoonlijk en contextueel) en specifieke motivaties (zoals uitdaging zoeken of status verwerven) aanwezig, die in verschillende combinaties en mate voorkomen. Dit leidt vervolgens tot (een bepaalde ontwikkeling in) het delictgedrag (criminele carrière). Om deze reden is de profilering van cyberdaders benaderd door het beschrijven van de

[8] Deze theorie veronderstelt dat delinquent gedrag wordt aangeleerd in hechte groepen. Daarbij gaat om zowel technieken om criminaliteit te plegen als normen, waarden en attitudes.
[9] Dit zijn technieken die daders kunnen gebruik om delinquent gedag goed te praten.
[10] Deze benadering gaat er vanuit dat delinquent gedrag voortvloeit uit en begrepen kan worden als een rationele kosten- en batenafweging. Het kan daarbij gaan om zowel materiële (geld) als niet- materiële kosten en baten (roem, plezier).
[11] Dit verwijst naar het wegvallen van remmingen door online anonimiteit.
[12] Dit verwijst naar de wijze waarop het internet zowel technische als sociale *affordances* biedt die bepaalde vormen van delinquentie kunnen intensiveren of daar nieuwe mogelijkheden voor bieden.
[13] Dit verwijst naar de behoefte of drang om de techniek meester te zijn en gaat gepaard met een gevoel van macht en controle.

impact van verschillende kenmerken en factoren op het delictgedrag, zowel individueel als in hun onderlinge samenhang.

Achtergrondkenmerken

Uit de literatuur is gebleken dat cybercriminaliteit in enge zin relatief vaker wordt gepleegd door jonge autochtone mannen met een redelijk tot goede sociaaleconomische achtergrond. Bij de subgroep financieel georiënteerde daders van cybercriminaliteit in enge zin ligt de leeftijd waarop gestart wordt met het plegen van cybercriminaliteit doorgaans hoger, lijkt vaker sprake te zijn van allochtone daders en zijn er indicaties voor een lagere sociaaleconomische status.

Hoewel het opleidingsniveau bij cyberdaders varieert, lijkt sprake te zijn van een relatief hoger intelligentie- en opleidingsniveau in vergelijking met traditionele daders. Soms maken daders hun opleiding niet af, wat niet automatisch betekent dat zij in laaggeschoold werk terechtkomen. Het werk en de opleiding die cyberdaders doen of hebben gedaan varieert, maar opleidingen en banen in de IT-sector zijn oververtegenwoordigd. In hun vrije tijd houden cyberdaders zich veel bezig met techniek, ICT, gamen en sociale media. Hiernaast hebben ze echter ook een breed scala aan andere hobby's. De thuissituatie (o.a. de rol van gezinsproblematiek) varieert sterk. Er blijkt vaak een gebrek aan ouderlijk toezicht op het online gedrag van cyberdaders te zijn, zowel in gezinnen met als zonder gezinsproblematiek. Dit beperkte toezicht wordt mede veroorzaakt door gebrekkige kennis van ouders[14] van het internet en de online wereld.

Tot slot kunnen de cyberdaders gekenmerkt worden als intelligent met vaker dan bij traditionele daders de aanwezigheid van kenmerken uit een autismespectrumstoornis (ASS) en een sterk probleemoplossend vermogen. Tevens suggereren de bevindingen dat er een tweedeling waarneembaar is tussen de cyberdaders die een lagere zelfcontrole ervaren en impulsief zijn en daders die juist lange termijn doelen stellen en perfectionistisch zijn. Sommige daders kunnen volgens de literatuur en de experts gekenmerkt worden als introvert of sociaal onhandig, maar een ander deel (waar veel van de door ons geïnterviewde cyberdaders zichzelf onder scharen) lijkt voldoende sociaal vaardig. Waar de meeste cyberdaders online een sociaal netwerk hebben opgebouwd lijkt het offline netwerk relatief kleiner te zijn en in mindere mate van invloed te zijn op het delictgedrag.

Drijfveren en beleving

Uit het onderzoek komt naar voren dat diverse drijfveren een rol spelen bij cyberdaders. Ook is gebleken dat daders meerdere motivaties hebben en dat motivaties over de tijd heen kunnen veranderen.

De drijfveren nieuwsgierigheid, leergierigheid en (mentale) uitdaging spelen voornamelijk een rol bij jeugdige cyberdaders. Deze motieven zijn niet per definitie kwaadaardig. Deze jongeren willen de *ins and outs* van systemen leren en ontdekken hoe ver ze kunnen gaan met de techniek. Anders dan bij de meeste traditionele vormen van criminaliteit is het leren een doel of drijfveer op zichzelf en niet slechts een middel of instrument om de delicten te kunnen plegen.

Andere motieven die naar voren komen zijn de kick, spanning, plezier, verveling, verzameldrang (naar informatie) en macht. Deze drijfveren kunnen ook bij traditionele criminaliteit spelen, maar bij cybercriminaliteit is er een meer nadrukkelijke samenhang met online vaardigheden en techniek.

Erkenning, status, peer respect en bewijsdrang komen als belangrijke motieven naar voren bij

[14] Mogelijk is de IT-kennis van ouders wel afhankelijk van hun leeftijd. Dit is in het huidige onderzoek niet specifiek onderzocht.

jeugdige daders. Deze jongeren willen bewijzen wat ze kunnen om respect of roem te verwerven. Het verschil met traditionele misdaad is dat de focus sterker ligt op de technische vaardigheden, werkwijze en prestatie (je 'kunnen').

Financiële motieven lijken in mindere mate een rol te spelen bij jeugdige (individuele) daders. In sommige gevallen kan geld wel op een later moment in de criminele carrière een rol gaan spelen. Dit is ook afhankelijk van de activiteiten die zij ontplooien. Het financiële motief lijkt vooral voor te komen bij (volwassen) daders die actief zijn in de context van fraude en georganiseerde cybercriminaliteit. In een deel van de gevallen gaat het dan om daders die de overstap hebben gemaakt van traditionele (offline) fraude naar cybercriminaliteit.

Aanvullend kan cybercriminaliteit (voornamelijk hacken of het uitvoeren van DDoS-aanvallen) gepleegd worden uit boosheid of om wraak te nemen op vrienden, familie, ex-werkgevers of ex-geliefden waar offline een conflict mee is ontstaan. Hierbij lijkt het voornamelijk te gaan om volwassen traditionele daders die een nieuw middel hebben ontdekt om hun frustratie te uiten. Ook zijn er daders die uit ideologische motieven handelen. Laatstgenoemde twee clusters van motieven zijn relatief onderbelicht gebleven in dit onderzoek.

Percepties strafbaarheid, pakkans en schade door gepleegde delicten

Als het gaat om de perceptie ten aanzien van strafbaarheid lijkt sprake te zijn van een glijdende schaal. Aan de ene kant van de schaal bevinden zich (veelal jonge) daders die zich niet of nauwelijks bewust zijn van de strafbaarheid en aan de andere kant daders die dat wel zijn en bijvoorbeeld via fora goed op de hoogte zijn van de straffen die ze riskeren.

De gebrekkige perceptie van strafbaarheid, die aanwezig is bij een deel van de daders, komt onder andere voort uit de afwezigheid van toezicht in de online wereld, de onzichtbaarheid van de aangerichte schade en - voor een deel van de daders - de aanwezigheid van drijfveren die in aanleg niet kwaadaardig zijn (nieuwsgierigheid, mentale uitdaging, erkenning van talenten). Binnen deze laatste categorie vallen ook de delicten waarbij beveiligingsproblemen worden aangetoond, maar onduidelijkheid bestaat over de juridische grenzen en de kaders van *responsible disclosure*.[15] Daarmee is de beperkte perceptie van strafbaarheid een belangrijkere criminogene factor bij cyberdaders dan bij traditionele daders. Met het voortgaan van de carrière neemt het besef van de strafbaarheid bij daders toe, maar wordt dit volgens experts deels weer teniet gedaan door de zeer beperkte zichtbaarheid van politie en justitie als het gaat om online criminaliteit.

De pakkans schatten daders over het algemeen erg laag in vanwege beperkte politiecapaciteit en de ruime mogelijkheden voor anonimisering. De bevindingen laten tevens zien dat daders het risico om gepakt te worden over tijd, naarmate men vaker ongezien wegkomt, steeds lager gaan inschatten.

Ten aanzien van de perceptie van de schade is naar voren gekomen dat daders, vooral jonge daders, de omvang en ernst van de schade als gering inschatten alsook de schade bagatelliseren of ontkennen (neutralisatie). Hoewel ontkenning van het slachtoffer of de aangerichte schade ook bij daders van traditionele criminaliteit voorkomt, wordt dit online versterkt door de afstand tot slachtoffer, de hyperrealiteit waarin het gedrag tot stand komt (het voelt als spel), de normalisering die ontstaat door gamen (waar het routine en normaal is om elkaar te DDoSsen of te hacken) en door het gemak waarmee bepaalde delicten (in hoge frequentie) gepleegd kunnen worden. Tevens zorgt

[15] *Responsible Disclosure* (RD) betreft het "binnen de ICT-wereld (...) op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure" (Nationaal Cyber Security Centrum, 2013, p. 5).

de online omgeving voor minder remmingen vanwege afwezigheid van het oordeel van anderen of andere gevreesde consequenties. Door de online anonimiteit van daders en slachtoffers vindt dus een andere evaluatie van het gedrag door de dader plaats, dan wanneer de interactie offline zou zijn (ook wel *online disinhibition effect* genoemd). Bij oudere daders lijkt het bagatelliseren van de schade een minder grote rol te spelen. Zij erkennen de schade maar de drijfveren die zij hebben voor het gedrag (financieel, wraak, ideologisch, etc.) zijn voor hen belangrijk genoeg om de carrière voort te zetten.

Criminele carrières

Bij het in kaart brengen van criminele carrières van daders is gekeken naar factoren die een rol spelen bij het ontstaan (de initiatie), de ontwikkeling van de carrière en wat daders (los van een interventie) doet stoppen.

Als het gaat om de initiatie, zien we dat net als bij traditionele criminaliteit factoren zoals de *maturity gap* (de discrepantie tussen biologische en maatschappelijke volwassenheid), de invloed van delinquente *peers* (vrienden of leeftijdsgenoten) en bepaalde drijfveren (bijvoorbeeld geld, uitdaging of spanning) een rol spelen. Daarnaast zijn er factoren naar voren gekomen die specifiek een rol spelen bij de initiatie bij cybercriminaliteit zoals de interesse voor/affiniteit met ICT, gamen, veel tijd op fora spenderen en/of gemakkelijke toegang tot (kant-en klare) tools. In het kader van de ontwikkeling en rijping van de criminele carrière is uitgegaan van vier fasen die daders deels of allemaal doorlopen: 1) affectie voor computers (fase waarin interesse voor computers/IT ontstaat), 2) nieuwsgierige exploratie (fase waarin een interesse in hacken ontstaat), 3) illegale excursie (fase waarin illegale activiteiten worden geëxploreerd en ook een start gemaakt wordt met het plegen hiervan) en 4) criminele exploitatie (fase waarin stelselmatig delicten worden gepleegd). Gebleken is dat er veel variatie is met betrekking tot welke fase(n) door de daders word(t)(en) doorlopen. Dit kan variëren van daders die niet verder komen dan 'nieuwsgierige exploratie' en (doorgaans volwassen opportunistische) daders die gelijk in de 'criminele exploitatie' fase terecht komen tot daders die alle fasen doorlopen.

Ook bij daders die dezelfde fasen doorlopen, bestaat variatie als het gaat om hoe de ontwikkeling van het delictgedrag eruit ziet en welke factoren daarop van invloed zijn. Deze variaties hangen grotendeels samen met factoren die een rol spelen bij de initiatie alsook met de motieven, vaardigheden en mate van professionalisering. Tegelijkertijd spelen andere processen een rol als het gaat om het verloop van de criminele carrière, waaronder veranderingen in morele percepties (ofwel richting pro-crimineel ofwel richting pro-sociaal gedrag) en veranderingen in motieven (bijvoorbeeld van erkenning naar financieel).

Bij *desistance* (het stoppen met criminaliteit) zien we eveneens dat diverse factoren een rol spelen. Net als bij traditionele daders hebben volwassenwording en het krijgen van werk en een wederhelft invloed op het stoppen. Verondersteld wordt hierbij wel, voornamelijk door de experts, dat cyberdaders relatief meer kansen hebben op een (goede) baan vanwege de maatschappelijk behoefte aan digitaal talent. Ook laten de bevindingen zien dat er door de tijd heen, wat ook weer samenhangt met leeftijd en sociale bindingen, andere kosten en baten een rol kunnen gaan spelen. Daarbij zien we ook terug dat de motieven die aanvankelijk ervoor zorgden dat de daders deze delicten gingen plegen (bijvoorbeeld kick, uitdaging en spanning) er ook weer voor zorgen dat ze er mee stoppen. Over tijd nemen deze aspecten af of vallen helemaal weg. In het kader van stoppen wordt ook gewezen op factoren die *desistance* bemoeilijken. Naast het hebben van een strafblad wordt in dit kader gewezen op het feit dat daders helemaal kunnen opgaan in de online (delinquente) wereld,

zowel in termen van status en identiteit als (het snelle) geld, waardoor er nog te veel (materiële en immateriële) baten zijn om niet te stoppen.

DEEL 2 Interventies

In het tweede deel van het onderzoek is gefocust op de vraag in hoeverre bestaande interventies[16] voldoende aansluiten bij de (in deel 1) geschetste kenmerken en factoren. Aangezien interventies voor specifiek cyberdaders schaars zijn en er bovendien weinig (evaluatie)onderzoek is gedaan naar zowel traditionele als alternatieve interventies voor cyberdaders, zijn de bevindingen vooral gebaseerd op verwachtingen over de effectiviteit die uit de literatuur en de interviews konden worden afgeleid.

In de analyse van potentieel effectieve interventies is in de eerste plaats gekeken naar interventies gericht op afschrikking en situationele criminaliteitspreventie, die direct ingrijpen op de perceptie van de kosten-baten verhouding bij het plegen van cybercriminaliteit (rationele keuzebenadering). In de tweede plaats zijn interventies besproken die ingrijpen op de bestaande criminogene en protectieve factoren voor het plegen van cybercriminaliteit bij het individu en de verschillende contexten waarin het individu verkeert (op basis van *What Works* en de *desistance* benadering[17]). Hierbij wordt een onderscheid gemaakt tussen *risk-based* interventies, die ingrijpen op kenmerken die van invloed zijn op het delictgedrag (criminogene factoren/behoeften) en *strength-based* interventies, die meer gefocust zijn op aangrijpingspunten om het proces van de ontwikkeling van pro-sociaal gedrag en een pro-sociale identiteit te ondersteunen. Deels betreffen dit aangrijpingspunten voor het opheffen van risicofactoren, maar vooral wordt aangesloten bij protectieve factoren (*strengths*), zoals het ontwikkelen van talent, waarmee kansen voor de toekomst en daarmee perspectief en hoop wordt geboden. De *responsiviteit* van daders voor de geboden interventie is bij beide benaderingen een belangrijke thema.

Interventies die aansluiten bij de theorie van afschrikking en situationele criminaliteitspreventie

Volgens de rationele keuzebenadering zouden interventies effectief zijn als ze ofwel de kosten voor het plegen van een delict verhogen ofwel de baten verlagen. Situationele preventiestrategieën[18] (zoals *warning banners*[19] en het verstoren van digitale markten) kunnen een rol spelen bij het verhogen van het risico en de noodzakelijke inspanningen voor criminaliteit. Van alle beschreven interventies is verstoring (maatregelen gericht op het verstoren van het criminele uitvoeringsproces) de interventie die het meest direct ingrijpt op de inspanningen die geleverd moeten worden om delicten te plegen en daarmee op de kosten van het delict. Subgroepen voor wie deze interventie mogelijk effectief zijn, zijn daders met financiële drijfveren in alle fasen van hun loopbaan en daders (ongeacht hun drijfveren) die hun delicten plegen met behulp van gekochte tools.

Andere interventies die zich richten op verhoging van de gepercipieerde kosten, zijn interventies gericht op bewustwording van de risico's die het delict voor de dader meebrengt (zoals de kans op straf) of van de aangerichte schade (bewustzijn over deze schade kan gewetensvragen oproepen). Of dergelijke interventies effectief zijn, hangt af van de mate waarin de daders open staan

[16] We hanteren in het rapport een vrij ruime definitie van het begrip interventie. Alternatieven zoals hackwedstrijden noemen we in dit rapport 'interventie' omdat ze ingezet kunnen worden om gedragsbeïnvloeding te bewerkstelligen.
[17] *Risk-based* interventies sluiten nauwgezet aan bij inzichten uit de *What Works* benadering, waarbij de nadruk ligt op de behandeling van criminogene factoren. *Strength-based* interventies vinden vooral aansluiting bij theorieën over desistance. Echter, de benaderingen en hun inzichten over effectieve interventies overlappen elkaar ook gedeeltelijk. In het huidige onderzoek zetten we ze dan ook niet tegen over elkaar, maar beschouwen we als complementair. Tevens moet benadrukt worden dat sommige interventies zowel *risk-based* als *strength-based* elementen hebben.
[18] Het gaat om preventieve strategieën die gericht zijn op het wegnemen van de gelegenheid om criminaliteit te plegen en dus de risicoperceptie (en kosten) van de dader vergroten.
[19] Dit zijn digitale waarschuwingsberichten om te voorkomen dat iemand online delictgedrag vertoont.

voor de informatie die in de interventies wordt overgedragen (responsiviteit). Verondersteld kan worden dat deze interventies niet effectief zijn voor meer ervaren daders en daders die er drijfveren op na houden waarbij de strafbaarheid een onderdeel is van de opbrengsten (bijvoorbeeld spanning of status).

Belangrijk is dat bij deze interventies door experts ook steeds gewezen wordt op mogelijk averechtse effecten, zoals het genereren van nog meer spanning (die juist ten grondslag ligt aan plegen van de delicten) en het nemen van extra afschermingsmaatregelen door de daders. Daarentegen kan door de zichtbaarheid (van politie/justitie) die bewerkstelligd wordt met interventies gericht op bewustwording van de risico's, ook het gevoel van onaantastbaarheid verdwijnen en een aangepaste kosten-batenuitkomst ontstaan, wat hen mogelijk doet afzien van cyberdelicten.

Uit de bevindingen kan verder worden opgemaakt dat ten aanzien van de zekerheid, ernst en snelheid waarmee straf volgt op cybercriminaliteit (voorwaarden voor een afschrikwekkende werking) nog veel winst valt te behalen. Zowel de gepercipieerde als de daadwerkelijke pakkans wordt als zeer laag beschouwd door experts evenals daders. Daarnaast lijken volgens de experts de doorlooptijden van opsporing, vervolging en berechting bij cyberzaken langer te zijn dan bij 'traditionele' zaken, hetgeen onder meer te maken heeft met het feit dat het opsporingsonderzoek en ook het leveren van het bewijs complexer is.

Het antwoord op de vraag hoe 'zwaar' de straffen dienen te zijn om voldoende afschrikwekkend effect te sorteren, hangt volgens experts vooral af van de motivatie van de dader, waarbij een onderscheid wordt gemaakt tussen daders met een financieel motief en daders die jong, *first offender* en door nieuwsgierigheid gedreven zijn. Voor de laatstgenoemde groep daders zou het opgepakt worden of zelfs de dreiging daarmee middels een waarschuwingsgesprek met de politie (*knock and talk*) vaak al voldoende afschrikwekkend kunnen werken en bewustwording van strafbaarheid en schade teweegbrengen. Indien een interventie lange tijd nadat het delict gepleegd is alsnog wordt opgelegd (en de jongere mogelijk alweer veel verder is in zijn of haar ontwikkeling en/of al gestopt is) kan de interventie, indien geen rekening wordt gehouden met resocialiserende aspecten (zoals het geval is bij hoge boetes of lange gevangenisstraffen), voor deze groep een averechts effect sorteren. Tegelijkertijd zou volgens de literatuur en experts een voorbeeld gesteld moeten worden naar de samenleving toe door bij ernstige cyberzaken waar ondanks de lage pakkans toch een arrestatie en veroordeling volgt, ook een zware straf op te leggen. Daarvan zou volgens de respondenten een generaal preventief effect uitgaan (signaalfunctie).

Interventies die aansluiten bij de *What Works* en de *desistance* benadering

Risk-based interventies

Over (de effectiviteit van) de inzet van interventies gericht op de criminogene behoeften van cyberdaders (*risk*-based interventies) is in de literatuur en bij experts nog weinig bekend. Een belangrijke constatering hierbij is dat er nog nauwelijks sprake is van gevalideerde risicotaxatie bij deze groep daders. In de eerste plaats bleek dat er nog maar beperkt zicht is op hoe de criminogene factoren bij cyberdaders precies gemeten moeten worden (voorbeelden waren de kwaliteit van de ouderlijke supervisie en de wijze waarop persoonlijke en psychologische kenmerken gerelateerd kunnen worden aan delictgedrag in de online context). Daardoor lijken bestaande diagnose-instrumenten nog onvoldoende gevalideerd ten aanzien van de criminogene en protectieve factoren waarop interventies specifiek bij cyberdaders ingezet moeten worden. Daarnaast geven verschillende

experts aan dat er van (tijdige) risicotaxatie met de noodzakelijke verdiepende analyse door deskundigen bij deze dadergroep nog onvoldoende sprake is. Hiervoor lijkt een juiste 'routering' in het afdoeningsproces noodzakelijk.

Als het gaat om de vraag welke interventies effectief zouden kunnen zijn voor cyberdaders, wordt door experts veelal verwezen naar bestaande interventies voor traditionele daders. Deze zijn gericht op diverse leefgebieden zoals het verbeteren van de relatie met ouders, het aanleren van sociale vaardigheden, het aanpakken van een pro-criminele houding en het werken aan schulden of verslaving. Deze interventies zouden effectief kunnen zijn voor het aanpakken van de betreffende criminogene factor bij daders van verschillende leeftijden en in verschillende fasen van de criminele loopbaan mits motivatie voor verandering aanwezig is of kan worden gecreëerd. De verwachting is echter dat cyberdaders in het algemeen onvoldoende responsief zullen zijn voor (de meeste van) deze interventies omdat deze geen of te weinig rekening houden met de online context waarin de delicten plaatsvinden (waarin schade minder zichtbaar is en het slachtoffer erg 'abstract'). Om daar meer rekening mee te houden, wordt door experts verwacht dat een methode als *mentaliseren*, wat inleven in een ander inhoudt, zinvol kan zijn. Ook verwachten experts, ondanks zeer beperkte ervaring hiermee, positieve effecten van contact met het slachtoffer door middel van herstelbemiddeling.

De enige specifiek op cyberdaders gerichte interventies die gevonden zijn, zijn het opleggen van restricties rondom computer- en internetgebruik en de inzet van *serious gaming*. Bij dit laatste worden jongeren op een spelende manier goede en slechte manieren van hacken geleerd en worden ze tegelijkertijd aan het denken gezet hierover. Dergelijke interventies kunnen onder meer zorgen voor het afsluiten van contact met online criminele *peers* (een belangrijke criminogene factor). Een dergelijke afsluiting is echter complex te bewerkstelligen en zal altijd tijdelijk zijn. Deze interventie moet dus gezien worden als een interventie die een momentum schept voor andere interventies die op de langere termijn *desistance* in gang kunnen zetten (door bijvoorbeeld het ombuigen van de pro-criminele houding en het aanreiken van alternatieven). De inzet van *serious gaming* is potentieel effectief voor jonge, niet-kwaadwillende daders die op deze manier spelenderwijs bewust worden gemaakt van goede en slechte aspecten van het hacken. Dit is daarmee een relatief lichte interventie die bij kan dragen aan kennis over ethiek en bewustwording bij jonge hackers. Hoewel geen negatieve effecten kunnen worden verwacht van deze interventie, blijft het nog de vraag of de effecten die gegenereerd worden in een spelsetting ook in 'real life' effect hebben. Daar staat weer tegenover dat *serious gaming* plaatsvindt in een context van begeleiding en er naar alle waarschijnlijkheid over ethische grenzen wordt gesproken. Bij dit laatste resteert de vraag in hoeverre men vatbaar (responsief) is voor deze informatie en of hun morele kompas daadwerkelijk wordt bijgestuurd. Meer onderzoek is nodig om antwoord te kunnen geven op deze vragen.

Strength-based interventies

Behalve voor interventies gericht op het verminderen van criminogene behoeften, is in de literatuur en onder experts ook aandacht voor *strength-based* interventies, interventies die vooral gericht zijn op het versterken van de pro-sociale identiteit. Meer dan bij daders van traditionele criminaliteit zijn bij een deel van de daders van cybercriminaliteit in engere zin talenten (technische vaardigheden) aanwezig die veel waarde hebben voor de samenleving mits ze op een pro-sociale manier worden ingezet (ethisch hacken). Interventies kunnen hierbij aansluiten door perspectieven te bieden van wat zij met deze vaardigheden zouden kunnen bereiken op de arbeidsmarkt. Door experts in dit kader veelgenoemde preventieve interventies zijn cyberwerkplaatsen[20] en hackwedstrijden.[21] Deze interventies zijn gericht op het vergroten van IT-vaardigheden en het aanleren van ethisch hacken.

[20] Een plek waar IT-vaardige jongeren terecht kunnen om bijvoorbeeld workshops te volgen of aan IT-projectjes te werken

[21] Dit zijn doorgaans door private partijen gesponsorde hackwedstrijden waarbij hackers op verzoek systemen hacken

Door dergelijke interventies krijgen jongeren tevens erkenning, leren zij gelijkgestemden kennen (die net als zij veel interesse in IT hebben) en wordt gebouwd aan (zowel technische als sociale) vaardigheden en toekomstperspectief. Een andere vorm van een *strength-based* interventie(onderdeel) is begeleiding door rolmodellen.[22] Uit zowel de literatuur als de expertinterviews komt naar voren dat dit een belangrijk element is bij het opbouwen van een nieuwe prosociale identiteit en relaties. Rolmodellen kunnen ook een signaalfunctie hebben, omdat eventueel grensoverschrijdend gedrag opgemerkt en gecorrigeerd kan worden.

Een specifiek op cyberdaders gerichte (reactieve) interventie is de recent ontwikkelde Hack_Right interventie, die zich onder meer richt op het versterken van talent en het ethisch leren hacken door middel van een leerwerkplek bij een IT-bedrijf, waarbij ervaren hackers als coaches (rolmodellen) worden ingezet. De interventie lijkt goed aan te sluiten bij de *desistance* benadering, omdat wordt beoogd jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving. Hoewel de interventie formeel nog door de Erkenningscommissie Justitiële Interventies[23] moet worden erkend, zijn experts erg verwachtingsvol over wat dit voor de doelgroep (jong, *first offender*, technisch vaardig, geen ernstig delict, schuld bekend en gemotiveerd) kan betekenen. Ook zijn er enkele kritische geluiden, bijvoorbeeld waar het gaat om de vraag of een dergelijke interventie strafbaar gedrag juist niet beloont. Bezien vanuit de theorie van afschrikking, genereert een dergelijke interventie mogelijk onvoldoende specifieke en wellicht ook generale afschrikking.

Bij de inzet van *strength-based* interventies is het uiteraard van belang dat de juiste doelgroepen worden geselecteerd, waarbij de drijfveren voor het delictgedrag een belangrijk criterium lijken te vormen. Alleen werken aan het vergroten van de IT-vaardigheden en het bieden van een netwerk of carrièrekansen zonder dat gewerkt wordt aan het moreel besef en het ombuigen van een eventuele pro-criminele houding, kan immers tot meer cybercriminaliteit leiden. Indien de verschillende onderdelen in combinatie terugkomen in de interventie, bieden *strength-based* interventies niet alleen kansen aan cyberdaders, maar zouden ze mogelijk ook tot een afname van toekomstig daderschap kunnen leiden en daarmee tot een positieve uitkomst voor de samenleving.

Conclusies en aanbevelingen

In dit onderzoek is een analyse gemaakt van de (unieke) kenmerken van cyberdaders en de mate waarin beschikbare interventies aansluiten bij deze kenmerken. Het onderzoek laat zien dat we met alles behalve een homogene groep daders te maken hebben. Er is veel variatie te zien, zowel wat betreft drijfveren als criminogene en protectieve factoren voor het plegen van cybercriminaliteit. In meer algemene zin kan geconcludeerd worden dat een aantal criminogene factoren zowel bij traditionele daders als bij cyberdaders een rol spelen, zoals gezinsproblematiek, bagatellisering van ernst en schade van het gepleegde delict evenals bepaalde motieven (kick, plezier en geld). Echter, door de online omgeving en (technische) aard van de delicten kunnen zij anders tot uiting komen. Tevens hebben we kenmerken aangetroffen die relatief vaker voor lijken te komen bij cyberdaders dan bij traditionele daders of vrij uniek zijn voor deze dadergroep. Hier gaat het bijvoorbeeld om persoonlijkheids- of psychologische kenmerken die bijdragen aan de noodzakelijke talenten voor het tot stand komen van de delicten (nieuwsgierigheid, leergierigheid, zelfcontrole, perfectionisme, behoefte aan erkenning en bewijsdrang ten aanzien van technische vaardigheden) of om

[22] In dit geval gaat het om mensen uit de hackerswereld (bijvoorbeeld ethische hackers) die een voorbeeldfunctie en/of mentorrol vervullen.

[23] Voor meer informatie over deze commissie en de werkwijze, zie: https://www.nji.nl/nl/Databank/Databank-Effectieve-Jeugdinterventies/Deelcommissie-Justitiele-interventies

persoonlijkheids- of psychologische kenmerken die offline sociale interactie bemoeilijken (zoals introversie, kenmerken van een autismespectrumstoornis en sociale onhandigheid).

Naar aanleiding van onze bevindingen kunnen een drietal aanbevelingen worden gedaan met betrekking tot de wijze waarop interventies voor cyberdaders vormgegeven moeten worden.

In de eerste plaats is het van belang dat er *meer* en meer *toegesnede*n verdiepingsdiagnostiek plaatsvindt ten behoeve van beslissingen over (strafrechtelijke) interventies voor cyberdaders. Nu de diversiteit onder cyberdaders groot blijkt, is een op maat gesneden aanpak van belang en daartoe moeten de criminogene en protectieve kenmerken en de wijze waarop deze het delictgedrag in de online omgeving beïnvloeden in kaart worden gebracht. De huidige instrumenten lijken nog onvoldoende in staat om deze specifieke cyberdader gerelateerde kenmerken te meten. Naast criminogene behoeften is daarbij ook specifiek aandacht nodig voor responsiviteit voor interventies (leerstijlen en motivaties) van cyberdaders die in een online omgeving hun delicten plegen. Voor cyberdaders lijkt het aangewezen dat specifieke aanvulling op bestaande diagnose-instrumenten beschikbaar komt.

In de tweede plaats lijken interventies waarin bewustwording, mentaliseren (inleven in de ander), moreel redeneren (in combinatie met ethisch hacken) en het aanbieden van kansen gecombineerd worden veel potentie te hebben om effectief te zijn voor met name jonge technisch vaardige daders. Echter, deze interventies blijken ook ongewenste effecten op te kunnen leveren, omdat ze daders onbedoeld op ideeën kunnen brengen of de status van cyberdaders bij hun peers kunnen verhogen. Het is dus belangrijk om van deze interventies zowel de bedoelde als de onbedoelde effecten goed te onderzoeken en duidelijke doelgroepen te beschrijven voor wie de interventies potentieel effectief zijn effectief zijn.

In de derde plaats bleek dat voor zowel jongere als oudere daders in verschillende fasen van de criminele loopbaan, maar met andere drijfveren dan nieuwsgierigheid en het zoeken van mentale uitdaging, traditionele interventies potentieel geschikt zijn. Dit betreft de interventies die zich richten op specifieke criminogene factoren (zoals verslaving, gebrek aan sociale vaardigheden of ondersteunende relaties). Deze interventies houden echter nog geen rekening met de responsiviteit van cyberdaders in de online context waardoor de effectiviteit voor deze doelgroep waarschijnlijk tegenvalt. Onze laatste aanbeveling is dan ook om na te gaan welke aanpassingen er in deze bestaande interventies nodig zijn om aan te sluiten bij de responsiviteit van cyberdaders.

Summary

Background and research question

Recent developments indicate that hacking[24], DDoS attacks[25], ransomware[26] and other forms of cyber-focused crime[27] are on the rise among both adolescents and adults. The scientific knowledge about cyber offenders is limited, anecdotal, outdated and fragmented. This research attempted to generate more systematic knowledge about the characteristics and profiles of juvenile and adult offenders of cyber-focused crime, as well as to provide insight into appropriate and effective interventions for this offender group. The following research question has been addressed in this research:

"What are the differences between the profile(s) of cyber offenders and offenders of" traditional "crime and what are the implications of those differences for the nature of interventions for cyber offenders?"

Research methods

In this qualitative research a combination of different research methods was used. First, two systematic literature studies have been conducted: one focused on characteristics of cyber offenders and one concentrated on interventions for cyber offenders. The first search yielded 99 sources about characteristics of offenders of cyber-focused crime, whether or not compared to traditional offenders. The second search yielded 25 sources about interventions aimed at offenders involved in cyber-focused crime. Secondly, expert interviews were conducted (29 individual interviews, 2 focus groups, 1 expert meeting and 1 round table). A total of 52 experts from virtually all partners in the security chain (police, Public Prosecution Service, judiciary, legal profession, (youth) probation service, Child Protection Board, Halt and care providers) were interviewed as well as industry experts, researchers and freelancers who have knowledge about cyber offenders and/or interventions. Thirdly, 14 interviews with adult offenders were conducted. Of these offenders, the majority was convicted of one or more cyber-focused offences (including hacking, DDoS attacks, virtual theft[28]) and the minority was involved in those crimes, but never got caught. Hacking was the primary offence in most cases. The judicial interventions imposed on the offenders mainly concern community service orders, but some offenders also received a (conditional) prison sentence, contact prohibition, fine, compensation or electronic detention. Four offenders did not receive any judicial intervention and two offenders were still awaiting their criminal case at the time of the interview.

Limitations of the research

The research has a number of limitations. First, the literature study has its limitations. For example, relatively much literature has been found on hackers (albeit much outdated literature and usually small samples), but little information was available on offenders involved in other forms of cyber-focused crime such as DDoS attacks and ransomware. In addition, only a few (effect) studies were found in which the application of traditional or cyber-related interventions to cyber offenders was examined. Hence little systematic knowledge is available about the effectiveness of interventions for cyber offenders. Secondly, regarding the expert interviews, various respondents only got involved with a limited number of cyber offenders. The answers of these experts are therefore based on a small number of cases and their perceptions are perhaps also partly influenced by stories from colleagues,

[24] This refers to the unlawful intrusion into a computer system.
[25] This refers to disrupting or breaking down a system through overloading it with traffic.
[26] This refers to malicious software (malware) that can be used to take a system "hostage" or block it so that the victim has to pay ransom.
[27] Cyber-focused crime refers to crime in which ICT is both the means and a substantial target. In the full Dutch report we use the term 'cybercrime in the narrow sense' [cybercrime in enge zin]
[28] This refers to theft of goods in a virtual game.

images from the media or the social debate. Thirdly, the interviewed offenders form a selective group (adult, majority convicted and hacking in most cases being the primary offence). Consequently, we obtained less information about other types of offending. Finally, the results depend on the self-report of the offenders. The offenders may not have reported all their delinquent behaviour, withheld recent offences or, on the contrary, portrayed their criminal career as "more successful" than they really were.

Findings

Part 1 Offender characteristics

The first part of the report focused on the specific characteristics of cyber offenders and the extent to which different offender profiles can be constructed based on those characteristics. Additionally, the characteristics were compared with the characteristics of traditional offenders, so that differences among them could be described. In this context we distinguished (offline and online) *criminogenic* (risk factors that contribute to the delinquent behaviour) and *protective* factors (factors that can prevent or restrain delinquent behaviour). In the analysis of the offender group, we used insights from various criminological approaches such as the differential association theory[29], neutralisation techniques[30] and the rational choice theory. [31] Concepts have also been applied that have been specifically developed to explain online and technical aspects of offending such as the online disinhibition effect[32], digital drift[33] and mastery. [34]

Profiles

During the research we came to the realisation that a simple clustering or profiling based on the presence or absence of certain characteristics does not produce a realistic picture. The offenders have different characteristics and factors (personal and contextual) and specific motivations (such as mental challenge or status) that occur in different combinations and degrees. This then leads to (a certain development in) the delinquent behaviour (criminal career). For this reason, the profiling of cyber offenders has been approached by describing the impact of various characteristics and factors on the delinquent behaviour, both individually and in their mutual coherence.

Background characteristics

Literature has shown that cyber-focused crime is relatively more often committed by young men with a non-migrant background and a reasonable to good socio-economic background. In the subgroup of financially oriented cyber offenders, the age of onset is generally higher. There are also indications that these offenders more frequently have an ethnic minority background as well as a lower socio-economic
status.

Although the level of education among cyber offenders varies, it appears that there is a relatively higher level of intelligence and education compared to traditional offenders. Sometimes

[29] This theory assumes that delinquent behavior is taught in intimate peer groups. This involves the learning of techniques for committing crime as well as norms, values and attitudes.
[30] This refers to techniques that offenders can use to legitimise delinquent behavior.
[31] This approach assumes that delinquent behavior results from and can be understood as a rational cost and benefit assessment. This can involve both material (money) and non-material costs and benefits (fame, pleasure).
[32] This refers to the disappearance of inhibitions due to online anonymity.
[33] This refers to the way in which the internet offers both technical and social affordances that can intensify certain forms of delinquency or offer new possibilities for committing crime.
[34] This refers to the need or urge to master the technology and is accompanied by a sense of power and control.

offenders do not complete their education, which does not automatically entail that they end up in low-skilled work. The work and training that cyber offenders do or have done varies, but training and jobs in the IT sector are over-represented. In their leisure time, cyber offenders spend a lot of time on technology, IT, gaming and social media. In addition, they also have a wide range of other hobbies. The domestic situation (including the role of family problems) varies greatly. There often seems to be a lack of parental controls on the online behaviour of cyber offenders, both in families with and without family problems. This limited supervision is partly caused by poor knowledge of parents[35] of the internet and the online world. Finally, cyber offenders can be characterised as intelligent. More often than traditional offenders, cyber offenders appear to have features from an autism spectrum disorder (ASD) and a strong problem-solving capacity. The findings also suggest that there is a distinction between cyber offenders who experience lower levels of self-control and are impulsive versus offenders who set long-term goals and are perfectionist. According to the literature and the experts, some offenders can be characterised as introvert or socially awkward, but another part (of which many of the interviewed offenders feel they belong to) seems to be sufficiently socially competent. Whereas most offender have built up an extensive online peer network, their offline network is relatively smaller and had less impact on their offending behaviour.

Motivations and experience

The research shows that various motivations are involved in cyber offending. We also found that offenders have multiple motivations simultaneously and that motivations can change over time.

The motivation curiosity, desire for knowledge and (mental) challenge are motivations that we mainly find among juvenile cyber offenders. These motivations are not necessarily malicious. Young offenders driven by these motivations want to learn the ins and outs of systems and seek to discover how far they can go with technology. In contrast to most traditional forms of crime, learning and obtaining knowledge is a goal or motivation in itself and not just a means or instrument for committing the offence. Other motives that we encountered in the research are the kick, excitement, pleasure, boredom, the urge to collect (information) and power. These drives can also play a role in traditional crime, but with cyber-focused crime there is stronger interconnection with online skills and technology. Recognition, status, peer respect and the urge to prove yourself are also important motives for juvenile offenders. They want to prove what they can do to gain respect or fame. The difference with traditional crime is that the focus lies more on technical skills, abilities and your performance (what you are able to 'do'). Financial motives seem to play a less prominent role for juvenile (individual) offenders. In some cases, money can in a later stage play a role in the criminal career, depending also on the activities in which the offender is involved. The financial motive seems to be most prominent among (adult) offenders who are active in the context of fraud and organised cybercrime. In some cases, the offenders involved have made the transition from traditional (offline) fraud to cybercrime. In addition, cybercrime (mainly hacking or carrying out DDoS attacks) can be committed out of anger or to take revenge on friends, family, former employers or former lovers with whom an offline conflict was going on. These motivations we mainly find among adult traditional offenders who have discovered a new means of expressing their frustration. There are also offenders who act on ideological grounds. The latter two clusters of motivations have remained relatively underexposed in this study.

Perceptions with regard to the likelihood of getting punished, the risk of getting caught and the damage of the committed crimes

When it comes to the perception with regard to the likelihood of getting punished, there seems to be a sliding scale. On the one side of the scale we find (mostly young) offenders who are not or hardly

[35] The IT knowledge of parents may depend on their age. This aspect we did not examine in the current study.

aware of the likelihood of getting punished and on the other end of the scale we can locate offenders who are well aware of the penalties they might face. They obtained this knowledge, for example, through online forums. The limited awareness of the likelihood of getting punished, which is present among part of the offenders, can be explained by different factors, including the absence of supervision in the online world, the invisibility of the inflicted damage and - for some of the offenders – the involvement of motivations that are not necessarily malicious in nature (curiosity, mental challenge, recognition of talents). The latter category also includes offences in which security problems are demonstrated, involving uncertainty about the legal boundaries and the frameworks of responsible disclosure[36]. The limited perception of the likelihood of getting punished is therefore a more important criminogenic factor for cyber offenders than for traditional offenders. As the career continues, the awareness of criminality among offenders increases, but according to experts, this is partly overturned by the very limited visibility of the police and the judiciary when it comes to online crime. The chance of being caught is generally very low due to limited police capacity and the possibility of anonymisation. The findings also show that the perception of the risk of being caught decreases over time, depending on the frequency of getting away with the crimes unseen.

With regard to the perception of the damage or harm, it appeared that offenders, especially young offenders, perceive the extent and seriousness of the damage their crime inflicts as minor. They also seem to downplay or deny the damage or victim (neutralisation). Although such denial can be also found among offenders of traditional crime, this aspect is reinforced online due to the distance to the victim, the hyper-reality in which the behaviour comes about (it feels like a game), the normalisation that arises from gaming (where it is both a routine and normalised practice to launch DDoS- attacks or hack each other) and the ease with which certain crimes can be committed (in high frequency). The online environment also ensures fewer inhibitions due to the absence of the judgment of others or other dreaded consequences. Due to the online anonymity of offenders and victims, a different evaluation of the behaviour of the offender takes place than when the interaction would be offline (also known as online disinhibition effect). For older offenders, the downplaying of the damage appears to play a lesser role. They acknowledge the damage but the motivations they have for behaviour (financial, revenge, ideological, etc.) are important enough for them to continue the career.

Criminal careers

In order to map the criminal careers of cyber offenders, we looked at factors that contribute to the onset (initiation), the development of the career over time and to what makes offenders (independent of an intervention) desist.

When it comes to the initiation, we observed that, like traditional crime, factors such as the maturity gap (the discrepancy between biological and social maturity), the influence of delinquent peers and certain motivations (such as money, challenge or thrill) play a role. In addition, we found factors that play a specific role in the initiation of cybercrime such as interest in or affinity with IT, gaming, spending a large amount of time on forums and/or easy access to (ready-to-use) tools. When it comes to the development and maturation of the criminal career, we presumed that offenders go through (in part or all) four phases: 1) affection for computers (phase where an interest in computers/IT arises), 2) curious exploration (phase in which an interest in hacking emerges), 3) illegal excursion (phase in which illegal activities are explored) and 4) criminal exploitation (phase in which offences are systematically committed). The findings suggest that there is quite some variation with regard to which phase (s) the offenders go through. This can vary from offenders who do not go further than "curious exploration" and (usually adult opportunistic) offenders who almost immediately end up in the "criminal exploitation" phase to offenders who go through all phases.

We can also observe variation among offenders who go through the same phases when it comes to how the development of the delinquent behaviour looks like and which factors influence it.

[36] Responsible Disclosure (RD) concerns the “disclosure of IT vulnerabilities in a responsible manner and in joint collaboration between the person reporting and the organisation on the basis of a responsible disclosure policy established by organisations for this purpose within the ICT world (...). (National Cyber Security Centre, 2013, p. 5).

These variations are largely related to factors that play a role in the initiation as well as the motivations, skills and degree of professionalisation. At the same time, other factors play a role in the course of the criminal career, including changes in moral perceptions (either towards pro-criminal or towards pro-social behaviour) and changes in motives (for example, a transition from recognition to financial drives). In the case of desistance (ending the criminal career) we also see that various factors play a role. Just as with traditional offending, maturing and getting employed and another half influence quitting. In this regard, it is assumed, mainly by the experts, that cyber offenders have relatively more chances of finding a (good) job due to the social need for digital talent. The findings also show that other costs and benefits can play a role over time, which is also related to age and social ties. In addition, we also see that the motives that initially contributed to the onset of committing these offences (such as challenge, kick and excitement) eventually also led to desistance for the reason that they fade away or disappear over time. In the context of desistance, the research also drew attention to factors that make this process more difficult. Apart from having a criminal record, offenders can be completely absorbed in the online (delinquent) world, both in terms of status and identity and (the fast) money, leaving too much (material and immaterial) benefits or incentives not to stop.

PART 2 Interventions

In the second part of the research, we focused on the extent to which existing interventions[37] adequately correspond to the characteristics and factors outlined in part 1. Since interventions for specific cyber offenders are scarce and, moreover, little (evaluation) research has been carried out into both traditional and alternative interventions for cyber offenders, the findings are mainly based on *expectations* about the effectiveness that could be derived from the literature and the interviews.

For the analysis of potentially effective interventions we firstly looked at interventions aimed at deterrence and situational crime prevention, involving interventions that directly aim to influence the perception of the cost-benefit ratio of offenders when committing cybercrime (rational approach to choice). Secondly, interventions were discussed that are directed to the involved criminogenic and protective factors for perpetrating cybercrime, taking into account the individual and the different contexts in which the individual finds himself (based on What Works and the desistance approach[38]). A distinction is made here between *risk-based* interventions, which target characteristics that influence the delinquent behaviour (criminogenic factors/needs) and *strength-based* interventions, which aim to provide assistance in the process of developing pro-social behaviour and a pro-social identity. In part, this assistance can also contribute to the elimination of risk factors. Yet, they mainly seek to focus on the protective factors (*strengths*), such as the development of talent, which offer opportunities for the future and thus offer perspective and hope. The responsiveness of offenders to the intervention offered is an important theme in both approaches.

Interventions that correspond with deterrence theory and situational crime prevention

According to the rational choice approach, interventions are effective if they either increase the costs of committing a crime or reduce the benefits. Situational prevention strategies[39] (such as warning banners[40] and the disruption of digital markets) can play a role in increasing the risk and the necessary

[37] In this research we maintain a broad definition of interventions. Alternatives such as hacker competition are also termed 'intervention' since they can contribute to behavioural change.

[38] Risk-based interventions closely correspond to insights from the What Works approach, which places the emphasis on the treatment of criminogenic factors. Strength-based interventions mainly correspond to theories about desistance. However, the approaches and their insights about effective interventions also partially overlap. In the current research, we therefore do not oppose them, but we regard them as complementary. It should also be emphasised that some interventions have both risk-based and strength-based elements.

[39] This refers to preventative strategies aimed at taking away the opportunity to commit crime and thus increasing the perception of risk (and costs) of the offender.

[40] This refers to digital warning messages to prevent someone from displaying online crime behavior

efforts for committing the crime. Of all the interventions described in the research, disruption (measures aimed at disrupting the criminal executive process) is the intervention that most directly affects the efforts that must be made to commit these offences and thus increases the costs of committing the offence. Subgroups for whom this intervention may be effective are offenders with financial motives in all phases of their criminal career and offenders (regardless of their motives) who commit their crimes with the help of purchased tools.

Other interventions aimed at increasing perceived costs are interventions directed at raising awareness of the risks that come along with committing the offence (such as the risk of getting punished) or awareness of the damage inflicted (awareness of this damage might affect the moral perception). Whether such interventions are effective depends on the extent to which the offenders are responsive to the information transferred in the interventions (responsiveness). It can be assumed that these interventions are not effective for the more experienced offenders and offenders for whom the likelihood of getting punished is actually part of the benefits that come along with the offending (for example, thrill or status).

The interviewed experts also point out that these interventions can have potential adverse effects, such as generating even more thrill (which is precisely why some offenders commit these offences) and taking extra measures for anonymisation by the offenders. On the other hand, the visibility (of law enforcement) that is achieved by means of interventions that are aimed at raising awareness of the risks, can also make the sense of inviolability disappear. Consequently, an adjusted cost-benefit outcome may arise, which may make them abandon cybercrimes.

From the findings it can further be concluded that still much could be gained in respect to the certainty, severity and speed with which punishment follows the crime (conditions for a deterrent effect). Both the perceived and actual chance of being caught is considered very low by experts as well as by offenders. In addition, according to the experts, the process of investigation, prosecution and trial appear to be longer in cyber cases than in "traditional" cases, which is partly due to the fact that the investigation and the provision of evidence is more complex.

According to experts, the answer to the question of how 'severe' the penalties should be in order to have sufficient deterrent effect depends mainly on the motivation of the offender, whereby a distinction is made between offenders driven by financial motivations and offenders who are young, first offender and driven by curiosity. For the latter group of offenders an arrest or even the threat of an arrest by means of a warning conversation with the police (knock and talk[41]) can often be sufficiently deterrent and raise awareness of the likelihood of getting punished and the inflicted damage. If an intervention is still imposed a long time after the offense has been committed (and the juvenile offender may be much further in his or her development and may have already desisted), the intervention may, if resocialising aspects are not taken into account (e.g. in the case of high fines or imprisonment), have a counterproductive effect for this group. At the same time, the literature and experts point out that – as the likelihood of getting caught (especially for more serious cybercrime cases is relatively lower), an example should be set towards society by also imposing a serious punishment. This could produce a general deterrent effect (signaling function).

Interventions that correspond with the What Works and the desistance approach

Risk-based interventions

Based on the literature study and the expert interview, we can conclude that still little is known about the (effectiveness of the) use of interventions aimed at the criminogenic factors of cyber offenders (risk-based interventions). An important observation is that there is hardly any validated risk assessment for this group of offenders. First of all, it turned out that there is only limited insight into how the criminogenic factors of cyber offenders should be measured precisely (for example when it comes to the quality of parental supervision and the way in which personal and psychological

[41] This intervention is also known as 'cease and desist'.

characteristics can be related to delinquent behaviour in the online context). As a result, existing diagnostic instruments still appear to be insufficiently validated with regard to criminogenic and protective factors on which interventions must be specifically deployed for cyber offenders. In addition, various experts indicate that there is insufficient evidence of (timely) risk assessment with the necessary in-depth analysis by experts in this offender group. In order to accomplish this, a correct "routing" seems necessary in the settlement process.

When it comes to the question of which interventions could be effective for cyber offenders, experts often refer to existing interventions for traditional offenders. These are aimed at various areas of life such as improving the relationship with parents, learning social skills, tackling a pro-criminal attitude and working on debts or addiction. These interventions could be effective in tackling the relevant criminogenic factor in offenders of different ages and in different phases of the criminal career, only in case the motivation for change is present or can be created. However, it is expected that cyber offenders generally will not be sufficiently responsive to (most of) these interventions because they take little or no account of the online context in which the offences take place (in which damage is less visible and the victim is very 'abstract'). To take this aspect more sufficiently into account, experts put forward that a method such as 'mentalising', involving empathising with another person, can be useful. Experts also expect, despite very limited experience, positive effects of contact with the victim through recovery mediation.

The only interventions specifically targeted at cyber offenders that we found, are the imposition of restrictions on computer and internet use and the use of serious gaming. In serious gaming, young people are taught good and bad manners of hacking in a playful way and at the same time they are encouraged to think about ethical issues. Such interventions can, among other things, ensure that contact with online criminal peers does not take place (an important criminogenic factor). However, preventing such contact is complex to achieve and will always be temporary. This intervention must therefore be seen as an intervention that creates a momentum for other interventions that can trigger desistance on the long term (by, for example, changing the pro-criminal attitude and offering alternatives). The use of serious gaming is potentially effective for young, non-malicious offenders who playfully get aware of good and bad aspects of hacking. This is therefore a relatively light intervention that can contribute to knowledge about ethics and awareness among young hackers. Although no negative effects can be expected from this intervention, the question remains whether the effects that are generated in a game setting also have a *real-life* effect. On the other hand, serious gaming takes place in a context of guidance and ethical boundaries are most likely discussed. Still, the question remains to what extent offenders are responsive to this information and thus susceptible to adjusting their moral compass. More research needs to be done to provide answers to these issues.

Strength-based interventions

In addition to interventions aimed at reducing criminogenic factors (needs), the literature and experts also focus on strength-based interventions, interventions that are primarily aimed at strengthening the pro-social identity. More than offenders of traditional crime, a part of the offenders of cyber-focused crimes have talents (technical skills) that are of great value to society, only in case they are used in a pro-social manner (ethical hacking). Interventions can respond to this by providing more information to offenders about what they could achieve on the labor market with these skills. Preventative interventions mentioned by experts in this context are cyber workplaces[42] and hacking competitions.[43] These interventions are aimed at increasing IT skills and teaching ethical hacking. Such interventions also give young people recognition, enable them to meet like-minded people (that share the same interest in IT) and build on (both technical and social) skills and future prospects. Another

[42] This refers to a place where IT-skilled young people can go to, for example, attend workshops or work on IT projects.

[43] This refers to hacking competitions that are (commonly) sponsored by private parties in which hackers hack systems on request.

form of a strength-based intervention (component) is guidance by role models.[44] Both the experts and the literature identify this as an important element in building a new prosocial identity and relationships. Role models can also have a signaling function, because any deviant behaviour can be noticed and corrected.

A specific (reactive) intervention aimed at cyber offenders is the recently developed *Hack_Right* intervention. This intervention among others aims to strengthen talent and to learn offenders to hack ethically through a working/learning trajectory at an IT company. In this context, experienced hackers are used as coaches (role models). The intervention seems to correspond well with insights from the desistance approach, because it assists young cyber offenders in developing a pro-social identity and role in society. Although the intervention still needs to be formally recognised by the Judicial Interventions Recognition Committee[45], experts have high expectations about what the intervention can achieve for the target group (young, first offender, technically skilled, no serious offence, pleading guilty and motivated). There are, however, also some critical notes, for example with regard to the question whether such an intervention actually rewards criminal behaviour. Viewed from the perspective of deterrence, such an intervention may generate insufficient special and perhaps also general deterrence.

When imposing strength-based interventions, it is of course important that the right target groups are selected, whereby the motives for the delinquent behaviour appear to be an important criterion. After all, only working on enhancing IT skills and offering a network or career opportunities without working on the moral awareness and turning a possible pro-criminal attitude can lead to more cybercrime. If the various components are combined in the intervention, strength-based interventions not only offer new opportunities to cyber offenders, but they could possibly also lead to a decrease in future offending and thus result in a positive outcome for society.

Conclusions and recommendations

In this research we analysed the (unique) characteristics of cyber offenders and the extent to which available interventions correspond to these characteristics. The research shows that we are dealing with everything but a homogeneous group of perpetrators. There is a lot of variation, both in terms of motivation and criminogenic and protective factors for committing cyber-focused crime. In a more general sense, it can be concluded that a number of criminogenic factors contribute both to traditional and cyber offending, such as family issues, downplaying the severity and damage of the crime committed and certain motives (kick, pleasure and money). However, due to the online environment and (technical) nature of the offences, they can be expressed differently. We have also found characteristics that seem to occur relatively more often with cyber offenders than with traditional offenders or characteristics that are quite unique for this offender group. This concerns, for example, personality or psychological characteristics that contribute to the necessary talents for the occurrence of the offences (curiosity, eagerness to learn, self-control, perfectionism, need for recognition and the urge to prove oneself of technical skills) or personality or psychological characteristics that make offline social interaction more difficult (such as introversion, characteristics of an autism spectrum disorder and social awkwardness). Based on our findings, we present three recommendations with regard to how interventions for cyber offenders must be designed.

In the first place, it is important that more and more tailored in-depth diagnostics take place for decisions about (criminal) interventions for cyber offenders. Since there is great diversity among cyber offenders, a tailor-made approach is important, and, to that end, the criminogenic and

[44] This concerns people from the hacker world (for example, ethical hackers) who play an exemplary role and/or mentor role.

[45] For more information about this commission and the procedures see: https://www.nji.nl/nl/Databank/Databank-Effectieve-Jeugdinterventies/Deelcommissie-Justitiele-interventies.

protective characteristics and the way in which they influence the delinquent behavior in the online environment must be mapped out. The current instruments still appear insufficiently capable of measuring these specific cyber-offender-related characteristics. In addition to criminogenic needs, specific attention is also needed for responsiveness to interventions (learning styles and motivations) of cyber offenders who commit their offences in an online environment. For cyber offenders, it seems appropriate that specific supplements to existing diagnostic tools become available.

Secondly, interventions that combine awareness, mentalising (empathising with others), moral reasoning (in combination with ethical hacking) and offering opportunities offer great potential to be effective, especially for young technically skilled offenders. However, these interventions also appear to produce unwanted effects, because they can unintentionally inspire potential offenders to explore these crimes or increase the status of cyber offenders with their peers. It is therefore important to thoroughly investigate both the intended and unintended effects of these interventions and to describe clear target groups for whom the interventions are potentially effective.

Thirdly, it appeared that traditional interventions are potentially suitable for both younger and older perpetrators in different phases of the criminal career, but with motivations other than curiosity and seeking mental challenge. This concerns interventions that focus on specific criminogenic factors (such as addiction, lack of social skills or supportive relationships). However, these interventions do not yet take into account the responsiveness of cyber offenders in the online context, so that effectiveness for this target group is probably disappointing. Our final recommendation is therefore to find out what adjustments are needed in these existing interventions to reflect the responsiveness of cyber offenders.

Voorwoord

In dit rapport werpen we licht op de (unieke) kenmerken van cyberdaders en de mate waarin beschikbare interventies aansluiten bij deze kenmerken. Voor dit onderzoek zijn twee systematische literatuurstudies uitgevoerd. Daarnaast hebben wij experts geïnterviewd (individueel en in focusgroepen) en is zowel een expertmeeting als roundtable georganiseerd. Vrijwel alle partners uit de veiligheidsketen waren hierbij vertegenwoordigd (politie, OM, rechterlijke macht, Reclassering, Halt en Jeugdzorg) evenals experts van andere organisaties (advocatuur, universiteiten en het bedrijfsleven). Al deze experts willen wij hartelijk danken voor het delen van hun kennis en ervaringen. Ook zijn voor dit onderzoek daders geïnterviewd die betrokken zijn geweest bij een of meer vormen van cybercriminaliteit in enge zin. We willen ook hen hartelijk danken voor hun waardevolle bijdrage aan dit onderzoek en het feit dat zij tijd wilden vrijmaken om hun ervaringen en visies met ons te delen.

De auteurs, Wytske van der Wagen, Elina van ’t Zand, Sifra Matthijsse en Tamar Fischer zijn bij de totstandkoming van het onderzoek bijgestaan door de begeleidingscommissie onder voorzitterschap van Theo de Roos (UvT). We danken hem en de overige leden van de commissie: Ton Eijken (MinVenJ, DSJ), Marleen Weulen Kranenbarg (VU), Lars Heuts (WODC) en Casper van Nassau (WODC) voor de adviezen, het naar voren brengen van literatuur en contactpersonen en bovenal voor de opbouwende commentaren op eerdere versies van dit rapport. Sophie Keizer (EUR) en Nicole Alberts (UL) danken wij voor het snel en zeer nauwkeurig transcriberen (en deels voor de afname) van de expertinterviews, focusgroepen en daderinterviews.

Rotterdam, 23 december 2019, Wytske van der Wagen, Elina van’t Zand, Sifra Matthijsse en Tamar Fischer

Hoofdstuk 1 Inleiding

1.1. Achtergrond

"Van de zolderkamer naar de rechtszaal dankzij zelfgemaakte software. Hoe twee jongens uit Amersfoort met hun zelfgemaakte software meer dan duizend slachtoffers afpersten."[46]

"Van hack op school tot DDoS aanvallen op overheidsinstellingen. Jelle wist niet van ophouden… Het waren niet de Russen, geen grote criminelen, maar het was vermoedelijk de 18-jarige Jelle uit Oosterhout die meerdere sites zoals de Belastingdienst de afgelopen maanden plat legde. Maar waarom? Waarschijnlijk voor de kick. Jelle wilde dolgraag gezien worden door kenners en vond het maar wat grappig dat de buitenwereld dacht dat de Russen erachter zaten."[47]

"Tegen een 19-jarige Rotterdamse hacker is donderdag vierenhalve maand cel en TBS[48] *met voorwaarden geëist. Volgens het Openbaar Ministerie hackte de Rotterdammer 1948 computers. In totaal zou hij 42 miljoen privé-bestanden hebben verzameld. "Ik raakte gebiologeerd door de mogelijkheden. Ik ging steeds een stapje verder", aldus de hacker. Hij was gefixeerd op de technische mogelijkheden en niet bezig met de morele of ethische aspecten. Ook het financiële aspect interesseerde hem niet."*[49]

Berichten zoals bovenstaande lijken steeds vaker in de media te verschijnen. Hoewel de casussen in veel opzichten van elkaar verschillen, kennen ze vaak een soortgelijke verhaallijn: het begint kleinschalig op een zolderkamertje, maar de betrokken dader glijdt steeds verder af in de cybercriminaliteit. Er wordt ook vaak grote schade aangericht. Er zijn aanwijzingen dat er een sterke toename is in het aantal daders van cybercriminaliteit. Zo meldt het Openbaar Ministerie in mei 2018 dat het totaal aantal criminele hackers dat voorkomt in strafzaken in de afgelopen 10 jaar is verzesvoudigd naar rond de 60 in 2016. Systematische kennis over de ontwikkelingen in de aard en omvang van cybercriminaliteit is echter slechts beperkt beschikbaar. De meeste informatie die in de wetenschappelijke literatuur beschikbaar is, heeft betrekking op jongeren en is via zelfrapportages of registratiedata verkregen. Hierin is gevonden dat het aandeel jongeren dat volgens zelfrapportage een cyberdelict heeft gepleegd één derde betreft (Van der Laan, Beerthuizen & Weijters, 2016). Tegelijkertijd worden er geen aanwijzingen gevonden dat dit aantal momenteel groeit (Zebel, de Vries, Giebels, Kuttschreuter & Stol, 2013; Van der Laan & Goudriaan, 2016). Nederland kent geen zelfrapportage-onderzoek over daderschap onder volwassenen en bovendien is het met de huidige meetinstrumenten voor criminaliteitstrends (politiestatistieken en slachtofferenquêtes) zeer problematisch om valide uitspraken te doen over de ontwikkelingen in de omvang van (daderschap van) cybercriminaliteit (Smit, Ghauharali, Van der Veen, Willemsen, Steur, Te Velde, Van der Vorst & Bongers, 2018). Wel zijn er indicaties dat ook volwassenen betrokken zijn bij cybercriminaliteit, bijvoorbeeld waar de delicten gepleegd worden binnen de context van georganiseerde criminaliteit (Kruisbergen, Leukfeldt, Kleemans, Roks, Kouwenberg, Nabi, Fiorito &

[46] https://www.volkskrant.nl/nieuws-achtergrond/van-de-zolderkamer-naar-de-rechtszaal-dankzij-zelfgemaakte-software~b6f2c54c/?referer=https%3A%2F%2Fwww.google.com%2F
[47] http://www.omroepbrabant.nl/?news/274508962/Van+hack+op+school+tot+DDoS-aanvallen+op+overheidsinstellingen,+Jelle+(18)+wist+niet+van+ophouden.aspx
[48] De dader heeft uiteindelijk alleen een celstraf opgelegd gekregen.
[49] https://www.rijnmond.nl/nieuws/119169/TBS-geeist-tegen-Rotterdamse-hacker

Ruitenburg, 2018; Leukfeldt, Kleemans & Stol, 2017a, 2017b, 2017c; Odinot, Verhoeven, Pool & de Poot, 2017).

Ook over de kenmerken en criminele carrières van cyberdaders is nog maar beperkt informatie beschikbaar (Rokven, Weijters & Van der Laan, 2017; Weulen Kranenbarg, 2018). Zo zijn er wel aanwijzingen dat cybercriminele carrières gedreven worden door nieuwsgierigheid, technologische fascinatie en de kick, maar zijn er mogelijk ook carrières die anders verlopen. Ook lijkt cybercriminaliteit door een heterogene groep daders te worden gepleegd, onder andere wat betreft de leeftijd, motivatie, technische vaardigheden, het type delict en de onderliggende problematiek (Hoek van Dijke, 2016; Van der Wagen, Althoff & van Swaaningen, 2016; Weulen Kranenbarg, 2018). Bij het in kaart brengen van de kenmerken van daders van cybercriminaliteit zijn belangrijke vragen: hebben we te maken met een uniek type dader in vergelijking met daders van traditionele vormen van criminaliteit en zo ja, in welke opzichten? Welke verschillen bestaan er tussen cyberdaders onderling? Om hier een genuanceerd beeld van te krijgen is meer onderzoek nodig.

Kennis over de kenmerken van cyberdaders is van groot belang om te kunnen bepalen of bestaande interventies toegepast kunnen worden op cyberdaders en welke eigenschappen nieuw te ontwikkelen interventies moeten hebben om het gedrag van de cyberdaders te kunnen beïnvloeden (Weulen Kranenbarg, 2018; Rokven, Weijters & Van der Laan, 2017). Immers, als er sprake is van een uniek of andersoortig profiel, dan zouden andersoortige interventies mogelijk wenselijk zijn. Een toegespitste aanpak op cyberdaders staat op dit moment nog in de kinderschoenen, alhoewel er wel nieuwe ontwikkelingen zijn. Het meest geijkte voorbeeld van een interventie die specifiek voor cyberdaders is ontwikkeld, is de recent ontwikkelde Hack_Right interventie waarbij de strafrechtsketen, bedrijven en wetenschappers samenwerken om cyberdaders op het rechte pad te krijgen door onder meer een positief alternatief te bieden en daders te coachen.[50]

Onderhavig onderzoek tracht een bijdrage te leveren aan meer kennis over de toepasbaarheid van zowel traditionele als alternatieve interventies voor daders van cybercriminaliteit in enge zin. Cybercriminaliteit in enge zin omvat delicten waarbij ICT zowel het middel als het doelwit is (Leukfeldt, Veenstra, Domenie & Stol, 2012) zoals hacken, het uitvoeren van DDoS-aanvallen, botnets en ransomware (zie verder paragraaf 1.3). Het onderzoek is uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie en Veiligheid.

1.2. Probleemstelling en onderzoeksvragen

In dit onderzoek staat de volgende probleemstelling centraal: *"In hoeverre bestaan er verschillen qua profiel(en) van cyberdaders en daders van 'traditionele' criminaliteit, en in hoeverre en op welke wijze dienen (eventuele) verschillen gevolgen te hebben voor de aard van interventies voor cyberdaders?"*
Om deze probleemstelling te kunnen beantwoorden hebben wij een vijftal onderzoeksvragen geformuleerd.

1. Wat zijn de kenmerken van cyberdaders en in hoeverre zijn er verschillende profielen van cyberdaders te onderscheiden?
Om deze onderzoeksvraag te beantwoorden zijn aspecten van daderschap onderzocht die een belangrijke rol spelen in de literatuur over cybercriminaliteit. Hierbij is gekeken naar achtergrondkenmerken, drijfveren, de verschillende fasen van de criminele carrière (initiatie,

[50] Zie verder: https://magazines.openbaarministerie.nl/opportuun/2018/02/hackright

ontwikkeling/rijping en stoppen) en de percepties ten aanzien van de strafbaarheid, pakkans en schade. Gezamenlijk geven deze kenmerken een beeld van de (verschillende) aanwezige profielen van daders van cybercriminaliteit.

2. Welke interventies gericht op cyberdaders kunnen (in binnen- en buitenland) worden onderscheiden en in hoeverre sluiten zij qua aard voldoende aan bij de geschetste kenmerken/profielen van daders van cybercriminaliteit?
Voor het antwoord op deze onderzoeksvraag is gekeken naar interventies voor cyberdaders die vanuit de overheid of door private partijen reeds toegepast worden of in ontwikkeling zijn. Tevens is onderzocht in hoeverre ze aansluiten bij de geschetste kenmerken/profielen. Om dit te onderzoeken is gekeken naar de kenmerken van cyberdaders die naar verwachting van belang zijn voor de responsiviteit voor interventies voor gedragsverandering (motivatie, leerstijlen) en in hoeverre bestaande interventies daarop aansluiten.

3. In hoeverre verschillen de kenmerken/profielen van daders van cybercriminaliteit van die van traditionele daders?
Om deze onderzoeksvraag te beantwoorden is in kaart gebracht wat de verschillen en overeenkomsten zijn tussen de verschillende kenmerken van cyberdaders enerzijds en de kenmerken van traditionele daders anderzijds. Het antwoord op deze vraag is van belang om de wenselijkheid van specifieke interventies voor cyberdaders te kunnen bepalen.

4. In hoeverre sluiten bestaande interventies (in binnen-en buitenland) gericht op traditionele daders qua aard aan op de kenmerken van cyberdaders?
Om deze vraag te beantwoorden is naar interventies gekeken die op traditionele daders worden toegepast. Bij welke criminogene en protectieve factoren van daders van cybercriminaliteit sluiten bestaande interventies aan en bij welke niet? Op welke wijze sluiten de interventies aan bij de responsiviteit van de daders van cybercriminaliteit? Welke aanvullingen/aanpassingen van bestaande interventies lijken nodig te zijn voor welk type dader en waarom?

5. Welke aanbevelingen kunnen op basis van het onderzoek gedaan worden met betrekking tot de wijze waarop interventies voor cyberdaders vormgegeven moeten worden?
Op basis van het onderzoek geven wij een aantal concrete aanbevelingen en aanknopingspunten voor interventies voor cyberdaders.

Om de onderzoeksvragen te beantwoorden zijn twee systematische literatuurstudies uitgevoerd en zijn interviews en focusgroepen gehouden met experts en interviews afgenomen met daders van cybercriminaliteit in enge zin. Daarnaast is een expertmeeting en roundtable georganiseerd om de onderzoekbevindingen te valideren.

1.3. Afbakening

Cybercriminaliteit is een terrein dat zich zeer lastig laat afbakenen doordat definities door elkaar heenlopen alsook omdat het onderscheid tussen klassieke criminaliteit en het gebruik van geavanceerde ICT-technieken niet altijd scherp is (Van der Hulst & Neve, 2008). Dit onderzoek heeft

zich gericht op individuele daders[51] die in ieder geval[52] betrokken zijn (of zijn geweest) bij cybercriminaliteit in enge zin, delicten waarbij ICT zowel het middel als het doelwit is. Delicten waarbij ICT alleen als een nieuw middel wordt gebruikt om traditionele delicten te plegen zoals online stalking, grooming, eenvoudige oplichting via het internet of het downloaden van kinderpornografie (vormen van cybercriminaliteit in ruime zin) vallen buiten het bereik van dit onderzoek. Ook online piraterij nemen we in dit onderzoek niet mee.

In box 1 wordt een overzicht gegeven van de delicten die binnen het onderzoek vallen met een korte beschrijving. Een kanttekening hierbij is dat het rapport voornamelijk zal gaan over daders betrokken bij hacken, omdat zal blijken dat hier de meeste kennis over beschikbaar is.

Box 1 Vormen van cybercriminaliteit in enge zin

- **Hacken/ binnendringen in een geautomatiseerd werk**. Artikel 138ab Sr. (zie bijlage 4)
  "Computerinbraak of hacken is een verzamelterm voor het wederrechtelijk binnendringen in een computersysteem […] Ongerichte cyberaanvallen zijn geautomatiseerd en hebben geen specifiek bedrijf of computersysteem als doelwit. Bij ongerichte aanvallen wordt grootschalig getest op het bestaan van kwetsbaarheden om vervolgens het computersysteem trachten te misbruiken, bijvoorbeeld door het installeren van malware. Bij gerichte cyberaanvallen is een specifiek bedrijf of computersysteem het doelwit. De cyberaanval bestaat uit maatwerk om de kans van slagen en het risico op detectie te verkleinen. Voor gerichte cyberaanvallen is meestal meer kennis nodig en het vergt een langere voorbereidingstijd." (NCSC, 2012, p. 43)

- **Stoornis in de gang of werking van een (publiek) geautomatiseerd werk.** Artikel 138b Sr, Artikel 161sexies Sr, Artikel 161septies Sr (zie bijlage 4)
  "Deze bepaling richt zich in het bijzonder op het strafbaar stellen van zogenoemde DDoS-aanvallen (distributed denial of service) en bijvoorbeeld e-mail bombing […] De computersystemen die de DDoS-aanval uitvoeren zijn vaak misbruikte systemen van onschuldige slachtoffers in een botnet. De botnet herder geeft aan de geïnfecteerde systemen (bots) de opdracht om een bepaald doelwit aan te vallen." (NCSC, 2012, p. 22-24, p.68)

- **Onbruikbaar maken, veranderen of aantasten van gegevens**. Artikel 350a en 350b Sr (zie bijlage 4)
  "Deze artikelen beschermen het ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens […] Voor dit artikel is specifiek gericht op computervirussen en andere vormen van malware. Voor strafbaarheid is het voldoende dat iemand de malware ter beschikking stelt of verspreidt, ongeacht of de malware ook daadwerkelijk schade aanricht" (NCSC, 2012, p. 25)

- **Afluisteren**. Artikel 139c Sr, Artikel 139d Sr, Artikel 139e Sr (zie bijlage 4)
  "Het aftappen en/of opnemen van gegevens door een geautomatiseerd werk of telecommunicatienetwerk is strafbaar gesteld in artikel 139c Sr […] Het plaatsen van opname-, aftap- c.q. afluisterapparatuur is strafbaar gesteld in artikel 139d Sr […]Het voorhanden hebben en gebruiken van gegevens die door onrechtmatig afluisteren, aftappen en/of opnemen zijn verkregen is strafbaar gesteld in artikel 139e Sr" (NCSC, 2012, p. 26)

Aan de keuze om vooral op de meer technische delicten te focussen, liggen drie redenen ten grondslag. Ten eerste is uit eerder onderzoek (o.a. Rokven, Weijters & Van der Laan, 2017) gebleken dat juist daders van cybercriminaliteit in enge zin een uniek profiel lijken te hebben. Onderhavig onderzoek kan door middel van kwalitatieve onderzoeksmethoden nader licht werpen op deze dadergroep en een genuanceerd beeld schetsen van eventuele verschillen in kenmerken binnen deze dadergroep. Ten tweede hebben we ervoor gekozen om op deze groep te focussen ten behoeve van de haalbaarheid en kwaliteit van het onderzoek. Als daders van cybercriminaliteit in ruime zin ook in

[51] Statelijke actoren als dader zijn dus niet meegenomen in dit onderzoek.
[52] Dit betekent dat we ook daders hebben meegenomen in het onderzoek die zowel bij cybercriminaliteit in enge zin als bij andere vormen van criminaliteit betrokken zijn (geweest).

het onderzoek zouden worden betrokken, zou het onderzoek mogelijk een te exploratief karakter kunnen krijgen. Ten derde zijn interventies voor cybercriminaliteit in ruime zin recentelijk reeds in kaart gebracht (zie Oosterwijk & Fischer, 2017). Om deze redenen is er voor gekozen om het onderzoek voornamelijk te richten op daders van cybercriminaliteit in enge zin en passende interventies voor deze groep, zowel als het gaat om jeugdige als volwassen daders. We spreken in deze context over 'voornamelijk' omdat, zoals ook zal blijken uit dit onderzoek, de grens tussen cybercriminaliteit in enge zin en ruime zin niet altijd scherp is.

Hoewel daders die betrokken zijn bij delicten zoals online stalking en grooming niet meegenomen zijn in dit onderzoek, wordt er wel aandacht besteed aan deze daders indien er sprake is van computervredebreuk om dit te bewerkstellingen. Gedacht kan worden aan situaties waarbij een dader andermans account hackt (computervredebreuk) met als doel om iemand te chanteren of om seksueel getinte afbeeldingen te verspreiden. Ook is er voor gekozen om daders van phishing mee te nemen in dit onderzoek. Hoewel phishing gezien kan worden als een vorm van fraude (ruime zin), worden de gegevens die middels phishing worden verkregen doorgaans ook weer gebruikt om te hacken (enge zin).

Als het gaat om interventies focust het onderzoek zich op interventies gericht op (potentiële) daders. Daarbij komen ook generale preventieve interventies, gericht op het voorkomen van daderschap onder het algemene publiek, aan bod, maar de focus zal sterker liggen op interventies die gericht zijn op het terugdringen van recidive bij opgepakte daders en dus op de beëindiging van de criminele carrière. Interventies die zich uitsluitend op doelbescherming richten (zoals firewalls, antivirusprogramma's en bewustwordingscampagnes voor potentiële slachtoffers) worden niet meegenomen in dit onderzoek. Zulke doelgerichte interventies vragen om een geheel andere benadering als het om de evaluatie van de (potentiële) effectiviteit gaat, die wellicht minder samenhangt met kenmerken van de individuele daders en meer met het gedrag van (potentiële) slachtoffers.

1.4. Toepassing daderprofilering in het huidige onderzoek

Zoals gaandeweg dit rapport duidelijk zal worden, gaat het bij cybercriminaliteit in enge zin om allesbehalve een homogene groep daders. Er is sprake van combinaties van eigenschappen zoals vaardigheden (o.a. technische kennis bezitten) en specifieke motivaties (zoals uitdaging zoeken of status verwerven) die in mindere of meerdere mate bij daders aanwezig zijn en gezamenlijk tot (een bepaalde ontwikkeling in) het delictgedrag leiden. Over tijd kunnen deze factoren en hun samenhang met het delictgedrag bovendien veranderen. Daarom zullen we geen vaste dadertypologieën construeren, maar benaderen we in dit onderzoek de profilering van cyberdaders door het beschrijven van de impact van verschillende factoren op het delictgedrag, zowel individueel als in hun onderlinge samenhang. Vervolgens wordt nagegaan wat de implicaties zijn van de aanwezigheid van deze factoren voor delictgedrag voor de verwachtingen over effectieve interventies.

1.5. Theoretische oriëntatie

Daderkenmerken

Voor het onderzoek naar daderkenmerken is gebruik gemaakt van inzichten uit bestaande criminologische literatuur en theorieën over daderschap en criminele carrières (zie voor een overzicht van de gebruikte concepten box 2, ingedeeld in vier domeinen).

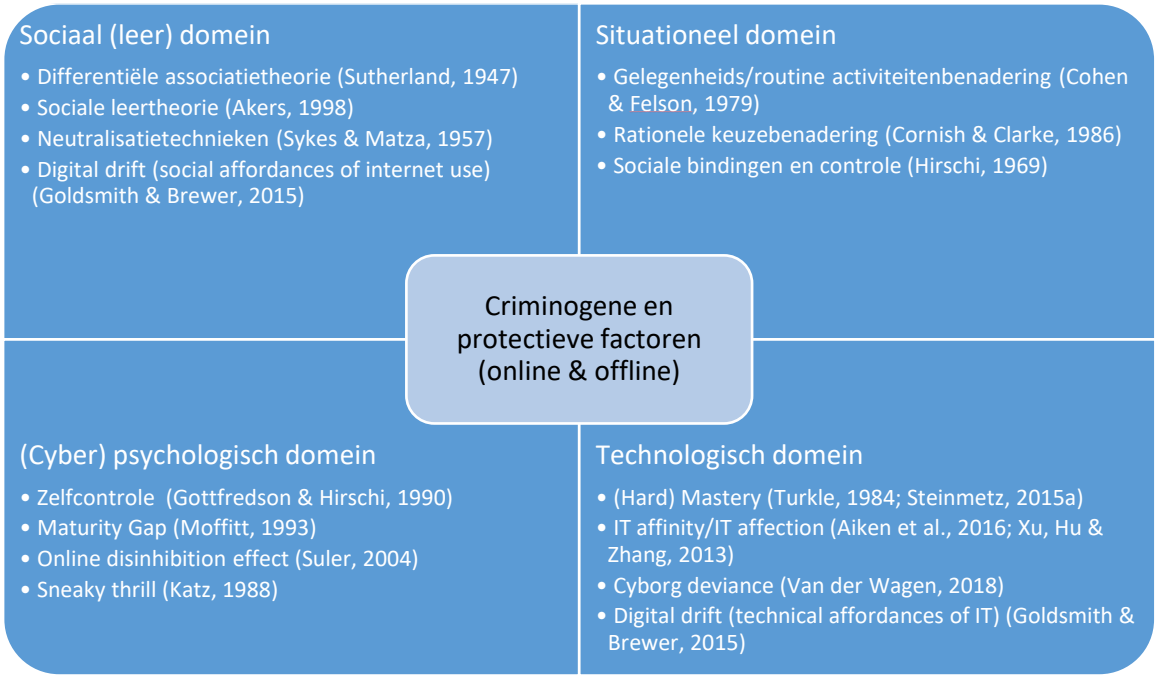
In de eerste plaats betreffen dit leertheorieën zoals de sociale leertheorie (Akers, 1998) en de differentiële associatietheorie (Sutherland, 1947). Dit betreffen theorieën die veronderstellen dat deviant en crimineel gedrag aangeleerd wordt in groepsverband. Dergelijke theorieën lijken ook relevant te zijn in het online domein, omdat daar veel sociale interactie plaatsvindt tussen daders (o.a. Hutchings, 2016; Goldsmith & Brewer, 2015). Ook wordt gekeken naar de rol van neutralisatietechnieken, legitimeringen die daders tijdens of na het plegen van delicten gebruiken (Sykes & Matza, 1957). Inzichten hierin zijn van belang om leerprocessen, attitudes, drijfveren en betekenisgeving van daders te duiden, zo ook van cyberdaders (Miller & Morris, 2014).

In de tweede plaats is gebruik gemaakt van situationele theorieën zoals de gelegenheidsbenadering (Cohen & Felson, 1979) die gericht zijn op rationele keuzes (kosten-batenafwegingen van daders) en de rol van sociale controle. Deze vorm van controle reduceert de gelegenheid voor het plegen van criminaliteit en kan ook weer een rol spelen bij het stoppen met criminaliteit (*desistance*).

Ten derde is gebruik gemaakt van concepten die geschaard kunnen worden in het (cyber)psychologische domein. Voor jeugdige daders is onder meer gebruik gemaakt van Moffitt's (1993) inzichten over criminaliteit bij jongeren en jongvolwassen en de rol van de *maturity gap* (discrepantie tussen biologische en sociale volwassenheid) hierbij. Een ander meer klassiek criminologisch concept waar naar gekeken is, is zelfcontrole (Gottfredson & Hirschi, 1990), waarbij verondersteld wordt dat mensen met een lage zelfcontrole sneller verleid worden om criminaliteit te plegen. Het concept *sneaky thrill* van Katz (1988) gaat voornamelijk over de verleidingen (attracties) van het plegen van criminaliteit zelf en kan onder andere licht werpen op de beleving van het plegen van delicten. Daar we te maken hebben met delicten die online gepleegd worden lijkt het *online disinhibition effect*, een door Suler (2004) geïntroduceerd concept, ook erg relevant te zijn. Dit concept beschrijft dat de anonieme online omgeving remmingen wegneemt, waardoor mensen zich anders gaan gedragen. In veel studies wordt dit als een zeer bruikbare en relevante verklaring gezien in het kader van daderschap van cybercriminaliteit, zowel voor cybercriminaliteit in ruime als enge zin (o.a. Zebel et al., 2013).

Aangezien er doorgaans sprake is van (zeer) technische delicten, is eveneens gebruik gemaakt van concepten – voor zover die er zijn – die zich meer op het technologische domein van daderschap richten. Onder de technische context valt ook het concept *digital drift* (Goldsmith & Brewer, 2015), dat inzicht geeft in de manier waarop computers en het internet zowel technische als sociale *affordances* hebben die bepaalde vormen van delinquentie kunnen intensiveren of daar nieuwe mogelijkheden voor bieden. Andere aspecten die daar van belang kunnen zijn, zijn het *cyborg deviance* concept (Van der Wagen, 2018), *mastery* (Turkle 1984; Steinmetz, 2015a) en *IT affinity* (Aiken, Davidson & Amann, 2016; Xu, Hu & Xhang, 2013). Deze concepten kunnen licht werpen op hoe en waarom daders met technologie interacteren en hoe zij daar betekenis aan geven.

Box 2 Overzicht gebruikte concepten



De aannames van en inzichten uit de verschillende theorieën worden in de hoofdstukken waarin de specifieke kenmerken van cyberdaders en hun delictgedrag aan bod komen (hoofdstuk 3 tot en met 6) nader uitgewerkt en geïntegreerd met de bevindingen.

Effectieve interventies

Voor het onderzoek naar passende interventies is gebruik gemaakt van een drietal hoofdbenaderingen. Ten eerste zijn inzichten aangewend uit traditionele benaderingen gericht op generale en speciale afschrikking, die zich onder meer baseren op inzichten uit de rationele keuzetheorie (Cornish & Clarke, 1986) en de situationele criminaliteitspreventie (Cohen & Felson, 1979). Deze theorieën gaan er vanuit dat daders een kosten-batenafweging maken als het om het plegen van criminaliteit gaat. Door het verhogen van de pakkans en de strafdreiging (en vooral de perceptie hiervan) worden de kosten verhoogd en zouden daders ervan weerhouden kunnen worden om (opnieuw) criminaliteit te plegen.

Ten tweede is een beroep gedaan op de *What Works* literatuur (Andrews, et al., 1990), een benadering die veronderstelt dat een exclusieve focus op afschrikking niet werkt. In plaats daarvan stellen zij resocialisatie meer centraal. Op basis van het in de *What Works* benadering ontwikkelde RNR-model worden specifieke kenmerken aangewezen die van belang zijn voor de effectiviteit van interventies. Dit model gaat uit van drie beginselen die nodig zijn om houding- en gedragsverandering tot stand te brengen, namelijk: 1) het risico (*Risk*)-beginsel (sluit de intensiteit van de interventie aan bij het risicoprofiel), 2) het criminogene behoeften (*Needs*)-beginsel (speelt de interventie voldoende in op de criminogene factoren die een rol spelen bij het delictgedrag) en 3) het responsiviteit (*Responsivity*)-beginsel (wordt er rekening gehouden met de motivatie voor verandering) (o.a. Lipsey

& Cullen, 2007; Lowenkamp, Latessa & Holsinger, 2006). In dit onderzoek zal vooral aandacht zijn voor de laatste twee beginselen.

Als aanvulling op de *What Works* benadering is in dit onderzoek gebruik gemaakt van inzichten uit de *desistance* literatuur. Deze benadering laat zich kritisch uit over de 'behandelretoriek' van de *What Works* benadering. Volgens de *desistance* benadering moet de nadruk niet zozeer liggen op risico's en het 'behandelen' van criminogene factoren, maar moet er meer aandacht zijn voor het dynamische karakter van *desistance*. Het beëindigen van een criminele carrière moet worden gezien als een proces van vallen en opstaan. Naast het stoppen met het plegen van criminaliteit (*primaire desistance*) is het van belang dat de dader een identiteitstransformatie ondergaat waarbij hij of zij zichzelf niet meer als 'dader' ziet (*secundaire desistance*) (o.a. Maruna & Farrall, 2004; Maruna & Toch, 2005).

In dit onderzoek gaan we er vanuit dat alle drie benaderingen, afschrikking, *What Works* en *desistance*, waardevolle inzichten kunnen bieden in de vraag wat mogelijk effectieve interventies[53] kunnen zijn voor daders van cybercriminaliteit in enge zin in het licht van de problematiek en responsiviteit. Ook is het belangrijk om aan te geven dat interventies elementen van verschillende benaderingen kunnen hebben. In hoofdstuk 7 en 8 komen de benaderingen en de interventies die onder deze benaderingen geschaard kunnen worden uitgebreider aan bod.

1.6. Leeswijzer

Dit rapport is opgebouwd uit negen hoofdstukken. Na het voorliggende inleidende hoofdstuk waarin de achtergrond, context en onderzoeksvragen uiteengezet zijn, volgt een methodologisch hoofdstuk waarin de drie methoden besproken worden die in het onderzoek gebruikt zijn om de onderzoeksvragen te beantwoorden. Vervolgens worden de bevindingen uiteengezet, waarbij per kenmerk of cluster van kenmerken de bevindingen uit de literatuur, expertinterviews en daderinterviews integraal worden besproken. De bevindingen zijn opgesplitst in twee delen.

Deel 1 beslaat vier hoofdstukken die ingaan op kenmerken van cyberdaders en in hoeverre en op welke wijze deze afwijken van traditionele daders. Hoofdstuk 3 gaat in op de achtergrondkenmerken, namelijk demografische kenmerken, sociaal economische kenmerken, vrije tijd, gezinsgerelateerde kenmerken, psychologische kenmerken en sociale kenmerken (online en offline). Hoofdstuk 4 gaat in op de drijfveren en beleving van cyberdaders. In hoofdstuk 5 wordt stilgestaan bij de percepties van daders ten aanzien van de strafbaarheid, de pakkans en de schade van de (door hen gepleegde) cyberdelicten. In hoofdstuk 6 wordt ingegaan op factoren die van invloed zijn op het verloop van de criminele carrière, waarbij het gaat om zowel de initiatie, de ontwikkeling en het stoppen.

Deel 2 van het rapport omvat twee hoofdstukken die, op basis van de bevindingen uit deel 1 en inzichten uit de literatuur over effectieve interventies, ingaan op de vraag wat mogelijk effectieve en passende interventies zijn voor cyberdaders. In hoofdstuk 7 wordt ingegaan op de effectiviteit van reactieve en preventieve interventies die aansluiten op de theorie van afschrikking en op inzichten uit de situationele criminaliteitspreventie. In hoofdstuk 8 wordt, in aansluiting op het gedachtegoed van *What Works* en de *desistance* benadering, ingegaan op de mogelijke effectiviteit van zowel *risk-based* als *strength-based* interventies. In hoofdstuk 9 worden ter afsluiting de belangrijkste conclusies en aanbevelingen gepresenteerd.

[53] We hanteren in het rapport een vrij ruime definitie van het begrip interventie. Alternatieven zoals hackwedstrijden noemen we in dit rapport een 'interventie' omdat ze ingezet kunnen worden om gedragsbeïnvloeding te bewerkstelligen.

Hoofdstuk 2 Methodologische verantwoording

De onderzoeksvragen zijn beantwoord met behulp van een systematische literatuurstudie, expertinterviews, focusgroepen en daderinterviews. De thema's uit de onderzoeksvragen zijn zo vanuit verschillende invalshoeken belicht en de visies van verschillende actoren zijn met elkaar en met de uitkomsten uit de literatuurstudie vergeleken. In dit hoofdstuk wordt beschreven hoe we deze methoden hebben uitgevoerd. In paragraaf 2.1 wordt ingegaan op hoe de systematische literatuurstudie is uitgevoerd. In paragraaf 2.2 wordt stilgestaan bij de expertinterviews, focusgroepen en expert meeting. Vervolgens wordt in paragraaf 2.3 stilgestaan bij de daderinterviews. Paragraaf 2.4 en paragraaf 2.5 zullen respectievelijk ingaan op de analyse van de data en de waarborging van privacy.

2.1. Systematische literatuurstudie

Voor dit onderzoek zijn twee losstaande literatuurstudies uitgevoerd die respectievelijk betrekking hebben op de onderzoekvragen naar de kenmerken en het delictgedrag van cyberdaders en naar interventies voor cyberdaders.

2.1.1. Literatuurverzameling rondom kenmerken en delictgedrag van cyberdaders (onderzoeksvragen 1 & 3)

De eerste systematische literatuurstudie is gericht op de onderzoeksvragen over de kenmerken van cyberdaders (onderzoeksvraag 1 en 3). Hierbij is gezocht naar zowel Nederlandse als internationale literatuur. In de eerste plaats zijn de internationale databases Scopus, Web of Science, PsychInfo, EBSCOHost en Sociological Abstracts geraadpleegd. Via de zoekmachine SSRN is gezocht naar grijze literatuur. Aanvullend is voor de Nederlandstalige literatuur de website van het WODC en Boom Juridische Tijdschriften geraadpleegd. Onder laatstgenoemde vallen onder andere het Tijdschrift voor Criminologie, het Tijdschrift voor Cultuur en Criminaliteit en het Tijdschrift voor Veiligheid. Tot slot is gebruik gemaakt van de drie voornaamste juridische zoekmachines, namelijk: Legal Intelligence, Rechtsorde en Kluwer. Om tot een complete selectie te komen is een uitgebreide verzameling zoektermen over cybercriminaliteit gebruikt. Een uitgebreide beschrijving van het proces waarin de zoektermen zijn vastgesteld, is te vinden in bijlage 1A. Hetzelfde proces is vervolgens toegepast om voor elk van de deelthema's in de onderzoeksvragen (persoonskenmerken, onderliggende problematiek en criminogene en protectieve factoren, de criminele carrière, drijfveren, neutralisaties en het verschil met traditionele daders) verzamelingen zoektermen te ontwikkelen. De algemene cyber-zoekreeks is gecombineerd aan de hand van Booleaanse operatoren met elk van de zoekreeksen voor de deelthema's om zo de literatuur in de databases te verzamelen (zie bijlage 1A).

Uit de internationale wetenschappelijke databases zijn 1529 unieke bronnen naar voren gekomen. Deze bronnen zijn beoordeeld op basis van de titel en abstract, waarbij er onder andere gekeken is naar het soort bron, in hoeverre er sprake is van cybercriminaliteit in enge zin en de relevantie voor de onderzoeksvragen. Daarbij zijn boekrecensies en nieuwsberichten over cybercriminaliteit buiten beschouwing gelaten, maar zijn masterscripties wel meegenomen. Studies over cybercriminaliteit in ruime zin buiten beschouwing gelaten, omdat de focus van het onderzoek op cybercriminaliteit in enge zin ligt. Studies over delicten als piraterij en phishing, die zowel onder cybercriminaliteit in enge als ruime zin kunnen vallen, zijn bij de *full text* beoordeling buiten

beschouwing gelaten indien er in de literatuur geen *hightech* component aan de delicten in kwestie verbonden was.

Deze afbakening heeft geresulteerd in een selectie van 159 publicaties uit de internationale wetenschappelijke databases. Uit de database SSRN zijn 29 unieke bronnen voortgekomen. Uit de Nederlandse en juridische databases zijn 16 unieke bronnen voortgekomen. In totaal kwam daarmee het aantal bronnen in de tussentijdse selectie uit op 204. Deze bronnen zijn vervolgens volledig gelezen en door twee onderzoekers beoordeeld op in- en exclusiecriteria die door de onderzoekers gezamenlijk, in overleg met de begeleidingscommissie, zijn samengesteld. Hierbij zijn exclusiecriteria gehanteerd zoals de beschikbaarheid en relevantie van de bron (zie bijlage 1B). Dit heeft uiteindelijk tot een selectie van 68 bronnen geleid. Tot slot zijn van de 68 overgebleven bronnen de literatuurlijsten handmatig doorzocht op aanvullende literatuur. Dit proces van *handsearching* heeft 31 aanvullende bronnen opgeleverd.

De uiteindelijke selectie van de systematische literatuurstudie bestaat uit 99 bronnen. Het betreffen zowel kwalitatieve als kwantitatieve, empirische als theoretische studies, geschreven in de Nederlandse of Engelse taal. Het selectieproces is weergegeven in tabel 2.1 en in een *flowchart* in bijlage 1C. De resultaten uit het literatuuronderzoek komen in hoofdstuk 3-8 aan bod.

Tabel 2.1 Overzicht van geselecteerde bronnen

Soort database	Aantal gevonden bronnen	Aantal bronnen beoordeeld op inhoud	Geïncludeerde bronnen
Wetenschappelijke databases	1529	159	51
SSRN	29	29	8
Nederlandse en juridische databases	16	16	9
Totaal	1574	204	68

2.1.2. Literatuuronderzoek rondom interventies voor cyberdaders (onderzoeksvragen 2 & 4)

Om de onderzoeksvragen over interventies (onderzoeksvraag 2 en 4) te beantwoorden, is tevens literatuuronderzoek verricht. In 2017 is een WODC onderzoeksrapport verschenen over interventies bij jeugdige daders van cybercriminaliteit (ruime en enge zin) (Oosterwijk & Fischer, 2017) waarbij een systematisch literatuurstudie naar deze interventies is uitgevoerd. In het huidige onderzoek is bekeken wat daar na twee jaar tijd aan toe te voegen is en is het overzicht uitgebreid met interventies voor volwassen daders. De systematische literatuurstudie voor dit onderzoek heeft zich op een aantal specifieke aspecten gericht. Ten eerste heeft het onderzoek zich toegespitst op interventies voor cybercriminaliteit in enge zin Ten tweede lag het accent in het onderzoek op specifieke interventies voor reeds opgepakte daders (recidivebeperking) en in mindere mate op generale interventies. Ten derde is gekeken naar interventies in alle fasen van (door)ontwikkeling, dus niet alleen naar reeds geëvalueerde en al dan niet effectief gebleken interventies. Uit eerder onderzoek is namelijk gebleken dat het aantal geëvalueerde interventies gericht op recidivebeperking bij daders zeer beperkt is (Oosterwijk & Fischer, 2017).

Er is gezocht in de eerdergenoemde databases. De eerdergenoemde zoektermenreeks over cybercriminaliteit is hierbij gecombineerd aan de hand van Booleaanse operatoren met een zoekreeks bestaande uit termen met betrekking tot interventies (zie bijlage 1A). Hiernaast is voor informatie over interventies in Nederland gezocht in wet- en regelgeving en andere overheidsinformatie zoals Kamerstukken en beleidsdocumenten. Dit heeft 15 bronnen opgeleverd. Tot slot zijn bij de gevonden

bronnen de literatuurlijsten en verwijzingen handmatig doorzocht op aanvullende literatuur. Dit proces van *handsearching* heeft 10 aanvullende bronnen opgeleverd.

2.2. Expertinterviews, focusgroepen en expertmeeting

Voor dit onderzoek zijn verschillende experts geïnterviewd die vanwege hun functie in contact staan en ervaring hebben met jeugdige en/of volwassen daders van cybercriminaliteit in enge zin. Tevens zijn experts geïnterviewd die interventies ontwikkelen of toepassen (specifiek voor deze doelgroep). In totaal is er met 52 experts gesproken (zie tabel 2.2) in 29 interviews, 2 focusgroepen, 1 expertmeeting en 1 roundtable sessie (zie tabel 2.3). De respons was over het algemeen heel goed. We hadden alleen moeite om politie-experts uit de regionale cybercriminaliteit teams bereid te vinden voor een interview. Dit had vermoedelijk vooral met overvolle agenda's te maken.

2.2.1. Expertinterviews

De expertinterviews betroffen semigestructureerde interviews. Tijdens de interviews zijn de experts allereerst gevraagd naar hun concrete ervaringen met de doelgroep zodat vastgesteld kon worden waar hun kennis, aannames en percepties op waren gebaseerd. Het volgende deel bestond uit vragen met betrekking tot cyberdaders en hun kenmerken. Er is zoveel mogelijk doorgevraagd naar concrete casussen waar de expert mee te maken heeft gehad. Dit geldt zowel voor experts die slechts met enkele daders te maken hebben gehad als voor experts die met tientallen daders in aanraking zijn gekomen (bijvoorbeeld medewerkers van Team High Tech Crime (THTC)). De laatste groep kon daarnaast ook in een meer algemene zin ingaan op kenmerken van cyberdaders, meer specifiek over aspecten die ze in mindere of meerdere mate zijn tegen gekomen.

De meeste experts bleken niet over een homogene groep daders te spreken, maar onderscheid te maken tussen verschillende subgroepen. Tijdens het interview is dan ook steeds aan de hand van de subgroepen die de experts zelf definieerden, ingegaan op de (onderscheidende) kenmerken. In het laatste deel van het interview zijn vragen gesteld over passende interventies en is gesproken over de eventuele ervaring met de toepassing van interventies op deze dadergroep (zie bijlage 2 voor het volledige interviewprotocol).

De interviews duurden tussen drie kwartier en ruim drie uur (gemiddeld anderhalf uur).[54] Alle interviews zijn met een digitale voice-recorder opgenomen.

[54] De interviews zijn allemaal afgenomen door de hoofdonderzoekers, meestal vergezeld door een junior onderzoeker of stagiair die aantekeningen maakte. 26 interviews en twee focusgroepen zijn face to face afgenomen (meestal op de werkplek van de experts) en drie interviews zijn telefonisch afgenomen.

Tabel 2.2 Overzicht van experts

Organisatie/branche	Aantal experts	Schatting aantal casussen in totaal	Cybercriminaliteit in enge of ruime zin	Leeftijdsgroep daders	Vorm gesprek
OM	4	50	Enge en ruime zin	Jeugd en volwassenen	Interviews, Focus groep
Politie (incl. Team High tech crime)	13	> 100	Beiden	Jeugd en volwassen	Interviews, Focus groep, expert meeting, Roundtable
Reclassering	7	Tientallen	Enge zin	Volwassenen	Interviews, Focus groep, expert meeting
Halt	6	39	Enge zin	Jeugd	Interviews, Focus groep, expert meeting
Advocatuur	3	50	Enge zin	Volwassenen	Interviews
Raad voor de Kinderbescherming & Jeugdzorg	3	Enkele	Enge zin	Jeugd	Interviews
Geestelijke gezondheidszorg	1	x[55]	Enge en ruime zin	Jeugd en volwassenen	Roundtable
Wetenschappelijk onderzoek	5	>100	Enge en ruime zin	Jeugd en volwassenen	Interviews, Roundtable
Computer- en cybersecurity	7	Tientallen	Enge zin	Jeugd en volwassenen[56]	Interviews
Trainingscentrum voor jeugdhulp, (speciaal) onderwijs en maatschappelijke opvang	1	x[55]	Enge en ruime zin	Jeugd	Roundtable
Non-profit cyberorganisatie	1	Enkele	x[57]	Jeugd en volwassenen	Interview
Journalist/schrijver	1	x[55]	Enge en ruime zin	Jeugd en volwassenen	Interview
Totaal	52				

Tabel 2.3 Overzicht van bijeenkomsten

Bijeenkomst	Aantal deelnemers	Deelnemers	Doel
Focusgroep	5	Reclassering toezichthouders en adviseur, leden cybercriminaliteit werkgroep	Bespreken casuïstiek
Focusgroep	7	Halt, OM, politie	Bespreken casuïstiek
Expertmeeting	10	Diverse organisaties (o.a. politie, Halt, Reclassering)	Validering en nuancering van voorlopige onderzoeksresultaten
Roundtable	6	Wetenschap en praktijk	Discussiëren over passende interventies cyberdaders

[55] In het betreffende interview of de betreffende roundtable is niet expliciet naar voren gekomen op hoeveel casussen de betreffende respondent zijn kennis en ervaring baseert.
[56] Dit betreffen Nederlandse en internationale actoren.
[57] Deze organisatie is vooral gericht op individuen met IT-talent en niet noodzakelijk op individuen die cybercriminaliteit hebben gepleegd. De nadruk ligt binnen deze organisatie dan ook op ethisch hacken.

2.2.2. Focusgroepen

Naast de expertinterviews zijn er twee focusgroepen georganiseerd. We hebben hiervoor gekozen omdat de medewerkers van de reclassering (allen betrokken bij de landelijke werkgroep Cyber van de reclassering[58]) aangaven slechts één, twee of drie cyberdaders onder toezicht te hebben (gehad). Tijdens de focusgroep is aan de hand van casussen gesproken over de kenmerken van (hun) cyberdaders, passende interventies voor (de desbetreffende) cyberdaders. Daarbij is vrij uitvoerig gesproken over de reclasseringscliënt(en) aan de hand van de topics uit het interviewprotocol. Ook is met hen gesproken over passende interventies. Een soortgelijke focusgroep is georganiseerd met drie medewerkers van Halt en drie (andere) betrokkenen bij het programma Hack_Right, namelijk een politiemedewerker, een medewerker van het OM en een stagiair van de Vrije Universiteit. Halt heeft in de periode 2014 tot 2019 39 zaken behandeld waarin het gaat om jeugdigen die een cyberdelict in enge zin hebben gepleegd. Een deel van deze jeugdigen is met het programma Hack_Right gestart. Tijdens de focusgroep is allereerst ingezoomd op enkele van deze casussen[59] en aan de hand van deze casussen is ook gesproken over passende interventies.

2.2.3. Expertmeeting en roundtable

De expertmeeting is georganiseerd om de bevindingen van de systematische literatuurstudie en de dader- en expertinterviews aan te vullen en nader te duiden. Hiervoor zijn mensen uitgenodigd die reeds geparticipeerd hadden in een interview alsook enkele andere experts die nog niet hadden meegewerkt, waaronder een ethische hacker. De expertmeeting had als doel om de eerdere bevindingen te verdiepen, aan te scherpen en te valideren. Voorafgaand aan de expertmeeting zijn een vijftal discussiepunten aan de experts gecommuniceerd (zie bijlage 3A). Op basis hiervan konden opvallende bevindingen, tegenstrijdigheden, verschillen en ook terugkerende punten uit de data besproken en nader geduid worden.

Naast de expertmeeting is een roundtable georganiseerd op het congres van de Nederlandse Vereniging voor Criminologie (21 juni 2019) met als doel om, op basis van een drietal vragen (zie bijlage 3B), input te krijgen over passende interventies voor daders van cybercriminaliteit. Daartoe waren specifiek experts uitgenodigd die werkzaam zijn op het gebied van de toepassing van bestaande interventies, zowel voor traditionele daders als cyberdaders. Op die manier konden ook de inzichten gebruikt worden die bestaan onder professionals met uitgebreide ervaring en kennis uit de praktijk van interventies voor traditionele daders. De deelnemers zijn werkzaam in de wetenschap, in de geestelijke gezondheidszorg, bij de politie en bij een trainingscentrum voor jeugdhulp, (speciaal) onderwijs en maatschappelijke opvang.

2.2.4. Mogelijkheden en beperkingen

De brede selectie van experts en de opzet van de interviews heeft een gevarieerde input opgeleverd over daders en interventies van cybercriminaliteit in enge zin. Het is echter belangrijk te benadrukken dat de geïnterviewde experts voornamelijk zicht hebben op cyberdaders die in beeld zijn bij politie en justitie. Over de grote groep daders waarvan de delicten niet zichtbaar zijn of die niet opgespoord zijn, bevat dit onderzoek daarom weinig informatie.

[58] Bij de reclassering is men op dit moment bezig om de kennis over cyberdaders te vergroten door o.a. casuïstiek met elkaar uit te wisselen. De werkgroep Cyber bestaat uit verschillende toezichthouders in het land die hier een bijdrage aan willen leveren.

[59] Met het oog op privacy zijn deze zaken op geanonimiseerde wijze (dus niet naam en toenaam) besproken

Verder bleken sommige experts nog maar beperkt met cyberdaders in aanraking gekomen te zijn in hun werk, of voornamelijk met een bepaald type dader (bijvoorbeeld alleen volwassenen, alleen jeugdigen, of alleen daders die relatief ernstige delicten hebben gepleegd). Dit heeft ertoe geleid dat soms kennelijk zeer relevante inzichten slechts vermeld zijn door een enkele respondent. Een ander risico dat aanwezig is, is dat door de beperkte persoonlijke ervaring die bepaalde experts hadden, zij meer algemene kennis in de interviews naar voren hebben gebracht in plaats van eigen ervaringen en inzichten. Daarmee kunnen bestaande maar niet-empirisch onderbouwde aannames gekopieerd en versterkt worden. Ook is niet bij alle uitspraken helemaal zeker of experts het wel over cybercriminaliteit in enge zin hebben. Door specifiek naar voorbeelden te vragen en in de interviews specifieke casussen te bespreken is geprobeerd om deze bias zo veel mogelijk te beperken, maar er dient rekening mee te worden gehouden dat deze desalniettemin nog aanwezig is.

2.3. Daderinterviews

Er is voor gekozen om tevens daderinterviews af te nemen. Daderinterviews kunnen in de eerste plaats helpen bij het beantwoorden van de onderzoeksvragen doordat achterhaald kan worden hoe daders zelf aankijken tegen hun betrokkenheid bij cybercriminaliteit. Daarbij kunnen verdiepende inzichten verworven worden over hun achtergrond, thuissituatie, zelfbeeld, drijfveren, criminele carrière, modus operandi, attitudes en morele percepties. Zoals Rokven, Weijters en Van der Laan (2017, p.3) in het kader van hun onderzoek naar (jonge) cyberdaders ook stellen: “Er is meer inzicht nodig over wie deze jongeren nu eigenlijk zijn.” In de tweede plaats is het perspectief van de dader zelf ook relevant in het kader van de ontwikkeling van interventies. Passende interventies moeten zoals duidelijk wordt in de *What Works* literatuur (Andrews et al., 1990) aansluiten bij de leerstijlen en mogelijkheden van de cliënten (responsiviteitsprincipe). Bij het ontwikkelen van wenselijke interventies, het formuleren van verwachte uitkomsten en het bepalen van de timing van interventies is kennis over persoonlijke ervaringen van de doelgroep dus belangrijk. Daarmee kan beter antwoord gegeven worden op de vraag ‘wat werkt, voor wie, en onder welke omstandigheden’? Tot slot zijn interviews van belang om nadere duiding te krijgen over de Nederlandse context. Aangezien de literatuur veelal uit het buitenland afkomstig is, dienen de bevindingen die hieruit gedestilleerd worden op het gebied van daderschap van cybercriminaliteit en passende interventies, vertaald te worden naar de Nederlandse context. Deze vertaalslag kan met behulp van daderinterviews worden gemaakt.

2.3.1. Werving van daders

Hackers zijn een duidelijk voorbeeld van zogenaamde ‘verborgen populaties’ (Hutchings, 2016; Decorte & Zaitch, 2016). We zijn er daarom vanuit gegaan dat het vinden van cyberdaders die mee willen werken aan een interview lastig zou zijn (zie ook Van der Wagen et al., 2016). Om de slagingskans te vergroten zijn er dan ook verschillende wervingsstrategieën ingezet. Hieronder worden de verschillende strategieën besproken (zie ook tabel 2.4).

Werving via de reclassering en Halt

De eerste wervingsstrategie die is toegepast, was het benaderen van daders via de reclassering (volwassenen) en Halt (jeugdigen). De werving via de reclassering heeft bij de drie reclasseringsorganisaties (Reclassering Nederland (RN), Stichting Verslavingsreclassering GGZ (SVG) en Leger des Heils Jeugdbescherming & Reclassering (LdHJ&R)) plaatsgevonden die alle middels een brief zijn benaderd. In de brief is medewerking gevraagd voor expertinterviews en is tevens gevraagd

of zij voor ons daders zouden kunnen benaderen die op het moment van schrijven onder toezicht stonden. Vervolgens is een viertal documenten aangeleverd: een lijst met wetsartikelen/delictcodes voor de selectie van toezichthouders van RN, SVG en LdHJ&R, verdachten en daders uit relevante zaken (zie bijlage 4); een brief namens de onderzoekers die aan de toezichthouders verstuurd konden worden; een wervingstekst die de toezichthouders konden gebruiken om hun cliënt te benaderen; een informed consent formulier dat door de cliënt moest worden ondertekend. Ook is er een apart (ProtonMail) e-mailadres aangemaakt waarop toezichthouders en/of cliënten ons konden mailen met vragen over het onderzoek.

De reclassering heeft op twee momenten toezichthouders benaderd. Bij de eerste wervingsronde kwamen er 28 daders in beeld, die via de betrokken toezichthouders zijn gecontacteerd. Het betrof 19 veroordeelde onder toezicht gestelden en 9 cliënten die onder toezicht waren gesteld tijdens een schorsing van voorlopige hechtenis. Van de 28 daders uit de eerste wervingsronde hebben uiteindelijk 8 respondenten meegewerkt aan een interview. Bij de tweede wervingsronde die enkele maanden later plaatsvond, zijn er 11 (nieuwe) daders benaderd. De tweede wervingsronde leverde helaas geen interviews op. We hebben niet volledig zicht gekregen of alle daders daadwerkelijk zijn benaderd door de toezichthouders, maar we gaan er vanuit dat dit in de meeste gevallen is gebeurd. Soms liet de toezichthouder expliciet weten dat de cliënt niet mee wilde werken. In een enkel geval kregen we ook de reden hiervan te horen. De voornaamste reden die werd genoemd was dat er geen vergoeding tegenover stond. Enkele respondenten wilden voordat zij instemden met het interview graag eerst telefonisch contact hebben met de onderzoeker om nog nadere inlichtingen in te winnen over het doel van het onderzoek en ook om vragen te stellen over de privacy.

Op soortgelijke wijze is gepoogd om via Halt jeugdigen te benaderen die op dat moment in een Halt-traject zaten. Hiertoe is de tekst meer toegespitst op jeugdigen en op het Halt-traject. Helaas waren er geen lopende trajecten in de betreffende periode en konden wij dus geen jeugdigen via deze weg interviewen.

In beide gevallen, zowel met betrekking tot de werving via de reclassering als de werving via Halt, was het niet mogelijk om daders te benaderen die niet meer onder toezicht stonden of in een Halt traject verbleven. Voor dit onderzoek zijn overigens ook diverse stappen gezet om daders via de politie te werven. Dit bleek uiteindelijk ook vanwege de nieuwe privacywetgeving niet mogelijk te zijn.

Eigen netwerk

Een andere wervingsstrategie die is toegepast, is het zoeken van daders via het eigen netwerk. Zo is er via een contact van de hoofdonderzoeker (in het kader van haar eerdere onderzoek naar cybercriminaliteit) een wervingstekst gestuurd naar enkele (ex-)daders. De benaderden konden aan de contactpersoon kenbaar maken of ze wilden meewerken aan een interview. Via deze weg heeft één interview plaatsgevonden.

Online werving

Tevens zijn online wervingsstrategieën ingezet. Door daders via fora te werven beoogden we daders in ons onderzoek te betrekken die nog niet gepakt zijn en ook trachtten we via deze weg meer jeugdige daders te kunnen spreken. Hierbij is zorgvuldig over verschillende methodologische en ethische aspecten nagedacht, zoals het wel of niet blootgeven van de identiteit van de onderzoeker(s). De wervingstekst is te vinden in bijlage 5. Het bericht is op 3, zowel Nederlandstalige als Engelstalige, hackerfora geplaatst, maar er kwam weinig respons op. We hebben via één van de fora slechts één

respondent kunnen interviewen. Vervolgens hebben we via deze respondent, bij wijze van *snowballing* wel nog 3 andere respondenten kunnen interviewen die ook zelf actief waren (geweest) op verschillende hackerfora en/of zelf administrator waren (geweest) van dergelijke fora.

Los van het verspreiden van de wervingstekst op hackerfora, is er nog een bericht verspreid op een IT-studie gerelateerde Telegram groep[60], waar iemand van het onderzoeksteam lid van was. Hier is één interview uit voortgekomen. Een van onze respondenten heeft bovendien het bericht verspreid in een IT-gerelateerde WhatsApp groep. Hier zijn verder geen interviews uit voortgekomen.

Tabel 2.4 Overzicht wervingsstrategieën en resultaten

Type werving	Aantal respondenten
Reclassering	8
Via netwerk onderzoekers	1
Online werving via hackerfora	1
Werving via Telegram & WhatsApp	1
Sneeuwbalmethode	3
Totaal	**14**

2.3.2. De afname van de interviews

Net als bij de expertinterviews is gekozen voor een semigestructureerd interview. We hebben de daders achtereenvolgens vragen gesteld over hun achtergrond, motieven, betrokkenheid bij cybercriminaliteit (van initiatie tot stoppen) en hun percepties ten aanzien van de strafbaarheid en de schade van (de door hen gepleegde) cyberdelicten. Ook hebben we gesproken over hun (eventuele) ervaring met interventies (zie het volledige interviewprotocol in bijlage 6). Van de 14 interviews zijn er 13 face to face afgenomen en heeft een interview plaatsgevonden via Skype (met camera). Een deel van de interviews is gehouden op één van de kantoren van de reclassering (meestal aansluitend op een regulier gesprek tussen de cliënt en toezichthouder), een ander deel heeft op locatie plaatsgevonden (in een café of op de universiteit) en één interview is gehouden bij de respondent thuis.

De validiteit van de antwoorden in dader-zelfrapportages is een belangrijk aandachtsgebied in de criminologische literatuur (Krohn, Thornberry, Gibson & Baldwin, 2010). In interviews met daders is het mogelijk dat daders niet al hun delictgedrag rapporteren, maar is het ook mogelijk dat ze de delicten of hun criminele carrière juist 'succesvoller' afschilderen dan ze werkelijk waren. Dit zou ingegeven kunnen zijn door het eergevoel en de behoefte aan status die bij sommige (groepen) hackers bestaat. Er zijn geen publicaties gevonden waarin de aanwezigheid van deze bias is onderzocht bij cyberdaders, maar het is belangrijk hier rekening mee te houden in de interpretatie van de gegevens.

De interviews duurden tussen een uur en ruim twee en een half uur (gemiddeld anderhalf uur).[61] Alle 14 interviews zijn opgenomen met een digitale voice-recorder, uiteraard na het verkrijgen van toestemming, en zijn vervolgens verbatim (letterlijk) getranscribeerd.

[60] Telegram is een chatservice (enigszins vergelijkbaar met WhatsApp) die met encryptie werkt (zie voor meer informatie: https://telegram.org/)

[61] Alle interviews (behalve één) zijn afgenomen door de hoofdonderzoekers, soms vergezeld door een junior onderzoeker of stagiair die aantekeningen maakten. In het kader van de afname van de interviews is er allereerst een pilot gedaan waarbij de twee hoofdonderzoekers samen het interview afnamen. Dit had als doel om te kijken of het samengestelde interviewprotocol goed uitpakte alsook om er voor te zorgen dat de vervolginterviews op een vergelijkbare manier zouden worden afgenomen door de individuele onderzoekers.

2.3.3. Beschrijving populatie

Qua persoonskenmerken zijn er zowel overeenkomsten als verschillen tussen de respondenten. Ze zijn allemaal man en tussen de 18 en 40 jaar oud. 11 van de 14 respondenten doen of hebben een IT-opleiding gedaan, 1 respondent rechten en 1 respondent een marketing opleiding met een IT-component. Het opleidingsniveau is divers maar relatief hoog. Negen respondenten hebben een opleiding op HBO/WO-niveau afgerond of zijn daar mee bezig, vier respondenten hebben als hoogste genoten onderwijsniveau een MBO en een LBO-niveau.

De geïnterviewden zijn bij één of meer vormen van cybercriminaliteit betrokken geweest. Sommige respondenten hebben zich nadrukkelijk toegespitst op een soort cyberdelict; andere respondenten zijn betrokken geweest bij verschillende delicten (voor een overzicht zie tabel 2.5). Zoals eerder aangegeven, kunnen slechts in beperkte mate details vermeld worden over de context van het delict om de anonimiteit van de respondenten te waarborgen.

Tabel 2.5. Overzicht gerapporteerde cyberdelicten

Gerapporteerde cyberdelicten/activiteiten	Aantal respondenten die aangaven hierbij betrokken te zijn geweest
Hacken (van een systeem, email-account, website, etc.)	11
DdoS	2
Fraude en oplichting (creditcardfraude, bankfraude, identiteitsfraude, clickfraude)	4
Virtuele diefstal	2
Webdefacements	1
Phishing	2
Afluisteren	1

Zoals uit tabel 2.5 kan worden opgemaakt heeft het merendeel van de respondenten zich in ieder geval schuldig gemaakt aan hacken, dat in juridische termen als computervredebreuk wordt aangeduid (art. 138ab Sr). Bij de meerderheid van de respondenten kan hacken als het primaire delict worden beschouwd. De respondenten hadden bijvoorbeeld een school, website(s), iemands persoonlijke e-mail, Facebook-account, iCloud-account of de server van een bedrijf gehackt. Middels het hacken was het dan mogelijk voor hen om gegevens (bijvoorbeeld inloggegevens, afbeeldingen, etc.) te kopiëren, te verzamelen, te veranderen, te wissen en/of te distribueren.

In enkele gevallen kan hacken meer als een secundair delict worden beschouwd. Twee respondenten waren betrokken bij online fraude/oplichting, maar computervredebreuk is ook opgelegd vanwege de inbreuk op de integriteit van een ICT systeem. Deze respondenten waren zich wel bewust van het feit dat ze voor computervredebreuk of cybercriminaliteit veroordeeld waren, maar zagen zichzelf niet als een hacker of cyberdader. Eén van hen zegt wel affiniteit te hebben met ICT, maar heeft hacken niet nodig gehad voor het plegen van het delict en heeft zich daar nooit in verdiept. De ander had de misbruikte inloggegevens online gekocht. Ook was er een respondent veroordeeld voor hacken in de relationele sfeer. Hij zegt überhaupt niets van computers te weten. Een respondent die hackte met als doel om afbeeldingen van personen te verzamelen, geeft aan dat hij geen geavanceerde technieken hoefde toe te passen. Ook hij ziet zichzelf niet als een hacker/cyberdader. Deze vier daders zijn dus wel veroordeeld voor cybercriminaliteit in enge zin, maar associëren zichzelf niet met deze vorm van criminaliteit.

De geïnterviewden zijn niet voor alle delicten opgepakt en/of veroordeeld. Zoals blijkt uit tabel 2.6, hebben vier van de respondenten geen justitiële interventie opgelegd gekregen. Twee daarvan

zijn nooit opgepakt, één respondent is gestraft door zijn ouders en de school en bij één respondent is de zaak geseponeerd. Twee van de respondenten waren ten tijde van het afnemen van het interview nog in afwachting van een uitspraak in de rechtszaak. Bij de overige respondenten is een (voorwaardelijke) gevangenisstraf, werkstraf, taakstraf, geldboete, schadevergoeding, contactverbod en/of een elektronische enkelband opgelegd. De opgelegde duur van deze straffen varieert van detentie voor een halfjaar tot vier jaar en een taak- of werkstraf van 14 uur tot 148 uur. Ook de hoogte van de schadevergoeding of geldboete varieert.

Tabel 2.6. Overzicht gerapporteerde opgelegde justitiële interventies

Gerapporteerde opgelegde justitiële interventies	Aantal respondenten
(Voorwaardelijke) gevangenisstraf	3
Werkstraf/Taakstraf	7
Geldboete	1
Schadevergoeding	2
Contactverbod	2
Elektronische enkelband	1
Nog geen interventie opgelegd ten tijde van interview (in afwachting van strafzaak)	2
Geen justitiële interventie opgelegd gekregen	4

2.3.4. Mogelijkheden en beperkingen

Gezien het geringe aantal respondenten beogen we niet om aan de hand van onze bevindingen generaliserende uitspraken te doen over alle cyberdaders. We trachten vooral om nadere verdieping te geven aan aspecten die ook in de literatuur en expertinterviews naar voren zijn gekomen en deze te belichten vanuit het perspectief van de dader. Tevens kunnen op basis van de daderinterviews eventuele blinde vlekken worden ingevuld. Op basis van 14 interviews is dit ons inziens goed mogelijk gebleken. De interviews hebben zeer rijke data opgeleverd en geven goed het perspectief weer van de dader ten aanzien van diverse aspecten die onderzocht zijn.

Naast het feit dat de respondentengroep qua omvang gering is, is er sprake van een hele specifieke selectie. Hier kleven voor- en nadelen aan. Allereerst betreft het een groep waarvan een groot deel één of meerdere keren is opgepakt en een interventie heeft gekregen of gaat krijgen. Aangezien de ervaringen van daders met interventies een belangrijke component is in ons onderzoek, beschouwen we het feit dat we vooral ‘gepakte’ daders hebben gesproken als een voordeel. We konden deze respondenten immers specifieke vragen stellen over hoe ze aankijken tegen hun interventie, hoe ze de interventie hebben ervaren en in hoeverre ze iets aan de interventie hebben gehad.

Tegelijkertijd heeft het interviewen van gepakte daders zijn beperkingen. Bepaalde subgroepen daders, die juist goed buiten beeld van justitie kunnen blijven, hebben we minder kunnen betrekken in ons onderzoek. Hier staat wel weer tegenover dat de respondenten die zijn geïnterviewd, soms wel een grotere criminele carrière hadden c.q. aangaven meer delicten te hebben gepleegd dan waarvoor ze zijn gepakt en/of veroordeeld. In de interviews is ook aandacht besteed aan hun betrokkenheid bij deze delicten. Voor de drie niet-gepakte daders gold dat ze wel aangaven gestopt te zijn met het illegaal hacken van systemen. Bij hen kon specifiek nagaan worden waarom ze zijn gestopt (zonder interventie).

Naast daders die aangaven meer delicten te hebben gepleegd dan waarvoor ze zijn gepakt en/of veroordeeld, is ook met enkele respondenten gesproken die (gedeeltelijk) ontkenden betrokken te zijn bij het delict waarvoor ze zijn gepakt en/of veroordeeld. Een van de respondenten ontkende

volledige betrokkenheid en een andere respondent gaf aan niet voor alle ten laste gelegde delicten schuldig te zijn. Het was bij deze respondenten, vooral bij de eerste, dan ook lastig om alle vragen uit het interviewprotocol te stellen.

Naast het feit dat we een groep daders hebben gesproken die (althans voor een groot deel) gepakt is, betreft het een groep daders die naar eigen zeggen geen actieve plegers meer zijn. Alle 14 daders, gaven aan gestopt te zijn met het plegen van (cyber)delicten. Ten tijde van het interview pleegden ze naar eigen zeggen geen delicten meer, wat zowel voordelen als beperkingen heeft voor onderhavig onderzoek. Het voordeel is dat op deze manier ook inzichten verworven konden worden met betrekking tot de beëindiging van de criminele carrière (*desistance*). We hebben de respondenten kunnen vragen waarom ze zijn gestopt (met of zonder interventie) en konden hen laten reflecteren op eventuele factoren die hiertoe hebben bijgedragen. Het nadeel van het interviewen van reeds gestopte daders is dat ze tijdens het interview moeten teruggrijpen naar hun verleden en de werkelijkheid achteraf mogelijk mooier of extremer voorspiegelen dan deze was. Mogelijk zijn ze anders tegen bepaalde zaken aan gaan kijken en/of kunnen ze zich bepaalde dingen niet meer goed herinneren. Een andere beperking is dat we niet het verhaal gehoord hebben van daders die (ondanks interventies) niet gestopt zijn en daardoor hebben we beperkte inzichten in redenen van doorgaan. Tot slot is het feit dat er geen minderjarige daders zijn geïnterviewd een beperking voor het onderzoek. Daar staat tegenover dat een aantal van de respondenten, hun delicten juist pleegde toen ze minderjarig waren en daar tijdens het interview op reflecteert. Ook is er relatief veel aandacht besteed aan jeugdige daders in de expertinterviews.

2.4. Analyse expert- en daderinterviews

Zowel de expert- als daderinterviews zijn na transcriptie geanalyseerd met behulp van het kwalitatieve analyseprogramma ATLAS.ti. De data zijn zowel op een deductieve als meer inductieve wijze gecodeerd. Bij de eerstgenoemde (meer *top-down*) analysestrategie worden datasegmenten gecodeerd en gecategoriseerd op basis van een vooropgesteld codeboek gerelateerd aan het theoretisch kader en de onderzoeksvragen. In het tweede geval worden codes toebedeeld aan segmenten die als het ware komen 'oprijzen' uit de empirie, ook wel *coding up* genoemd (Van Staa & Evers, 2015). Door beide te combineren hebben we getracht om de theorie tegen de empirie af te zetten c.q. te 'confronteren' en daarmee beter begrip te krijgen van het fenomeen. Vanwege de grote hoeveelheid verzamelde data in combinatie met de uitvoerige vragenlijsten over zowel daderkenmerken als interventies in brede zin heeft het deductief coderen in de analyse meer nadruk gekregen.

2.5. Waarborging privacy

Voor het onderzoek is het van groot belang om de anonimiteit van de respondenten te waarborgen. Daartoe zijn alle transcripten direct geanonimiseerd opgeslagen op een extra beveiligde omgeving (Blackberry Workspace). Tevens is in samenspraak met het WODC een Privacy Impact Assessment (PIA) uitgevoerd. Hierbij is in kaart gebracht wat de eventuele privacyrisico's kunnen zijn voor betrokkenen en hoe deze voorkomen kunnen worden. Uiteraard is alles in het werk gezet om de data te anonimiseren en er voor te zorgen dat niets herleidbaar is tot individuele personen. Niet alleen de persoonsgegevens zijn geanonimiseerd, maar ook specifieke details over de delicten die de daders hebben gepleegd en de context waarin de delicten zijn gepleegd. Op deze manier is getracht om de anonimiteit en vertrouwelijkheid volledig te waarborgen.

DEEL 1: Kenmerken van daders van cybercriminaliteit in enge zin

In paragraaf 1.1 is beschreven dat er nog maar beperkt systematisch inzicht is in de kenmerken van cyberdaders. Daarbij gaat het in de eerste plaats om achtergrondkenmerken die als criminogene factoren voor het ontstaan van cyberdaderschap gelden. In de tweede plaats gaat het om de drijfveren voor en beleving van het delictgedrag door cyberdaders. In de derde plaats gaat het om de percepties die daders hebben over de schade die hun gedrag aanricht en de inschatting van de juridische gevolgen die op het gedrag kunnen volgen. En in de vierde plaats gaat het om de manier waarop de criminele loopbanen zich ontwikkelen. Voor het inrichten van effectieve interventies is het van belang het inzicht in deze kenmerken te vergroten. In de komende vier hoofdstukken staan we uitgebreid bij deze kenmerken stil op basis van het literatuuronderzoek, de expertinterviews en de daderinterviews.

Zoals in dit eerste deel duidelijk zal worden, komt er uit de literatuurstudie relatief veel informatie naar voren over de achtergrondkenmerken en drijfveren van cyberdaders, van hackers in het bijzonder. De studies naar achtergrondkenmerken baseren zich vooral op registratie- en dossierstudies en daderzelfrapportages. Studies naar drijfveren maken gebruik van zowel daderzelfrapportages als interviewdata. Bij veel van deze onderzoeken is de kanttekening te plaatsen dat zij vooral zicht hebben op gearresteerde en/of veroordeelde cyberdaders. Deze beperking geldt ook voor onze eigen interviewdata (onder experts en daders). Voor studies die gebruik maken van interviewdata geldt bovendien dat er vaak sprake is van een (zeer) kleine onderzoekspopulatie. Deze beperking geldt ook voor onze daderinterviews. De onderzoeken die gebruik maken van zelfrapportage vragenlijsten onder daders betreffen wel de algemene populatie maar richten zich meestal op jongeren en vooral op de lichtere delicten. De komende hoofdstukken moeten in het licht van deze beperkingen gelezen worden.

Bij het bespreken van de percepties over schade en juridische gevolgen (hoofdstuk 5) en de factoren die een rol spelen bij de criminele carrière (hoofdstuk 6) hebben de interviewdata die voor het huidige onderzoek zijn verzameld een belangrijke rol omdat in de literatuur hierover relatief weinig informatie is gevonden. Hoewel in de literatuur wel relatief veel is geschreven over de drijfveren en beleving van cyberdaders bieden de daderinterviews ook hier verdiepende inzichten (hoofdstuk 4).

Op de hierboven beschreven wijze levert deel I de input voor het tweede deel van dit rapport. In deel 2 van het rapport wordt besproken welke interventies er potentieel effectief kunnen zijn. Daarbij wordt ingegaan op de (online en offline) criminogene- en protectieve factoren en de responsiviteit bij (verschillende type) daders van cybercriminaliteit in enge zin.

Hoofdstuk 3 Achtergrondkenmerken

In dit hoofdstuk worden de achtergrondkenmerken van cyberdaders beschreven zoals die uit de literatuurstudie, de expertinterviews en de daderinterviews naar voren komen. Daarbij komen achtereenvolgens de demografische- en sociaaleconomische kenmerken, vrijetijdsbesteding, gezinsgerelateerde- en psychologische kenmerken van cyberdaders aan bod en wordt ingegaan op het zelfbeeld en de sociale contacten (online en offline) van cyberdaders. Het accent ligt in dit hoofdstuk op de informatie uit de literatuur en de expertinterviews omdat de geïnterviewde daders met betrekking tot achtergrondkenmerken maar een klein deel van de daderpopulatie vertegenwoordigen. Een algemene beschrijving van de achtergrondkenmerken van de veertien geïnterviewde daders is reeds gegeven in paragraaf 2.3.3. In enkele paragrafen zal wel gebruik gemaakt worden van de daderinterviews omdat zij daar een waardevolle aanvulling of verdieping geven, bijvoorbeeld daar waar het gaat over hun sociale leven.

3.1. Demografische kenmerken

3.1.1. Leeftijd

Volgens de literatuur wordt het grootste deel van de cybercriminaliteit in enge zin gepleegd door daders jonger dan twintig jaar. Dit geldt zowel voor hacken (Yar, 2005; Marcum, Higgins, Ricketts & Wolfe, 2014) als voor de bredere categorie cybercriminaliteit in enge zin (naast hacken o.a. ook het uitvoeren van DDoS-aanvallen en malware verspreiden) (Aiken et al., 2016; Hutchings, 2016; Ruiter & Bernaards, 2013). Volgens Ruiter en Bernaards (2013) wijkt het leeftijdscriminaliteitspatroon daarmee niet af van die van traditionele daders. Voor sommige delict typen ligt de leeftijd waarop gestart wordt met cybercriminaliteit echter wel relatief laag. In een onderzoek onder 535 hackers (Chiesa, Ducci & Ciappi, 2009) blijkt dat 61% van de ondervraagden begon met hacken tussen het 10^{e} en 15^{e} levensjaar, 32% tussen het 16^{e} en 20 levensjaar en 8% na het 21ste levensjaar.

Bij meer financieel georiënteerde georganiseerde cybercriminaliteit, waarin onder andere het maken en distribueren van malware een belangrijke activiteit is, lijken relatief vaker volwassen daders betrokken te zijn. In onderzoek onder 107 cyberverdachten lag de leeftijd tussen 17 en 72 met een gemiddelde van 37 jaar (Odinot et al., 2017). De subgroep verdachten die zich met de feitelijke ICT georiënteerde activiteiten bezighield was met gemiddeld 29 jaar wel jonger dan de andere verdachten. Deze subgroep lijkt jonger dan daders van traditionele vormen van georganiseerde misdaad (zie bijvoorbeeld Van Koppen, De Poot, Kleemans & Nieuwbeerta, 2010).

Het beeld dat uit de literatuur naar voren komt ten aanzien van de leeftijd van cyberdaders, wordt grotendeels bevestigd door de experts in de interviews. Een belangrijk verschil is echter dat de experts een grotere bijdrage van de jongvolwassenen vermelden. De leeftijd van daders van cybercriminaliteit in enge zin kan volgens de experts variëren van 11 tot en met 60 jaar, maar de jongeren (12-18 jaar) *en* de jongvolwassenen (18-23 jaar) behelzen de grootste categorie binnen de dadergroep. Het beeld dat de startleeftijd vaker lager ligt dan bij traditionele daders wordt door enkele experts bevestigd. Een expert van de politie haalt hier het voorbeeld aan van een 12-jarige jeugdige dader die administrator (beheerder) was op een cybercrimineel platform.

Wat betreft de financieel georiënteerde georganiseerde criminaliteit, geven experts (voornamelijk politiemedewerkers) in de interviews aan dat er een categorie volwassen daders bestaat die al actief is in de traditionele misdaad en die op latere leeftijd de overstap maakt naar cybercriminaliteit. Daarbij maken ze zichzelf soms bepaalde (IT) vaardigheden eigen of gaan

samenwerken met iemand (vaak een jonger persoon) die deze IT vaardigheden al bezit. In dit kader wijzen diverse experts op actieve rekrutering van (jonge) technische specialisten, alhoewel er weinig bekend is (ook niet in de literatuur) over hoe frequent dit gebeurt. Bijlenga en Kleemans (2017) wijzen bijvoorbeeld op de benadering van medewerkers in de ICT-sector voor criminele activiteiten.

De verklaring voor het feit dat jeugdigen mogelijk een groot aandeel hebben in cybercriminaliteit in enge zin, wordt in de literatuur vooral gezocht in het feit dat het internet tegenwoordig (op steeds jongere leeftijd) een belangrijk onderdeel uitmaakt van hun educatieve en recreatieve omgeving. Tegelijkertijd is de adolescentie een turbulente periode waarin jeugdigen allerlei biologische, psychologische en sociale veranderingen ondergaan en volop experimenteren en risicovolle activiteiten ondernemen. Het internet biedt juist daar nieuwe mogelijkheden voor, inclusief het plegen van cybercriminaliteit (Brewer, Cale, Goldsmith & Holt, 2018; Zebel et al., 2013). Het feit dat jeugdigen zo vroeg starten met het plegen van cybercriminaliteit, wordt door verschillende experts tevens gekoppeld aan het feit dat jeugdigen al vroeg beginnen met gamen en via de gaming wereld bij cybercriminele activiteiten terechtkomen (zie verder hoofdstuk 6). Van de 14 volwassen daders die zijn geïnterviewd, pleegde een groot deel (N=9) de delicten uitsluitend of voornamelijk toen ze jonger dan 18 jaar waren. Het verloop van de criminele carrière zal nader aan de orde komen in hoofdstuk 6.

Kortom, zowel uit de literatuur als uit de interviews blijkt dat er een sterke oververtegenwoordiging is van jongeren onder de cyberdaders, maar er zijn geen sterke aanwijzingen dat deze oververtegenwoordiging groter is dan bij traditionele criminaliteit. Daar waar het om een relatief vroege startleeftijd gaat zou dat vooral de subgroep van hackers betreffen. Met name door de experts wordt verder benadrukt dat ook jongvolwassenen oververtegenwoordigd zijn onder daders van cybercriminaliteit in enge zin.

3.1.2. Sekse

De literatuur beschrijft dat het overgrote deel van de daders van cybercriminaliteit in enge zin man is zowel als het gaat om jeugdige daders (Yar, 2005; Aiken et al., 2016) als volwassen daders (Ruiter & Bernaards, 2013; Weulen Kranenbarg, 2018). Exacte percentages mannelijke daders die in studies genoemd worden, liggen tussen de 78 en 95% (Chiesa et al., 2009; Ruiter & Bernaards, 2013; Weulen Kranenbarg, 2018). Vrouwelijke daders blijken wel actief in cyberdelicten zoals online fraude, maar zijn nauwelijks actief in de meer technische delicten (Hutchings, 2016). Zo beschrijven Chiesa et al. (2009) dat 94% van de 535 onderzochte hackers man is. Weulen Kranenbarg (2018), die niet alleen verdachten van hacken maar ook andere daders van cybercriminaliteit in enge zin in haar onderzoek heeft betrokken (N=870, periode 2000-2012), heeft gevonden dat 80% van de verdachten man was. Dit percentage komt overeen met het door haar gevonden percentage mannen onder daders van traditionele criminaliteit (N = 1,144,740). Ook Ruiter en Bernaards (2013), die zich specifiek toespitsten op verdachten (N=323) van computervredebreuk (crackers), hebben een man/vrouw verhouding gevonden onder de verdachten (78% man, 22% vrouw) die vergelijkbaar is met de verhouding bij traditionele criminaliteit.

Voor de bevinding dat bij hacken mannen relatief sterk vertegenwoordigd zijn, geeft de literatuur verschillende verklaringen. Een eerste verklaring is dat mannen en vrouwen psychologisch van elkaar verschillen. Zo zijn mannen volgens Taylor (1999, in Yar, 2005) meer geïnteresseerd in wiskunde en logica. Een tweede hiermee verbonden verklaring is het feit dat kinderen worden getraind om bepaalde genderrollen aan te nemen. Techniek is doorgaans een veld dat wordt toebedeeld aan het mannelijke domein (Taylor, in Steinmetz, 2015a). Volgens Turkle (1984, in Yar, 2005) hebben mannen daardoor een sterke behoefte aan *hard mastery*. Dit verwijst naar de drang om

machines te beheersen, een aspect dat ook in latere hackerstudies terugkomt (Steinmetz, 2015a; Van der Wagen, 2018). Een derde verklaring is de maatschappelijke druk waar jonge mannen mee te kampen hebben. Jongens worden geacht zich als 'echte mannen' te gedragen, wat inhoudt dat er van ze wordt verwacht dat ze autoriteit, controle en macht uitoefenen over anderen. Hacken biedt de mogelijkheid om deze controle en macht te verkrijgen (Sterling, 1994, in Yar, 2005). Een vierde verklaring die in de literatuur wordt aangehaald, gaat vooral in op factoren die vrouwen ontmoedigen om een hacker te worden. De masculiene en competitieve hackerwereld zou vrouwen afschrikken en het gebruik van technisch en mannelijk jargon sluit vrouwen buiten (Taylor, 1999, in: Steinmetz, 2015a). Hutchings (2016) geeft daarnaast nog aan dat vrouwen minder geaccepteerd worden in online sociale gemeenschappen en ook met een zekere argwaan worden bejegend. Steinmetz (2015a) signaleert echter op basis van participerende observatie dat dit langzamerhand begint te veranderen.

Met name de eerste twee verklaringen zijn bruikbaar om te begrijpen waarom de man-vrouw ratio bij hacken groter is dan bij traditionele criminaliteit. De laatste twee verklaringen zijn minder bruikbaar, die spelen immers ook een rol bij traditionele criminaliteit.

Overeenkomstig de literatuur signaleren de experts dat daders van cybercriminaliteit in enge zin voornamelijk jongens en mannen zijn. Enkele experts van de politie geven aan dat vrouwen wel geregeld betrokken zijn bij hacken in de conflictsfeer, waarbij het overigens niet gaat om de toepassing van geavanceerde technieken. Ook zijn er volgens hen, conform de studie van Hutchings (2016), indicaties dat vrouwen soms betrokken zijn bij de meer financiële cyberdelicten zoals phishing.

Alle door ons geïnterviewde daders zijn man. Bij enkele respondenten is als drijfveer het hebben van macht en controle over de machine naar voren gekomen. Juist deze drijfveer draagt volgens de literatuur bij aan de verklaring voor het relatief grote man-vrouw verschil in daderschap van cybercriminaliteit in enge zin ten opzichte van traditionele criminaliteit (zie ook hoofdstuk 4).

Samenvattend, maken alle bronnen duidelijk dat er net als bij traditionele criminaliteit onder jeugdige en volwassen daders van cybercriminaliteit een sterke oververtegenwoordiging is van mannelijke daders. Bij hacken blijkt volgens een groot deel van de studies dat deze oververtegenwoordiging van mannen zelfs nog sterker te zijn dan bij traditionele criminaliteit. Er zijn wel indicaties dat vrouwen betrokken zijn bij (laagdrempelige vormen van) hacken in de conflictsfeer en soms een rol spelen bij delicten zoals phishing.

3.1.3. Etniciteit

Nederlandse en buitenlandse studies beschrijven dat daders van cybercriminaliteit in enge zin voornamelijk autochtone daders zijn (o.a. Steinmetz, 2015a; Zebel et al., 2013,). Voor jeugdige (minderjarige en jongvolwassen) daders van cybercriminaliteit in enge is bovendien gevonden dat zij ook vaker autochtoon zijn dan traditionele daders (Rokven, Weijters & Van der Laan, 2017[62]). Voor bepaalde subgroepen is die oververtegenwoordiging van autochtone daders minder prominent. Zo vonden Ruiter en Bernaards (2013) dat van de 323 jeugdige en volwassen verdachte crackers 59% autochtoon, 12% Westers allochtoon en 29% niet-Westers allochtoon was. Daarmee ligt de verhouding volgens hen niet heel anders dan bij verdachten van traditionele criminaliteit. Weulen Kranenbarg, Ruiter, van Gelder & Bernasco (2018) laten zien dat er onder volwassen daders meer autochtonen (71%) in de cybercriminaliteit (in enge zin) groep zaten dan in de groep met traditionele criminaliteit (66%). De andere etniciteiten (overigens niet gespecificeerd in het onderzoek) waren in hun onderzoek gelijk verdeeld in beide groepen.

[62] De exacte verhouding wordt in dit onderzoek niet gespecificeerd.

De experts doen weinig uitspraken over de etnische achtergrond van cyberdaders. De informatie die wel uit de expertinterviews komt, lijkt vrij sterk overeen te komen met wat er in de literatuur naar voren komt. Men veronderstelt dat (jeugdige) daders die betrokken zijn bij de meer technische delicten waar lol, plezier en technologische uitdaging op de voorgrond staan, voornamelijk autochtone Nederlanders zijn. Als het gaat om cyberdelicten waar financieel gewin de belangrijkste drijfveer is en waar sprake is van een georganiseerd verband, wordt een relatief grotere deelname verondersteld van vooral niet-Westerse allochtonen. Zo wordt gesuggereerd dat Russische of Oost-Europese daders of dadergroepen voornamelijk actief zijn bij vormen van cybercriminaliteit waarbij geavanceerde (banking) malware wordt gebruikt. Ook zijn zij betrokken bij delicten als creditcardfraude. Als het om phishing of cyberoplichting gaat, bestaan er volgens enkele politie-experts aanwijzingen dat hier regelmatig Noord- en West-Afrikaanse daders bij betrokken zijn. Er is echter weinig bekend over hoe frequent dat is en hoe de verhoudingen liggen. Kortom, het enige wat we op basis van de bevindingen met enige zekerheid kunnen zeggen over de etniciteit van daders, is dat er relatief meer autochtone dan allochtone jeugdigen bij cybercriminaliteit betrokken zijn en dat er bij fraude-gerelateerde cyberdelicten en georganiseerde misdaad een relatief groter aantal autochtone daders betrokken lijkt te zijn.

3.2. Sociaaleconomische kenmerken en vrijetijdsbesteding

3.2.1. Sociaal milieu/sociaaleconomische status

Uit oudere studies komt het beeld naar voren dat hackers doorgaans tieners zijn of studenten uit relatief welgestelde middenklasse gezinnen (Chiesa, et al., 2009; Sterling, 1993 in Richet, 2013; Turgeman-Goldschmidt, 2005). Zo was in het onderzoek van Chiesa et al. (2009) van de ondervraagde hackers 8% afkomstig uit een *highclass* milieu, 44% uit een *upper high class* milieu, 37% uit een *middle class* milieu en 11 % uit een *lower class* milieu. Recenter onderzoek naar cyberdaders geeft weinig informatie over het sociaal milieu of de sociaaleconomische klasse waaruit daders van cybercriminaliteit komen. Enkele kwalitatieve studies (o.a. Dupont, 2014) brengen naar voren dat de meeste hackers uit welgestelde gezinnen lijken te komen, maar zijn bevindingen zijn gebaseerd op een kleine steekproef (N=10). Verscheidene geïnterviewde experts stellen dat cyberdaders over het algemeen een goede sociaaleconomische achtergrond hebben. Dit beeld komt ook naar voren in de daderinterviews. De cyberdaders komen volgens de experts vaak uit een gezin waarin beide ouders werk hebben of hadden of waarbij een ouder een goede baan had. Er wordt in de interviews niet gesproken over armoede of werkloze ouders. Bij de subgroep van phishing zou dit volgens enkele experts anders zijn. Zo stelt een expert dat er bij deze subgroep vaker sprake is van achterstandsgezinnen die bepaalde dingen niet kunnen betalen, als gevolg waarvan dit type dader niet gericht is op lange-termijn investeringen zoals werk, carrière of een opleiding, maar op het verdienen van geld door middel van het plegen van criminaliteit.

We kunnen concluderen dat er weinig (recente) informatie beschikbaar is over de sociaaleconomische status van cyberdaders en als die er is, is deze vaak gebaseerd op kwalitatieve studies met een (zeer) kleine steekproef.

3.2.2. Opleiding(sniveau)

Het overheersende beeld in de literatuur wat betreft de opleidingsachtergrond van cyberdaders is dat zij een relatief hoog intelligentie- en opleidingsniveau hebben en goede technische vaardigheden (Stambaugh, Beuapre, Icove, Baker, Cassady & William, 2001; Turgeman-Goldschmidt, 2005). Op basis

van dit profiel worden zij weleens vergeleken met witteboordencriminelen, die eenzelfde soort profiel zouden hebben (Cho, 2016). Ook zijn er studies die meer variëteit laten zien als het gaat om opleidingsniveau, alhoewel het hier wel vooral lijkt te gaan om daders die betrokken zijn bij georganiseerde cybercriminaliteit. Zo hadden de 107 verdachten van georganiseerde cybercriminaliteit uit het onderzoek van Odinot et al. (2017), waarvan 39 van de daders onder de noemer enge zin vallen, zeer uiteenlopende opleidingen: van universitair opgeleid en gediplomeerde IT-specialisten tot verdachten die hooguit hun een middelbare school hadden afgemaakt.

Als het gaat om het effect van het wel of geen opleiding hebben op delinquent gedrag laat bestaand onderzoek zien dat opleiding een andere rol speelt voor cyberdaders dan voor traditionele daders. Hoewel de kans op het plegen van traditionele criminaliteit afneemt wanneer de jeugdigen een opleiding volgen, geldt dat niet voor de kans op daderschap van cybercriminaliteit (Weulen Kranenbarg et al., 2018). Deze afwijkende rol van opleiding lijkt vooral van belang in de groep hackers. Echter, ook op het effect van opleiding binnen de groep hackers worden verschillende nuances aangebracht. Marcum et al. (2014) hebben op basis van een survey onder 1617 middelbare schoolstudenten in de VS gevonden dat studenten met betere schoolprestaties een grotere kans hebben om betrokken te raken bij hacken, maar ander onderzoek laat zien dat veel hackers hun opleiding vroegtijdig verlaten, omdat zij het te makkelijk of te saai vinden en niet gestimuleerd worden; ze houden van leren, maar niet van leren op school (Chiesa et al., 2009).

De meeste experts stellen dat het opleidingsniveau van cyberdaders in enge zin inderdaad hoger lijkt te zijn dan dat van de gemiddelde traditionele dader. Ook door experts wordt de kanttekening gemaakt dat niet alle daders hun opleiding afmaken of beginnen met een vervolgopleiding. Dit zou minder dan bij traditionele daders te maken hebben met capaciteiten en meer met motivatie. Enkele experts van de politie zijn van mening dat er vaak te snel wordt gedacht dat alle cyberdaders hoogopgeleid zijn. Ze hebben ook best veel verdachten van cybercriminaliteit in enge zin gezien met een gemiddeld of laag opleidingsniveau, hetgeen onder meer zou kunnen samenhangen met het feit dat het instapniveau bij veel cyberdelicten steeds makkelijker wordt door de beschikbaarheid van kant-en-klare tools (zie hoofdstuk 6). Bij de geïnterviewde daders is wat betreft de opleiding en het opleidingsniveau een grote variëteit waar te nemen. Sommige respondenten zijn van school gestuurd omdat zij hun school hadden gehackt en/of opstandig gedrag vertoonden in de klas en ook vaak te laat kwamen of spijbelden. De oorzaak was dan volgens deze daders niet zozeer dat ze het niveau niet aankonden, maar juist dat het te gemakkelijk was en ze zich gingen vervelen. Het type opleiding was bij de meeste respondenten (N = 11) een technische, ICT-opleiding.

Wat uit bovenstaande in ieder geval duidelijk wordt, is dat het volgen van een opleiding minder duidelijk als protectieve factor voor criminaliteit geldt bij daders van cybercriminaliteit in enge zin dan bij daders van traditionele criminaliteit.

3.2.3. Werk

In sommige studies wordt het beeld geschetst dat het gehele leven van hackers – werk, vrije tijd, muziek, boeken en films – op een of andere manier gelinkt zou zijn aan de computer (Dremliuga, 2014). Er zijn echter weinig kwantitatieve studies waarin de werksituatie van cyberdaders wordt beschreven en kwalitatieve studies laten geen eenduidig beeld zien. Verschillende kwalitatieve studies (Chiesa et al., 2009; Dupont, 2014; Goode & Cruise, 2006) omvatten een steekproef van cyberdaders die in een diversiteit aan beroepen werkzaam zijn, terwijl anderen beschrijven dat de onderzochte

daders vooral in de IT-sector werken (Bijlenga & Kleemans, 2017; Steinmetz, 2015a, 2015b). Odinot et al. (2017) laten in een wat grotere steekproef zien dat de werksituatie van verdachten van georganiseerde cybercriminaliteit varieert: van personen met een eigen bedrijf, werkend of studerend tot werkloos, drugsverslaafd of dakloos.

Uit het onderzoek van Bijlenga en Kleemans (2017) komt naar voren dat cyberdaders die samenwerking zoeken met ICT-specialisten dit vooral via hun (eerdere) werkrelaties doen. Op die manier zou het werken in de ICT de kans verhogen gerekruteerd te worden als dader van cybercriminaliteit. De enige door ons gevonden kwantitatieve studie naar werk en cybercriminaliteit (Weulen Kranenbarg et al., 2018) concludeert dat werken, ongeacht of dit in de IT-sector is of niet, een protectieve factor is voor traditioneel daderschap. Voor cyberdaderschap gaat dit niet op. Werken in de IT sector lijkt zelfs de kans op cyberdaderschap te vergroten (het effect is weliswaar niet significant, maar wordt toch beschouwd als een duidelijke aanwijzing).

Volgens de geïnterviewde experts zijn de cyberdaders vaak nog aan het studeren op het moment dat zij hun delicten plegen en hebben in sommige gevallen ook een bijbaan. Bij de oudere cyberdaders die al wel een baan hebben, maken zij een onderscheid tussen de daders die een legale baan hebben en de daders die van cybercriminaliteit hun 'werk' hebben gemaakt. Daders met een legale baan zijn niet altijd in een IT-gerelateerde vakgebied werkzaam. De daders die wel een IT-gerelateerde baan hebben zijn volgens de experts bijvoorbeeld werkzaam als IT-beheerder, software tester, innovatiemanager of ethisch hacker. Hiernaast is er een groep (voornamelijk financiële) cyberdaders, die van criminaliteit hun werk heeft gemaakt en hier een inkomen mee verdient. Dit zijn vaak de daders die fulltime bezig zijn met het plegen van delicten. Voor hen is criminaliteit, aldus sommige experts, een levensstijl. Tot slot vermelden sommige reclasseringsmedewerkers een categorie cyberdaders die werkloos is.

Bij de geïnterviewde cyberdaders is een meerderheid (N = 9) werkzaam of werkzaam geweest in de ICT-sector of op het gebied van online marketing. Van de andere vijf zijn er vier nog studerend en heeft een vooral fabriekswerk gedaan. Enkele respondenten waren als zelfstandig ondernemer werkzaam in de IT of online marketing. Ze hebben een eigen bedrijfje (of in het verleden gehad), onder andere op het gebied van sociale media, websites maken en hosten, IT of hacken.

3.3. Vrijetijdsbesteding

Sinds de opkomst van de computer worden hackers vooral gezien als enthousiastelingen of hobbyisten die een groot deel van hun (vrije) tijd online doorbrengen (Aiken et al., 2016; Furnell, 2009). Twee recente studies hebben ook een daadwerkelijk verband aangetoond tussen de mate van computergebruik en het plegen van cybercriminaliteit. Holt, Kilger, Chiang & Yang (2017) hebben op basis van een survey onder 779 universitaire studenten uit de VS en Taiwan gevonden dat het hebben van een computer en tijd online doorbrengen positief samenhangen met allerlei vormen van *web defacen*. Ook in een grootschalige, vijfjarige follow-up studie onder 2844 Koreaanse tieners is meer computergebruik in verband gebracht met meer zelf-gerapporteerde cyberdelinquentie, zowel in enge als ruime zin, en een versnelde toename van cyberdelinquentie over de tijd (Bae, 2017). Computergebruik blijkt in deze grootschalige, longitudinale studie de sterkste voorspeller van cyberdelinquentie, boven zelfcontrole, offline slachtofferschap van pesten en stress. Het gevonden verband wordt verklaard vanuit een gelegenheidsperspectief: hoe meer blootstelling er is aan een online omgeving, hoe meer gelegenheid er is voor online delinquentie (Bae, 2017). In een kwalitatief onderzoek (Chiesa et al., 2009) is daarnaast beschreven dat sommige hackers niet geïnteresseerd zijn in de doorsnee vrijetijdsactiviteiten van hun leeftijdsgroep, zoals muziek, tv, sport en uitgaan. Een

overweldigende meerderheid van de hackers in deze studie was groot fan van lezen en dan voornamelijk van sciencefiction. Bepaalde boeken of films zouden hen aangezet hebben tot hacken. Daarnaast zouden jonge hackers vaak zelf hun eigen pc hebben gebouwd.

Veel experts hebben het beeld dat cyberdaders zich in hun vrije tijd veel bezighouden met techniek en ICT. Dit betreffen uiteenlopende activiteiten op het gebied van ICT, waaronder veel gamen en websites of fora beheren, maar ook actief zijn op sociale media, veel YouTube-filmpjes kijken of online grafische vormgeving en fotoshoppen. Uit de daderinterviews blijkt echter dat, anders dan de respondenten uit het onderzoek van Chiesa et al. (2009) aangeven, cyberdaders een breed scala aan (ook niet IT-gerelateerde) hobby's hebben, waaronder sporten en muziek (maken). De daderinterviews maken ook duidelijk dat de mate waarin online bezigheden de vrijetijdsbesteding bepalen mogelijk afhangt van de leeftijd van de dader. Degenen die kinderen hebben, geven aan dat tijd spenderen en dingen ondernemen met hun kinderen hun belangrijke tijdsbesteding is. Over deze leeftijdsverschillen is geen informatie teruggevonden in de literatuur. Het algemene beeld is dus dat bij het merendeel van de cyberdaders activiteiten in de ICT en online wereld van jongs af aan een belangrijke interesse vormen, maar dat sommige daders ook andersoortige (offline) vrijetijdsbesteding kunnen hebben. Eventuele veranderingen in vrijetijdsbesteding van cyberdaders over de levensloop zijn in de literatuur nog niet beschreven. De resultaten uit onze daderinterviews geven aan dat deze mogelijk wel aanwezig zijn.

3.4. Gezin- en thuissituatie

3.4.1. Gezinssituatie

Zowel uit de literatuur als uit de expert- en daderinterviews komt naar voren dat de thuissituatie van cyberdaders sterk varieert. Hoewel er geen publicaties zijn gevonden met exacte cijfers, wordt, gezien de lage leeftijd van de dadergroep (zie paragraaf 3.1), aangenomen dat een groot deel van de groep nog in het ouderlijk huis woont (zie ook: Preuß, Furnell & Papadaki, 2007; Sterling, 1993 in Richet, 2013). Verschillende studies beschrijven dat hackers vaak in eenouder- of stiefgezinnen opgroeien (Chantler, 1996, in Lickiewicz, 2013; Chiesa et al., 2007; Kao, Huang & Wang, 2009). Er zijn geen Nederlandse publicaties gevonden met informatie over de gezinssituatie van jonge hackers. De geïnterviewde experts geven aan ervaring te hebben met daders uit diverse gezinstypen (tweeouder, eenouder-, stief- en pleeggezinnen).

Studies naar volwassen daders van cybercriminaliteit in enge zin laten zien dat zij relatief vaak alleenstaand zijn (Lickiewicz, 2013; Rogers, 2001; Weulen Kranenbarg, 2018; Steinmetz, 2015a). Daartegenover staan ook onderzoeken die geen verschillen in relatiestatus vinden bij bachelor studenten (Henson, Zwartz & Reyns, 2017) en in een algemene populatie hackers (Lieberman, 2003, in: Lickiewicz, 2013). De experts vermelden in de interviews dat zij veelal ervaring hebben met studerende cyberdaders. Verschillende keren wordt aangegeven dat deze daders relatief snel uit huis gaan, mogelijk omdat ze met het hacken daarvoor voldoende geld verdienen. Deze vroege zelfstandigheid zou gedeeltelijk de oververtegenwoordiging van alleenstaanden onder de hackers kunnen verklaren. De experts hebben zowel ervaring met hackers die alleenstaand zijn als met hackers die met partner en/of kinderen wonen. Uit de daderinterviews komt niet duidelijk naar voren in welke verhouding dit gebeurt en of dit afwijkt van de populatie traditionele daders.

De door ons geïnterviewde daders zijn opgegroeid in diverse gezinssituaties: zes in een tweeoudergezin, vijf in (vaak afwisselend) een eenouder- of stiefgezin, van drie is de gezinssamenstelling onbekend.

3.4.2. Band met de ouders en ouderlijk toezicht

Verschillende studies besteden aandacht aan het opvoedklimaat tijdens de jeugd. Ouderlijk toezicht en een positieve band met de ouders worden in het algemeen gezien als protectieve factoren voor illegaal hacken. Dit komt naar voren in tal van oudere studies die vaak een beperkte steekproefomvang hebben (o.a. Chiesa et al., 2007; Kao et al., 2009), maar wordt ook gevonden in recentere studies (Kong & Lim, 2012; Low & Espelage, 2013 in Bae, 2017), waaronder een grootschalig onderzoek onder 68.000 middelbare scholieren in 30 verschillende landen (Udris, 2016). Het ouderlijk toezicht op het online gedrag is volgens de experts (OvJ, Medewerker RvK, onderzoekers) en de daders zelf inderdaad beperkt. De daders worden volgens de experts redelijk vrijgelaten door hun ouders en krijgen zo veel gelegenheid om tijd online te spenderen. In sommige gevallen hangt dit ook samen met het feit dat beide ouders fulltime werken, waardoor ze weinig zicht hebben op hoeveel tijd hun kind online spendeert en wat hij/zij daar doet. De ouders controleren te weinig wat hun kind doet of denken dat het kind goede dingen doet achter de computer. Dit komt volgens sommige experts ook omdat veel ouders geen interesse hebben in de digitale wereld[63]. Ze snappen niet hoe alles werkt en haken al af “op het moment dat een kind het heeft over de bits en bytes”. Ook hebben ouders vaak geen weet van wat jeugdigen allemaal bespreken in chatkanalen of op game fora. Andere experts geven aan dat ouders vooral zoekende zijn naar een effectieve manier van begeleiding. Ouders proberen soms wel beperkingen op te leggen (zoals een tijdslot op de computer of het afsluiten van de Wifi) maar de hackers kunnen die gemakkelijk omzeilen. Ook de daderinterviews brengen het beeld naar voren dat het toezicht door de ouders beperkt is. Slechts 3 van de 14 hackers geven aan dat hun ouders beperkingen op hun gedrag probeerden op te leggen, maar in die gevallen werd dit gemakkelijk omzeild volgens de respondenten. Zo vertelt een respondent:

> Op een gegeven moment werd ik ouder, dan trok ze het internet eruit en dan kon ik op het internet van de buren gaan. Of toen had ik wel een UPS batterij achter m’n computer draaien die nog wel een half uur aan stond. Weet je, dan probeerde ze de computers uit te zetten, alle knopjes in te drukken, maar die kabeltjes heb ik ook doorgeknipt. Ze had er gewoon geen zin meer in om ruzie erover te maken. (Daderinterview 9)

3.4.3. Gezinsproblematiek

In verschillende relatief oude publicaties wordt benadrukt dat veel cyberdaders (hackers voornamelijk) uit gezinnen komen met aanzienlijke problemen en een dysfunctioneel opvoedklimaat (Casey, 2002, in Van der Hulst & Neve, 2008; Kao et al., 2009; Verton, 2002 in Morris, 2010). Dit betreft onder andere conflicten tussen de ouders, echtscheiding, alcoholproblematiek bij de ouders en huiselijk geweld. Deze studies beschrijven veelal op basis van kwalitatieve informatie uit interviews of verhoren hoe dergelijke problematiek heeft bijgedragen aan de ontwikkelingen van het illegaal hacken bij de jeugdigen (Kao et al., 2009). Het ontbreken van supervisie op het gedrag, de aanwezigheid van gevoelens van eenzaamheid en emotionele onzekerheid door het ontbreken van aandacht en ondersteuning door de ouders kunnen zich uiten in het stoppen met een reguliere opleiding en een vlucht naar de computer (Siegal, et al., 2003 in Kao et al., 2009). De afwezigheid van betrokken ouders zou bovendien samenhangen met een beperkte ontwikkeling van het moreel kompas (Dennission and Stewart, 2006 in Kao et al., 2009). Verton (2002, in: Yar, 2005) concludeert op basis van interviews met hackers dat het hacken vooral een gevolg is van het gebrek aan een liefdevolle, zorgzame en

[63] Mogelijk is dit afhankelijk van de leeftijd van ouders. Deze factor hebben we in dit onderzoek niet meegenomen.

stabiele familie. Er is echter ook veel kritiek op deze benadering, omdat deviant of afwijkend gedrag verklaard wordt door te kijken naar afwijkingen of 'abnormaliteit' in de persoonlijke en sociale omstandigheden van een individu. Dit wordt ook wel de *pathological falacy* genoemd (Felson, 1998, in Yar, 2005). Hiernaast stelt Fitch (2004, in Yar, 2005) dat hackers niet gezien moeten worden als "vervreemde, angstige tieners" maar als normale tieners die niet veel verschillen van hun *peers*. Het is opvallend dat er geen recente studies gevonden zijn waarin gerapporteerd wordt over de relatie tussen gezinsproblematiek en cybercriminaliteit.

Over de mate waarin er problemen spelen in het gezin waarin hackers zijn opgegroeid lopen de visies en ervaringen van de geïnterviewde experts uiteen. Dit kan deels te maken hebben met het type dader waar zij mee in aanraking komen. Door sommige experts is problematiek in de thuissituatie van hackers geïdentificeerd zoals trauma's of een slechte band met een ouder. Andere experts herkennen dat beeld niet. Een medewerker van de Raad voor de Kinderbescherming (RvdK) onderscheidt een groep daders waarbij sprake is van civiele problematiek zoals trauma's in de gezinssituatie. Dit betreft volgens de expert een groep daders die vrijwel volledig in een online identiteit opgaan. Reclasseringsmedewerkers beschrijven diverse casussen waar sprake was van een slechte band tussen de dader en (een van de) ouders, drugs- en alcoholverslaving of een criminele achtergrond van een ouder (informatie uit focusgroep). Dit beeld sluit aan bij de conclusies van Siegal et al., (2003 in: Yar, 2005) en Verton (2002, in: Yar, 2005) dat het hackgedrag (deels) voort zou komen uit een vlucht naar de computer.

Daarnaast is er een groep experts die stelt dat de cyberdaders uit welgestelde gezinnen komen waar thuis geen problematiek speelt. Zo spreken experts van de RvdK en Halt van respectievelijk keurige gezinnen of modelgezinnen en stelt de Halt-medewerker dat er tussen de zes casussen die zij recentelijk hebben behandeld nauwelijks afwijkende of problematische gezinnen zitten. Alle drie de advocaten stellen dat cyberdaders opgroeien in een normaal gezin met hoogopgeleide ouders die een fatsoenlijke baan hebben en waar de ouders volgens twee advocaten vaak nauw betrokken zijn bij de strafzaak. Het is uiteraard mogelijk dat de zaken waarmee deze advocaten te maken hebben een specifieke selectie betreffen. Ook lijkt het uit te maken om welk type hacker het gaat. Eén van de experts (medewerker RvdK) spreekt van een contrast tussen de minder technisch vaardige hackers en de 'pure whizzkids' die in mindere mate te kampen lijken te hebben met civiele problematiek.

Ook uit de daderinterviews komt een variatie aan gezinsproblematiek naar voren. 3 van de 14 hackers rapporteren dat zij een negatieve band hadden met (een van de) ouders. Drie andere hackers die in wisselende gezinssituaties hebben geleefd of vaak verhuisd zijn, gaven aan dat ze desalniettemin een prima jeugd hebben gehad met een goede band met de ouders. Uit de daderinterviews komt daarmee geen sterke ondersteuning voor het standpunt van Verton (2002, in: Yar, 2005) dat hacken vooral een gevolg zou zijn van het gebrek aan een liefdevolle, zorgzame en stabiele familie.

De systematische literatuurstudie heeft ook studies opgeleverd die laten zien dat betrokken ouders met veel hulpbronnen juist een criminogene factor voor hackgedrag kunnen zijn. Zo laat de kwalitatieve studie van Steinmetz (2015b) zien dat vrijwel alle hackers (12 van de 14 respondenten) technisch georiënteerde ouders hebben. Bovendien geeft een meerderheid van de hackers aan dat de ouders hen openlijk ondersteunden in hun interesse voor de technologie die uiteindelijk tot het hacken heeft geleid. In lijn met de gedachte dat de hulpbronnen van de ouders het hackgedrag juist stimuleren, is de bevinding van Donner, Jennings en Banfield (2015) dat online delictgedrag van middelbare scholieren positief gerelateerd is aan het opleidingsniveau van de ouders. In de expert- en daderinterviews is, zoals hierboven beschreven, naar voren gekomen dat een deel van de hackers uit welgestelde gezinnen komt maar is niet gesproken over concrete aanmoedigingen voor de

technologische ontwikkelingen die tot het hackgedrag leiden. Wel wordt door enkele daders een paar keer genoemd dat hun ouders hen hun gang lieten gaan omdat ze dachten dat ze goede dingen aan het leren waren.

Over de vergelijking van de gezins- of thuissituatie van daders van cybercriminaliteit in enge zijn met daders van traditionele criminaliteit is weinig informatie gevonden. Uiteraard zijn de vermelde stressoren waaronder familieproblemen ook gerelateerd aan traditionele criminaliteit (Booth & Anthony, 2015, in: Bae, 2017). Tevens hangen positieve banden met de ouders samen met minder traditioneel delictgedrag. Daarbij zijn ook het ouderlijk toezicht en uitleg door ouders aan kinderen over de negatieve gevolgen van crimineel gedrag van belang (Harris-McKoy & Cui, 2013; Lippold, Coffman, & Greenberg, 2014; Veronneau & Dfishion, 2010 in Bae, 2017). Het belangrijke verschil lijkt vooral te zitten in de mate van de invloed die ouders kunnen uitoefenen op het gedrag. Deze zou bij cybercriminaliteit minder zijn dan bij traditionele criminaliteit omdat de betrokkenheid bij en controle van kinderen online veel lastiger is dan offline (Udris, 2016). Dit sluit aan bij de inzichten van de experts en daders over de beperkingen waar ouders tegenaan lopen wanneer ze bij hun kinderen grenzen willen aangeven.

Meer in het algemeen hebben de geïnterviewde experts het gevoel dat het verband tussen de gezinsproblematiek en het delictgedrag anders is bij daders van cybercriminaliteit in enge zin dan bij plegers van traditionele criminaliteit. Het meest duidelijk komt dat naar voren in het onderstaande citaat:

> Vanuit de praktijk hebben we al langer het idee dat traditionele criminogene factoren niet per se van toepassing zijn op cybercriminaliteit. Dus de thuissituatie en factoren die voor andere vormen van criminaliteit wel een verhoogd risico opleveren zoals bij de gezinssituatie een compleet of gebroken gezin. (Expertinterview 13, Officier van Justitie)

3.5. Psychologische kenmerken en zelfbeeld

In de literatuur worden diverse psychologische kenmerken aangehaald die daders van cybercriminaliteit in enge zin zouden typeren. Een eerste kenmerk is een hoog IQ (Aiken et al., 2016; Hutchings, 2016). Het onderzoek van Chiesa et al. (2009) onder hackers beschrijft hen als 'briljante' jongeren, die allemaal een bovengemiddeld IQ hebben, veel technische vaardigheden en een groot probleemoplossend vermogen. Daders beschrijven zichzelf ook vaak zo. Daarbij wijzen ze ook op het meer 'out of the box' kunnen denken en handelen (Steinmetz, 2015a; Van der Wagen et al., 2016; Van der Wagen, 2018; Matthijsse, 2017). De experts die wij geïnterviewd hebben, stellen eveneens dat daders van cybercriminaliteit in enge zin over het algemeen intelligent zijn en intellectueel uitgedaagd willen worden. Twee experts spreken zelfs van een bepaalde mate van hoogbegaafdheid bij daders. Enkele experts geven aan dat het uitblinken vaak wel beperkt is tot bepaalde interesses zoals ICT. Verschillende daders die wij hebben gesproken, geven ook aan dat zij zichzelf zien als (super) slim of ('redelijk') intelligent. Ook analytisch en 'out of the box' denkend wordt een paar keer genoemd. Eén van de daders geeft aan dat bij hem een bovengemiddeld IQ is gemeten toen hij jong was en dat hij bijvoorbeeld zonder rekeningmachine hele complexe sommen kan maken.

Een tweede kenmerk dat genoemd wordt in studies over daderschap van cybercriminaliteit in enge zin, is de aanwezigheid van een autismespectrumstoornis (Aiken et al., 2016; Ledingham & Mills, 2015; Schell & Dodge, 2002, in Ledingham & Mills, 2015; Seigfried-Spellar, O'Quinn & Treadway, 2015) Empirisch bewijs voor de aanwezigheid van een autismespectrumstoornis (ASS) op grote schaal in deze groep daders wordt echter niet geleverd. Verschillende experts veronderstellen, op basis van

hun contact met cyberdaders, ook dat sommige cyberdaders in mindere of meerdere mate autistiforme trekken hebben, wat overigens niet per definitie als iets problematisch wordt gezien. Het gaat bijvoorbeeld om wegkijken, een specifieke blik in de ogen, in de eigen wereld zitten, moeite met communiceren hebben en het niet goed kunnen praten over gevoelens of alledaagse menselijke dingen (wel over de techniek). Een van de politie-experts geeft de volgende beschrijving van een casus waar hij nauw bij betrokken was:

> Vroeg ik hem naar een technisch iets of wat dan ook, dan begon hij enthousiast te kletsen en bleef maar ratelen. Dat is het probleem niet. Dan zag je hem gewoon opleven en zag je het enthousiasme in zijn ogen en dan begon die. [….] Naar zichzelf […] kijken van wat ben ik nu eigenlijk aan het doen en wat zijn de gevolgen daarvan en wat vinden anderen daarvan, die denkslagen die kwamen er niet. Als je hem hielp, dan kwam hij er uiteindelijk wel. (Expertinterview 28, Politie)

Als het gaat om autistiforme trekken signaleren twee experts dat er overeenkomsten bestaan tussen het psychologische profiel van cyberdaders en zedendaders. Daarbij gaat het vooral om aspecten zoals het in de eigen wereld zitten en weinig communiceren met mensen in de directe omgeving. Naast een ASS, waaronder het syndroom van Asperger, gaat het dan om diagnoses zoals ADD, ADHD, een aanpassingsstoornis, borderline, angstklachten of waanbeelden. Op basis van de expertinterviews kunnen echter geen uitspraken worden gedaan over aantallen en de exacte inhoud van de diagnoses. Hetzelfde geldt voor de daderinterviews. Dit thema is niet expliciet besproken met de daders, maar soms zeiden ze er iets over uit zichzelf. Zo vertelt een respondent dat hij denkt autistische trekjes te hebben:

> Ik vind sociaal contact heel leuk, je zou wel misschien kunnen zeggen dat ik bepaalde autistische trekjes heb zeg maar, dat het moeilijk voelt zeg maar om sociaal contact [te hebben], bijvoorbeeld van nieuwe mensen daar contact mee te leggen. Maar ik voel me totaal niet alleen of afgezonderd of iets in die richting. (Daderinterview 10)

Voor dit kenmerk en het hierop volgende zal de (zelf)selectie in de dadergroep die we hebben gesproken mogelijk een belangrijk vertekenend effect hebben, omdat daders met de in de literatuur beschreven eigenschappen zoals sociale isolatie of autistiforme trekken waarschijnlijk minder bereid zijn om geïnterviewd te worden.

Een derde kenmerk dat genoemd wordt in de literatuur en dat ook al in bovenstaand citaat herkend kan worden, is dat cyberdaders in enge zin vaak enigszins kwetsbaar, sociaal onhandig en teruggetrokken (Aiken et al., 2016) of introvert zijn (Rogers, Smoak & Liu, 2006). Dit kenmerk wordt ook in de beschrijving van diverse experts benadrukt, waarbij ook vaak benadrukt wordt dat daders in een sociaal isolement zitten, niet populair op school zijn en een verstoord nachtritme hebben (zie ook hoofdstuk 6).

Verschillende daders die we hebben gesproken geven nadrukkelijk aan dat bovengenoemd stereotype niet op hen persoonlijk van toepassing is, maar mogelijk wel op anderen om hen heen. Ook hierin kan de selectie van geïnterviewde daders weer een rol spelen. Ze beschrijven het stereotype van de cyberdader of de hacker als volgt: “nerds”, “zonder vrienden”, “met capuchon”, “niet-sociaal”, “introvert”, “autistisch”, “ingekeerd zijn”, “alleen maar de hele dag over het toetsenbordje heen gebogen zitten”, met “puisten of overgewicht”. Verschillende daders beschrijven zichzelf qua sociale

vaardigheden en sociaal contact als een sociaal persoon. Twee daders geven daarbij aan dat ze niet heel actief contact opzoeken of *heel* sociaal zijn, maar sociaal contact ook zeker niet ontwijken. Zo stelt een van hen:

> Ik haat het om te alleen te zijn zeg maar, dus ik heb het liefst gewoon sociaal contact met anderen. Ik bedoel ik vind het wel fijn om een paar uurtjes per dag gewoon lekker voor jezelf te hebben, maar niet meer dan dat zeg maar. Ik ben niet iemand die zich hele dagen kan terugtrekken en dan met niemand contact heeft. (Daderinterview 6)

Slechts een dader geeft aan een min of meer solistisch bestaan te leiden (met ook een zeer laat dag- en nachtritme), wat naar eigen zeggen een bewuste keuze is. Hij distantieert zichzelf ook van bovenstaand stereotype, omdat hij heel open is en graag met mensen praat en mensen helpt. Daarbij geeft hij wel aan dat hij er totaal niet van houdt om over huisje, boompje beestje-gerelateerde dingen te praten. Liever praat hij over ICT-gerelateerde onderwerpen. Een andere dader geeft aan dat hij tijdens de periode op de middelbare school (de periode dat hij hackte) erg verlegen en een beetje 'een loner' was, maar dat dit over de tijd heen veranderd is.

Ook wordt in de literatuur stilgestaan bij psychologische factoren die juist *niet* zo'n prominente rol spelen bij daders van cybercriminaliteit in enge zin. Hierbij gaat het bijvoorbeeld om de rol van (lage) zelfcontrole (Weulen Kranenbarg, 2018; Holt, Bossler & May, 2012; Nodeland & Morris, 2018). De zelfcontroletheorie gaat er vanuit dat mensen met een lage zelfcontrole impulsief zijn, een korte termijn focus hebben en sneller risico's nemen waardoor zij minder goed de verleiding kunnen weerstaan om criminaliteit te plegen (Gottfredson & Hirschi, 1990). Als het specifiek gaat om daders van cybercriminaliteit in enge zin wordt door sommige auteurs verondersteld dat een lage zelfcontrole als criminogene factor niet aan de orde is, omdat delicten zoals hacken juist veel zelfcontrole en geduld vereisen (Bossler & Burruss, 2011; Weulen Kranenbarg, 2018) zowel als het gaat om de uitvoering als het verbergen van sporen. Voor delicten zoals het uitvoeren van een DDoS-aanval ligt dit mogelijk anders, want dit kan middels enkele muisklikken gerealiseerd worden. De rol van een lage zelfcontrole is niet veelvuldig aan de orde gekomen in de expertinterviews. Wel verwijzen experts naar impulsief handelen, wat ze soms ook aan de leeftijd/adolescentie relateren.

Enkele daders brengen zelf wel aspecten naar voren die gerelateerd kunnen zijn aan een (lage) zelfcontrole, zoals impulsief handelen, het maken van verkeerde keuzes, gericht zijn op de korte termijn en verslavingsgevoeligheid. Er zijn ook daders die aspecten vermelden waar juist het tegendeel uit blijkt, zoals lange termijn doelen stellen, discipline hebben en perfectionistisch zijn. Er is geen literatuur gevonden waarin de psychologische en persoonlijkheidskenmerken van daders van cyberdelicten direct worden vergeleken met de kenmerken van daders van traditionele delicten. Wel beschrijft de literatuur een duidelijke oververtegenwoordiging bij daders van traditionele criminaliteit van de volgende kenmerken: licht verstandelijke beperking (Kaal, 2016; Popma & Doreleijers, 2019), problemen in de executieve functies (zoals plannen, impulscontrole en bijstellen van een plan als dat nodig is) (Ogilvie, Stewart, Chan & Shum, 2011) en problemen in de sociale informatieverwerking (Schuiringa, et al., 2017). Mensen met (alleen) een ASS zijn niet oververtegenwoordigd of volgens sommige studies zelfs ondervertegenwoordigd in de groep daders van traditionele criminaliteit (Heeramun, Magnusson, Cumpert, Granath, Lundberg, Dalman & Rai, 2017; King & Murphy, 2014).

Op grond van de literatuur en interviews kan dus met enige zekerheid gesteld worden dat er binnen de groep daders van cyberdelicten in enge zin een oververtegenwoordiging is van personen met kenmerken uit een ASS. Er zijn aanwijzingen dat zelfcontrole en verstandelijk vermogen onder

cyberdaders hoger is dan gemiddeld, zeker wanneer dit vergeleken wordt met daders van veel vormen van traditionele criminaliteit. Daarbij bestaan er net als bij traditionele criminaliteit grote verschillen tussen daders van verschillende vormen van cybercriminaliteit. Voor de meer technisch geavanceerde delicten (zoals hacken) hebben daders een hogere intelligentie en meer zelfcontrole nodig dan voor andere cyberdelicten (zoals het uitvoeren van DDoS-aanvallen).

3.6. Sociale contacten (online en offline)

Het hebben van delinquente vrienden wordt doorgaans beschouwd als een belangrijke criminogene factor voor het plegen van criminaliteit (Rokven, de Boer, Tolsma & Ruiter, 2017; Weerman, 2011; Paternoster, McGloin, Nguyen & Thomas, 2012), omdat individuen gedrag aanleren door het observeren en imiteren van gedrag van anderen (Hutchings, 2014; Rokven, de Boer, Tolsma & Ruiter, 2017). Ook in studies op het gebied van cybercriminaliteit in enge zin wordt gewezen op de rol van (delinquente) vrienden (Weulen Kranenbarg, 2018; Hutchings, 2014; Rokven, Weijters & van der Laan, 2017). In een onderzoek van Weulen Kranenbarg (2018) aan de hand van surveydata is gebleken dat er een verband is tussen het delinquente gedrag van een individu en dat van sociale netwerkleden, maar dit verband is minder sterk bij cybercriminaliteit dan bij traditionele criminaliteit. Tevens is gebleken dat het verband sterker is voor zowel cybercriminaliteit als traditionele criminaliteit wanneer er sprake is van dagelijks contact en de respondent en het sociale netwerklid hetzelfde geslacht hebben (Weulen Kranenbarg, 2018). Tot slot is gebleken dat oudere rolmodellen belangrijker zijn bij daders van cybercriminaliteit, terwijl dit bij traditionele criminaliteit juist netwerkleden van dezelfde leeftijd zijn.

Zoals in de vorige sectie aan de orde kwam, wordt er zowel in de literatuur als door de experts vanuit gegaan dat cyberdaders überhaupt weinig offline vrienden hebben en juist aangewezen zijn op online *peers* (Aiken et al., 2016). Een deel van de cyberdaders wordt omschreven als sociaal geïsoleerd, introvert en als loners (Chiesa et al., 2009; Aiken et al., 2016; Kao et al., 2009). Als ze al offline vrienden hebben, dan is dat vaak een klein aantal (Zebel et al., 2013). De geïnterviewde daders voldoen maar gedeeltelijk aan dat beeld maar dat kan wederom met de selectieve samenstelling van de groep te maken hebben en mogelijk ook met het feit dat ze geen negatief beeld over zichzelf willen schetsen. Hoewel sommige respondenten spreken van periodes in hun leven waarin ze eenzaamheid ervoeren en weinig tot geen vrienden hadden, geven veel respondenten ook aan één of meerdere (offline) vrienden te hebben waar ze op frequente basis mee afspreken of mee 'chillen.' Daarbij wordt onder meer gewezen op uitgaan, samen gamen, rondhangen en samen blowen. Verschillende daders geven overigens wel aan vrienden kwijt te zijn geraakt door hun strafzaak.

Hoewel de literatuur beschrijft dat cyberdaders geen groot *offline* sociaal leven hebben, benadrukken veel studies over daderschap van cybercriminaliteit in enge zin het belang van *online* vrienden (Woo, Kim & Dominick, 2004). Rogers (2010) benadrukt dat cyberdaders goed kunnen communiceren via computers en goed in staat zijn om online relaties op te bouwen. Hoewel sommige relaties oppervlakkig zijn (Holt, 2005; Chiesa et al., 2009), zijn er ook studies die wijzen op een mentor-student relatie (Chiesa et al., 2009; Nycyk, 2016; Steinmetz, 2015a), hechte vriendschappen en zelfs romantische relaties (Goode & Cruise, 2006; Levin, Richardson, Warner & Kerley, 2012; Rogers, 2010), waarbij de vriendschap ook om meer kan gaan dan de gemeenschappelijke interesse in ICT (Goode & Cruise, 2006). Volgens Rogers (2010) functioneren veel Internet Relay Chats[64] bijvoorbeeld als een virtueel café en beschrijft Steinmetz (2015a) de online hacker community als een gilde. De literatuur

[64] Dit betreft een online chatsysteem.

benadrukt tevens dat veel van deze online relaties voortduren zonder dat de individuen elkaar in de offline wereld zien, al gebeurt dit soms wel, bijvoorbeeld op conferenties zoals DEFCON (Rogers, 2010). Op basis van deze studies kan geconcludeerd worden dat het niet zondermeer juist is te spreken van loners of einzelgängers.

De bevindingen uit de literatuur worden (deels) ondersteund door de expertinterviews. Veel experts geven aan dat cyberdaders online een groter sociaal netwerk lijken te hebben dan offline. De vraag is in hoeverre de contacten binnen dit netwerk anders van aard zijn dan offline contacten. Mogelijk draait het sociale contact vooral om kennis uitwisselen en van elkaar leren binnen het sociale netwerk. Veel van de cyberdaders, aldus de experts, zien hun online contacten wel echt als vrienden. Eén expert stelt bijvoorbeeld dat toen een jongere gevraagd werd naar zijn sociale netwerk, hij reageerde met 'joh, ik heb zoveel vrienden'. Wanneer dit nagelopen werd, bleek er sprake te zijn van een handjevol mensen omdat veel van de contacten online plaatsvinden, zoals ook uit de literatuur is gebleken. Hoewel er soms fysieke bijeenkomsten plaatsvinden met online vrienden, zijn er volgens de experts ook veel cyberdaders die hun online sociale netwerk nog nooit in het echt hebben ontmoet. Ook de daders beamen dat zij online contacten beschouwen als vrienden. Meerdere respondenten (N= 5) beschrijven dat ze online vrienden bijvoorbeeld via fora of via het spelen van games hebben ontmoet. Sommigen van hen hebben deze vrienden ook in de offline wereld ontmoet.

Daarnaast zijn er volgens de experts ook daders die hun online sociale contacten juist *niet* als vrienden beschouwen. Bij deze daders lijkt het online sociale netwerk meer in het teken te staan van het plegen van criminaliteit en het eventueel benaderen van mogelijke medeplegers. Een Halt-medewerker beschrijft bijvoorbeeld hoe een cliënt de andere forumgebruikers niet per se vrienden noemde, ook al sprak hij hen elke dag en wisselden ze informatie en scripts uit. Dit zien we ook terugkomen in enkele daderinterviews. Zo geeft een respondent aan online netwerkleden alleen als vrienden te zien als hij ze via school of via anderen heeft leren kennen. Hij beschrijft dat hij op het internet terughoudend is en de voorkeur geeft aan face-to-face contact boven appen of chatten, omdat je online geen gezichten of emoties kunt zien.

Enkele respondenten maken een expliciet onderscheid tussen online en offline vrienden (en spreken ook zelf van 'offline' en 'online' vrienden), een aspect dat ook in eerdere studies naar voren is gekomen (Van der Wagen et al., 2016). Dat betekent niet dat offline vrienden helemaal los staan van de online activiteiten of hier helemaal geen weet van hebben. De jongeren die Hoek van Dijke (2016) heeft geïnterviewd gaven aan dat sommige vrienden wel op de hoogte waren van hun hackactiviteiten, maar dat ze geen details verstrekten. Soms laten ze vrienden wel wat zien, maar dan doen ze dat vooral in de beginfase. Daarna wordt het steeds anoniemer en steeds onzichtbaarder. Ook enkele van de door ons gesproken daders geven dit aan. Zo stelt een van de respondenten dat hij in het begin wel open was naar vrienden toe op de middelbare school als het ging om hacken:

> Ik was er wel open over. Ik wilde juist dat ze het ook gingen doen, want ik vond het cool. En als ik ergens enthousiast over was had ik zoiets van dan maak ik jullie ook enthousiast. Mensen vroegen zich af, is het dan moeilijk dat hacken of dit of dat. En het was ook wel een manier om ook even te laten zien van nou ja zo overdreven moeilijk is het nou ook weer niet. (Daderinterview 4)

Samenvattend blijkt uit de bovenstaande paragraaf dat de offline netwerken bij daders van cybercriminaliteit vaak kleiner zijn dan bij traditionele daders en veel minder invloed op het delictgedrag hebben. Daarbij varieert het over de groep cyberdaders in hoeverre leden uit het online

netwerk ook als vrienden worden beschouwd. Over de invloed van het online netwerk op het delictgedrag hebben we geen onderzoek gevonden. Wel wordt duidelijk dat binnen het online netwerk kennis en scripts worden uitgewisseld die indirect tot delicten kunnen leiden, of dat contact wordt gelegd met toekomstige medeplegers. Uit de literatuur komt tot slot naar voren dat bij cyberdaders oudere rolmodellen belangrijker zijn voor het eigen gedrag terwijl bij traditionele criminaliteit leeftijdsgenoten het belangrijkst zijn.

3.7. Conclusie

In dit hoofdstuk is stilgestaan bij de demografische, sociaaleconomische, psychologische en gezinsgerelateerde kenmerken van cyberdaders, evenals hun vrijetijdbesteding en sociale contacten. Uit de literatuur is gebleken dat cybercriminaliteit in enge zin relatief vaker wordt gepleegd door jonge autochtone mannen met een redelijk tot goede sociaaleconomische achtergrond. Bij de subgroep financieel georiënteerde daders van cybercriminaliteit in enge zin ligt de leeftijd waarop gestart wordt met het plegen van cybercriminaliteit doorgaans hoger, lijkt vaker sprake te zijn van allochtone daders en zijn er indicaties voor een lagere sociaaleconomische status.

Hoewel het opleidingsniveau bij cyberdaders varieert, lijkt sprake te zijn van een relatief hoger intelligentie- en opleidingsniveau in vergelijking met traditionele daders. Soms maken daders hun opleiding niet af, wat niet automatisch betekent dat zij in laaggeschoold werk terechtkomen. Het werk en de opleiding die cyberdaders doen of hebben gedaan varieert, maar opleidingen en banen in de IT-sector zijn oververtegenwoordigd. In hun vrije tijd houden cyberdaders zich veel bezig met techniek, ICT, gamen en sociale media. Hiernaast hebben ze echter ook een breed scala aan andere hobby's.

De thuissituatie (o.a. de rol van gezinsproblematiek) varieert sterk. Er blijkt vaak een gebrek aan ouderlijk toezicht op het online gedrag van cyberdaders te zijn, zowel in gezinnen met als zonder gezinsproblematiek. Dit beperkte toezicht wordt mede veroorzaakt door gebrekkige kennis van ouders van het internet en de online wereld. Tot slot kunnen de cyberdaders gekenmerkt worden als intelligent met vaker dan bij traditionele daders de aanwezigheid van kenmerken uit een autismespectrumstoornis (ASS) en een sterk probleemoplossend vermogen. Tevens suggereren de bevindingen dat er een tweedeling waarneembaar is tussen de cyberdaders die een lagere zelfcontrole ervaren en impulsief zijn en daders die juist lange termijn doelen stellen en perfectionistisch zijn. Sommige daders kunnen volgens de literatuur en de experts gekenmerkt worden als introvert of sociaal onhandig, maar een ander deel (waar veel van de door ons geïnterviewde cyberdaders zichzelf onder scharen) is voldoende sociaal vaardig. Waar de meeste cyberdaders online een sociaal netwerk hebben opgebouwd lijkt het offline netwerk relatief kleiner te zijn en minder van invloed te zijn op het delictgedrag.

Hoofdstuk 4 Drijfveren en beleving

In de literatuur worden veel verschillende drijfveren aangehaald voor daderschap van cybercriminaliteit in enge zin. Het motief wordt in de literatuur vaak als een onderscheidend kenmerk gebruikt om verschillende soorten daders te clusteren.[65] Hierbij gaat het voor een groot deel over de motieven van hackers. Een van de meest bekende classificaties[66] in dit kader is het onderscheid tussen *black*, *white* en *grey* hat hackers (o.a. Chiesa et al., 2009; Nyciek, 2016). *Black hat* hackers worden gedefinieerd als hackers die illegaal systemen binnendringen en een criminele intentie hebben. *Grey hat* hackers zijn hackers die niet als black of white gelabeld willen worden en/of op de grens opereren. *White hat* hackers zijn hackers die wel dezelfde vaardigheden hebben als black hat hackers, maar deze voor legale doelen inzetten (Chiesa et al., 2009, pp. 72-73).[67] Ook zijn er studies te vinden die binnen een groter veld van cybercriminaliteit verschillende subgroepen cyberdaders onderscheiden met bijbehorende motieven (o.a. Brar & Kumar, 2018; Leukfeldt, Domenie & Stol, 2010; Van der Hulst & Neve, 2008; Weulen Kranenbarg, 2018). Zoals reeds aangegeven in hoofdstuk 1 beogen we in dit onderzoek daders niet enkel op basis van motieven in te delen, mede omdat, zoals ook uit onderstaande zal blijken, vaak meerdere motieven tegelijkertijd een rol spelen en ook omdat ze veranderlijk zijn. Wel beogen we in dit hoofdstuk om op basis van de literatuur, expert- en daderinterviews in kaart te brengen wat de belangrijkste drijfveren zijn van cyberdaders en hoe zij het plegen van cyberdelicten beleven. Ook wordt bij ieder cluster van motieven ingegaan op de vraag in hoeverre en op welke wijze deze motieven ook een rol spelen bij traditionele daders.

4.1. Nieuwsgierigheid, leergierigheid en (mentale) uitdaging

Nieuwsgierigheid, leergierigheid en (mentale) uitdaging, motieven die sterk met elkaar verbonden lijken te zijn, zijn motieven die voornamelijk in studies over (jeugdige en volwassen) hackers worden genoemd (Chiesa et al, 2009; Steinmetz, 2015a; Van der Wagen, 2018). Zo heeft maar liefst 30% van de respondenten in de studie van Chiesa et al. (2009) aangegeven te hacken vanwege nieuwsgierigheid: het willen exploreren van systemen en het ontdekken van geheimen. Ook voor daders die zich bezighouden met het distribueren van malware geldt dat nieuwsgierigheid een belangrijk motief is (Weulen Kranenbarg, 2018). De nieuwsgierigheid lijkt voor een groot deel betrekking te hebben op wat er allemaal mogelijk is met de technologie, dus wat ervoor zorgt dat het systeem wel of juist niet werkt (Steinmetz, 2015a; Van der Wagen, 2018). Mogelijk ligt dit wel anders voor verschillende soorten hackers. Waar scriptkiddies, beginnende hackers, vooral nieuwsgierig zijn

[65] Andere kenmerken die worden gebruikt om daders te clusteren zijn bijvoorbeeld vaardigheden, het gebruik van tools, modus operandi, *threat properties* (dit zijn de intenties, triggers, vaardigheden, hulpbronnen en methoden die bij het hacken horen) (Hald & Pedersen, 2012) of individuele kenmerken zoals leeftijd of persoonlijkheidskenmerken (Seigfried-Spellar & Treadway, 2014).

[66] Een andere bekende typologie is die van Rogers (2006). Hij onderscheidt negen categorieën hackers en heeft deze onderverdeeld in verschillende subcategorieën. De goedwillende hackers worden aangeduid als *old guard* hackers. De kwaadwillende hackers (waar volgens hem het minst over bekend is) zijn de 'professional criminals' en de *information warriors*. Laatstgenoemde zijn voormalige *intelligence agents* die gespecialiseerd zijn in spionage. De meelopers zijn de *novices* en de overige hackers vallen volgens Rogers in tussencategorieën.

[67] Het feit dat lang niet alle hackers zich met het binnendringen van systemen bezighouden en bijvoorbeeld hacken uit ethische overwegingen (Steinmetz, 2015a; Best, 2006), maakt het dan ook lastig om alle hackers per definitie te scharen onder het begrip cyberdader of dader.

over wat je met bepaalde (bestaande) tools kunt bereiken, willen de meer ervaren hackers alle ins en outs leren van systemen en ook (deels) zelf tools maken of aanpassen (zie verder hoofdstuk 6). Nieuwsgierigheid gaat ook hand in hand met leergierigheid. Verschillende studies geven aan dat (*black* en *white hat*) hackers ijverig zijn om nieuwe dingen te leren. Leren is dan niet alleen een middel, maar ook een doel op zichzelf (Steinmetz, 2015a; Van der Wagen, 2018). Turgeman-Goldschmidt (2005) definieert dit als "*curiosity for its own sake*" (p.13). Uit de studie van Weulen Kranenbarg (2018) blijkt dat leren of educatie als motief niet alleen bij hacken en gerelateerde delicten zoals *web defacen* voorkomt, maar ook bij phishing.

De experts zien nieuwsgierigheid en het willen leren hoe systemen werken ook als een veelvoorkomend motief bij cyberdaders, maar veronderstellen dat dit motief vooral centraal staat bij jeugdige cyberdaders. Deze (jonge) daders hebben, zoals een expert het verwoordt, een zekere 'verkenningsdrift'. Ze willen ontdekken hoe ver ze kunnen gaan met de techniek en kijken wat er allemaal mogelijk is. Ook verschillende daders (N=8) hebben aangegeven dat ze gedreven werden door nieuwsgierigheid: "kijken of en hoe het werkt of juist niet werkt", zonder per se een specifiek doel voor ogen te hebben. Ze wilden bijvoorbeeld weten hoe een systeem in elkaar zit door het eerst kapot te maken en daarna weer te installeren of wilden exploreren of en hoe ze informatie kunnen verkrijgen die ze niet zouden mogen verkrijgen. Waar die nieuwgierigheid vandaan komt, vinden de respondenten lastig te zeggen. Sommige respondenten beschouwen de nieuwsgierigheid als iets dat ze van nature bezitten. Ze kunnen het bijvoorbeeld niet uitstaan als ze niet weten hoe iets werkt en gaan net zo lang door tot ze het wel weten.

Ook de daders die (ook) aangeven een financieel motief te hebben gehad, geven aan dat het leren en het willen ontdekken van de ins en outs van informatietechniek een hele belangrijke drijfveer is. Een respondent die een tijdje bij creditcardfraude betrokken is geweest (naast ook andere delicten), wilde graag weten hoe het frauderen met creditcards in zijn werk gaat, omdat het volgens hem *ook* deel uitmaakt van informatietechniek. Naar eigen zeggen raakte hij hier snel op uitgekeken en is hij weer overgestapt naar de 'wereld van hacken'.

Nieuwsgierigheid en leergierigheid gaan, zo blijkt uit verschillende studies, voor sommige daders ook gepaard met een zekere mentale uitdaging (Dalal & Sharma, 2007; Holt & Kilger, 2008; Schell & Melnychuk, 2010; Van der Wagen, 2018). Hackers houden van de intellectuele uitdaging om de mogelijkheden en beperkingen van de techniek te beheersen (Bachmann, 2010). Men wil het systeem als het ware meester worden (Steinmetz, 2015a; Van der Wagen, 2018), een aspect dat ook een relatie lijkt te hebben met motieven als macht (zie verder paragraaf 4.3). Floyd, Harrington en Hivale (2007) spreken van een *autelic high* die gepaard gaat met hacken. Hier wordt onder verstaan dat hacken voor hackers een soort van mentale gymnastiek is en een activiteit is waar ze helemaal in op kunnen gaan. Volgens Taylor (1999, in Chiesa et al., 2009) kunnen hackers zo betrokken zijn bij het hacken dat ze niet een bepaald doel voor ogen hebben. Ze hacken als het ware om te hacken. Door deze intrinsieke motivatie kunnen grenzen ook gemakkelijk overschreden worden (Ryan & Deci, 2000).

Ook verschillende experts hebben gewezen op het belang van uitdaging. Sommige experts (N=5) evenals enkele daders (N=6) spreken in dit verband van hacken als een spel of (een leukere variant van een) puzzel. Een expert beschrijft dat het in de virtuele wereld een spel is om zo snel mogelijk de kwetsbaarheid te vinden zodat je sneller en slimmer bent dan de eigenaar van het systeem én de andere hackers. Dit competitieve element wordt ook door een dader naar voren gebracht:

> Ik heb ook wel momenten gehad dat het echt een soort gevecht was, wie het snelste was. Dat je een website aan het hacken was en dat die persoon erachter door heeft dat je aan het

> hacken bent…Ik was dan allemaal backdoors aan het plaatsen en dan zie ik ze een voor een verdwijnen, en dan snel op een andere gaan. Dan is het een soort gevecht, wie kan het snelste dit doen. (Daderinterview 8)

Als het hem dan lukte om binnen te dringen, beschouwde hij dit als een 'trofee' en gaf dit hem een kick. De mentale uitdaging lijkt daarmee niet alleen te gaan over de mogelijkheden van de techniek, maar ook over de eigen capaciteiten. Hackers willen graag hun eigen kunnen, hun persoonlijke mogelijkheden en beperkingen op de proef stellen (Van der Wagen, 2018). Aiken et al. (2016, p. 16) spreken in deze context van het belang van *self-challenge.*

Ook andere daders vermelden de uitdaging expliciet als een drijfveer, soms als een primair motief en soms in combinatie met andere motieven. Volgens hen is het ontdekken van hoe systemen te hacken of te misbruiken zijn en te leren welke trucjes je daarvoor kunt toepassen, leuk, fascinerend en vooral uitdagend. Sommige respondenten geven aan dagelijks met 'dit soort gedachten' rond te lopen en dat ze zich bij alles wat ze tegenkomen afvragen hoe het te misbruiken is. Dit hoeft zich niet alleen te beperken tot computersystemen of websites. Zo heeft een respondent verteld dat hij een klassieke winkeldiefstal ook zeer uitdagend zou vinden. Hij zou het superleuk vinden om de opdracht te krijgen van een winkeleigenaar om bij de winkel in te breken en dus de beveiliging te kraken (zonder consequenties uiteraard). Verschillende daders voor wie de uitdaging een belangrijke drijfveer is, geven aan dat je ook steeds op zoek bent naar nieuwe uitdagingen. Als situaties steeds hetzelfde zouden zijn of indien je steeds dezelfde stappen zou moeten zetten om kwetsbaarheden te ontdekken of systemen te misbruiken, dan wordt het saai. De factor uitdaging lijkt dan ook een rol te spelen bij de duur en het verloop van de criminele carrière van de dader. Als er geen uitdaging meer is, dan zal de dader mogelijk sneller stoppen of zich juist gaan storten op een andere, moeilijkere soort hack of een ander soort cyberdelict (zie verder hoofdstuk 6).

Of de drijfveren nieuwsgierigheid, leergierigheid en (mentale) uitdaging typische motieven zijn voor cyberdaders, hackers in het bijzonder, is een interessant discussiepunt. Verondersteld kan worden dat sommige daders van traditionele misdrijven, bijvoorbeeld dieven of overvallers, ook nieuwsgierig kunnen zijn en dingen willen leren (bijvoorbeeld hoe je sloten op innovatieve manieren kunt openbreken). Niet voor niets trok een van de daders een gelijkenis met een winkeldiefstal. Ook daar zit mogelijk een aspect van (mentale) uitdaging bij (zie bijvoorbeeld de studie van Kroese en Staring, 1993 over overvallers). Weulen Kranenbarg (2018), een van de weinige studies die expliciet een vergelijking trekt tussen cyberdaders en traditionele daders, concludeert echter dat nieuwsgierigheid (samen met de motieven verveling en opwinding) vaker voorkomt bij cybercriminaliteit dan bij traditionele criminaliteit, vooral in vergelijking met witteboordencriminelen en in mindere mate in vergelijking met delicten zoals vandalisme, overvallen, diefstal of geweld. Ook de drijfveren educatie en uitdaging zijn volgens haar meer prevalent bij daders van de meeste cyberdelicten dan bij daders van traditionele criminaliteit.

Daarnaast is het de vraag of de drijfveer op dezelfde wijze een rol speelt c.q. dezelfde invulling krijgt. Zo lijkt het leren bij de meer traditionele (vermogens)delicten vooral een instrumentele rol te hebben, terwijl bij hacken het leren ook een drijfveer op zichzelf kan zijn (intrinsieke motivatie). Sommige hackers halen al voldoening uit het leren zelf. Mogelijk hangt dit samen met de aard van cyberdelicten. De mogelijkheden zijn eindeloos en er valt heel veel te leren, te experimenteren en te groeien. Wellicht speelt ook de intelligentie van de dader een rol. Zoals reeds naar voren is gekomen, zijn cyberdaders over het algemeen hoger opgeleid (en dus mogelijk educatiever ingesteld dan

traditionele daders). Als dat niet het geval is, zijn ze vaak wel specifiek geïnteresseerd en vaardig in de IT en willen ze daar alles over leren.

4.2. Kick, spanning, plezier en verveling

Diverse studies wijzen op de kick, spanning en/of plezier als belangrijke drijfveren voor daders van cybercriminaliteit in enge zin (Bachmann, 2010; Hoek van Dijke, 2016; Steinmetz, 2015a; Van der Wagen, 2018; Weulen Kranenbarg, 2018). Volgens Turgeman-Goldschmidt (2005) ervaren hackers gevoelens van sensatie, spanning, mysterie en adrenaline, wat het hacken zo verleidelijk maakt. Ook het gevoel dat je een systeem binnenkomt en informatie te zien krijgt die je niet mag zien kan een kick genereren (Van der Wagen, 2018). Hoek van Dijke (2016) geeft aan dat ook het gevoel van 'het is me gelukt' gepaard gaat met de kick, waarmee de kick niet helemaal los lijkt te staan van andere motieven zoals de hiervoor besproken (mentale) uitdaging. Steinmetz, Schaefer & Green (2017) beschrijven dat hackers een emotionele sensatie ervaren nadat het hen (na veel moeite en frustratie) lukt om een systeem te hacken. Ze krijgen een *reward* als de hack uiteindelijk slaagt, een soort emotionele *payoff*. De auteurs refereren in dit kader naar de rol van *flow*, een psychologisch proces waar iemand helemaal opgaat of ontsnapt in hetgeen hij/zij doet en ook geen perceptie meer heeft van tijd en plaats. Een cybersecurityexpert geeft in dit kader aan dat de moeilijkheidsgraad een versterkend effect heeft: hoe lastiger het systeem te hacken is, hoe groter de kick en hoe langer de puzzel duurt, hoe meer euforie de dader ervaart als het uiteindelijk lukt. Ook andere experts wijzen op het belang van de kick, die zowel een rol speelt tijdens het plegen van het delict als op het moment dat de dader zijn doelen heeft bereikt en ermee wegkomt. Ook enkele daders (N= 5) brengen de spanning en kick naar voren als het gaat om hun drijfveren, die zij voornamelijk ervaren bij een geslaagde hack. Daarnaast wordt er op gewezen dat het illegale karakter of de media-aandacht nog een extra kick of dimensie kan geven. Zo stelt een van de daders dat hij, nu hij op legale wijze penetratietesten uitvoert, niet of nauwelijks een kick ervaart terwijl wat hij feitelijk doet hetzelfde is:

> Hoe ik het nu doe is allemaal legaal, dus ja, van te voren wordt er iets getekend dat ik alles mag doen en het maakt eigenlijk niet uit of ik wel of niet iets vind, ik krijg toch wel betaald, weet je wel. En als ik iets vind, is er niet iemand die mij gaat stoppen en als ik iets vind kan ik niet de database gaan downloaden weet je wel. Dus het is wel, het is wel anders. Toen ik het illegaal deed zat er nog een kick achter, was er inderdaad die reward. Maar nu is het gewoon mijn werk. (Daderinterview 8)

Het feit dat deze dader aangeeft dat het hacken hem meer voldoening gaf toen hij het illegaal deed, is mogelijk gerelateerd aan de inzichten van Katz (1988) over het belang van de *sneaky thrill* bij daderschap. Dit verwijst naar de aanname dat juist het verboden karakter van criminaliteit het verleidelijk maakt om te doen, wat Katz onder andere terugzag bij overvallers. Ook in bestaande studies over hackers wordt naar dit aspect verwezen (Steinmetz, 2015a; Van der Wagen, 2018; Steinmetz et al., 2017). Zo stelt Steinmetz (2015a) dat sommige hackers spanning opzoeken en afstand willen nemen van het 'alledaagse' en 'veilige' gebruik van ICT. Er kan zelfs een verslavende werking vanuit gaan, een aspect dat ook door enkele experts naar voren wordt gebracht. Niet alleen verslaafd zijn aan hacken of het uitvoeren van een DDoS-aanval wordt genoemd, maar bijvoorbeeld ook dat sommige daders een drang hebben om zoveel mogelijk informatie te verzamelen. Vooral dit laatste komt in verschillende daderinterviews terug. Verscheidene daders geven aan dat het hen een kick geeft om zoveel mogelijk databases of gegevens binnen te halen. Het gaan dan niet zozeer om het

misbruiken van die gegevens, maar puur het verzamelen zelf, waarbij het doel is om de hoogte van het 'getal' (hoeveelheid data), je score, zo hoog mogelijk te krijgen.

Plezier of lol maken wordt in de literatuur ook regelmatig aangehaald als een motief. In het onderzoek van Jansen (in Kerstens & Stol, 2012) komt naar voren dat één op de tien ondervraagde jongeren heeft aangegeven zich wel eens schuldig te maken aan virtuele diefstal met als voornaamste reden dat ze het wel grappig vinden. Weulen Kranenbarg (2018) beschrijft dat het motief plezier/een goed gevoel hebben het tweede belangrijkste motief is voor daders die betrokken zijn bij delicten als het onderscheppen van communicatie, het gebruik of distribueren van malware of de verkoop van data.

Ook verschillende experts stellen dat een deel van de daders, vooral jeugdigen, tijdens het plegen van de daad lol ervaren of het grappig vinden en ook dat het voelt voor daders als het spelen van een spelletje, wat op zijn beurt ook weer in verband wordt gebracht met de (lage) perceptie van de schade. Dit beeld wordt ook ondersteund door wat er in de daderinterviews naar voren komt. Enerzijds wordt 'het grappig vinden' naar voren gebracht (zowel door daders die de school of e-mailaccounts hebben gehackt als door daders die DDoS-aanvallen hebben uitgevoerd) als een drijfveer om aan te geven dat er plezier of lol wordt beleefd aan het plegen van bepaalde delicten. Anderzijds wordt het, door vrijwel alle daders die de delicten hebben gepleegd toen ze nog niet volwassen waren, gebruikt om het onschuldige karakter van hun delicten en hun beperkte inzicht in de schade te benadrukken (zie verder hoofdstuk 5).

De behoefte aan de kick, spanning en plezier kan ook samenhangen met verveling in de offline-wereld (Schell & Holt, 2010). 12% van de respondenten uit de studie van Chiesa et al. (2009) begon met hacken vanwege verveling in hun offline leven. Volgens Steinmetz et al. (2017) heeft hacken als activiteit ook elementen van verveling, wat samenhangt met het feit dat men bepaalde handelingen steeds moet herhalen. Tegelijkertijd is er, zoals eerder besproken, de sensatie of *rush* indien de hack slaagt. Verveling wordt niet heel expliciet als motief door de experts naar voren gebracht. Wel wordt door een tweetal daders gewezen op verveling, bijvoorbeeld op school, die een rol heeft gespeeld bij het feit dat ze zijn gaan hacken. Zo beschrijft een respondent dat hij het saai vond op de middelbare school en dat hij niet aan zijn trekken kwam als het ging om IT. Hij maakte op een gegeven moment geen huiswerk meer en was liever met computers en hacken bezig. In de literatuur wordt ook aandacht besteed aan dit aspect. Volgens Árpád (2013) zouden informaticalessen door ongeïnteresseerde of onervaren docenten worden gegeven en zijn deze lessen onvoldoende uitdagend. Daardoor is er sprake van een gebrek aan basiseducatie en het leren van ethische normen, wat op zijn beurt kan resulteren in onverantwoordelijk online gedrag, een gebrekkig begrip van professioneel internetgebruik en/of een passie voor illegale activiteiten en een verheerlijking van degenen die daar goed in zijn.

De kick, spanning en ook plezier zijn geen motieven die uniek zijn voor cyberdaders. Ook bij andere delicten kunnen dergelijke drijfveren aan de orde zijn. Chandler (1996, in Morris & Blackburn, 2009) vergelijkt hackers bijvoorbeeld met joyriders, een risicovolle activiteit waar ook spanning en adrenaline bij komt kijken. Eerder werd ook al genoemd dat overvallers door spanning of adrenaline kunnen worden gedreven. Het verschil ten opzichte van traditionele (criminele) of risicovolle activiteiten waar de kick een rol speelt, is dat er in cyberspace geen risico bestaat om zelf fysiek gewond te raken. Ook is de pakkans veel kleiner (zie hoofdstuk 5). Wel lijkt het psychologische gevoel van een geslaagde hack hetzelfde te zijn als bij een succesvolle beroving (Árpád, 2013).

4.3. Macht

Ook macht wordt in enkele studies (o.a. Chiesa et al. 2009; Weulen-Kranenbarg, 2018) als motief aangemerkt, waarbij het gaat om macht over het systeem van een derde (persoon of organisatie) alsook over macht c.q. 'heer en meester willen' zijn over de machine (Turgeman-Goldschmidt, 2005; Van der Wagen, 2018). Het gevoel om de controle over andermans systeem te hebben en daarmee te doen wat je wilt creëert voor sommige hackers het gevoel van macht (Turgeman-Goldschmidt, 2005; Van der Wagen, 2018). Dit laatste is ook terug gekomen in enkele daderinterviews. Zo geeft een respondent aan dat het hacken van websites hem een gevoel van macht gaf, omdat je de eigenaar van de website slimmer af bent en je de website kan laten doen wat 'jij wilt dat hij doet'.

Volgens Turgeman-Goldschmidt (2005) kan het bij macht ook gaan om het gevoel overal toe in staat te zijn, een aspect dat ook in het volgende citaat bovenkomt: "Laten we eerlijk zijn, ik heb geen vuurwapen nodig, mijn vuurwapen is het keyboard en de computer." (Daderinterview 9).

De daders die specifiek macht als motief vermelden, brengen het meestal in samenhang met de (adrenaline) kick naar voren. Wanneer de hack slaagt, ervaren sommige daders zowel een kick als macht. Een andere respondent geeft aan dat je een gevoel van macht ervaart zodra je toegang weet te verkrijgen tot persoonlijke gegevens zonder dat iemand het weet, wat ook weer aansluit bij de eerder besproken rol van de sneaky thrill (Katz, 1988). Zo zegt hij:

> Je voelt toch een soort macht denk ik, dat je denkt van ja weet je, niemand heeft het door, kijken hoe ver je kunt gaan inderdaad. Ja, de mensen die, naja de coole vervelende jongens in de klas, die een beetje vervelend aan het doen zijn, als je een wachtwoord hebt van hun mail weet je, dan kun je wel zo stoer in de klas mensen gaan lopen lastig vallen, maar ik kan overal bij jou, dus misschien moet jij maar gewoon wat minder stoer doen zeg maar. (Daderinterview 10)

Macht als drijfveer komt eveneens voor bij traditionele delicten zoals moord, verkrachting en beroving, waarbij het doorgaans gaat om macht over een menselijk slachtoffer. Bij cybercriminaliteit kan het ook gaan om macht over een ander persoon, maar kan het tevens gaan om het hebben van macht over een computer, systeem of netwerk. Macht over en interactie met de machine zijn aspecten die niet of nauwelijks terugkomen bij andere vormen van criminaliteit. Van der Wagen (2018) spreekt in dit verband dan ook van *cyborg deviance* om het belang van de mens-machine interactie te benadrukken zowel als het gaat om de uitvoering als de beleving. Daarnaast suggereren de bevindingen dat de drijfveer macht niet alleen over controle gaat, maar ook een sterk competitief element heeft.

4.4. Erkenning, bewijsdrang en peerrespect

Erkenning wordt in verschillende studies naar voren gebracht als een belangrijke drijfveer voor daders van cybercriminaliteit in enge zin (o.a. Aiken et al., 2016; Cayubit, Rebolledo, Kintanar, Pastores, Santiago & Valles, 2017; Chiesa et al., 2009). Sommige studies spreken over een zekere drang om iets te bewijzen, vooral in de cirkel van *peers*.

Ook verschillende experts wijzen hierop. Zo wordt het voorbeeld gegeven van een jeugdige dader die ging opscheppen bij zijn vrienden dat hij cijfers kon ophogen en vervolgens uitgedaagd is door anderen die zeiden dat hij dat toch niet kon. Vervolgens heeft deze dader bewezen dat hij dit wel degelijk kon. De drang om te bewijzen hoeft zich echter niet te beperken tot *peers*. Ook is door een expert een voorbeeld aangehaald van een hacker die wilde dat de 'hele wereld wist wat hij kon'.

Dat bleek bijvoorbeeld uit het feit dat hij een manifest had geschreven. In verschillende studies wordt de drang om jezelf te bewijzen gekoppeld aan de zogenaamde *I'll show you* mentaliteit die veel hackers hebben (Jordan, 2008; Taylor, 1999; Thomas, 2002, in Steinmetz et al., 2017).

Ook in de online wereld speelt erkenning en bewijsdrang een rol. Zoals eerder beschreven, spenderen de cyberdaders veel tijd online, bijvoorbeeld op fora. Daar spelen aspecten zoals uitdaging, reputatie of status en competitie volgens de experts een grote rol. Status of reputatie kan online alleen verkregen worden door ook daadwerkelijk te laten zien wat je kunt. Zoals een expert stelt, juist als je iets kunt wat anderen niet kunnen, verdien je op dergelijke fora veel aanzien. Men probeert elkaar te overtroeven. Volgens Cayubit et al. (2017) streven sommige hackers ook een zekere superioriteit na. Als er sprake is van afwijzing binnen de vriendenkring kan dit echter ook leiden tot gevoelens van wraak (Árpád, 2013). Volgens Chiesa et al. (2009) kan een *white hat* hacker zelfs in een dag transformeren naar een black hat hacker indien er niet geluisterd wordt wanneer hij of zij een beveiligingslek meldt of geen waardering krijgt voor zijn of haar ontdekkingen. Dit type hacker is gericht op prestatie en haalt persoonlijke voldoening uit het inzetten van zijn of haar vaardigheden. Na een geslaagde hack is er sprake van een ego-boost en een gevoel van trots. Superieur willen zijn wordt ook expliciet door sommige experts naar voren gebracht. Deze daders willen ook heel graag laten zien wat ze kunnen.

De daders wijzen ook op motieven die onder de noemer erkenning, status en bewijsdrang vallen. Zo geven verschillende respondenten aan specifiek erkenning te zoeken op hackerfora en vermelden dit ook als een drijfveer. Als hacker begin je doorgaans als ondergewaardeerde scriptkiddie en je moet er wel iets voor doen, jezelf bewijzen, om *wel* die waardering te krijgen. Zo betitelt een respondent scriptkiddies als 'de feuten' onder de hackers en beschrijft hij hoe hij dit zelf ervaarde:

> Die naam [scriptkiddie] wil je zo snel mogelijk kwijt zijn… Ik had iets gemaakt waar ik helemaal trots op was. Dat had ik op een forum gezet en toen ben ik helemaal compleet afgebrand op ja, je bent alleen maar aan het kopiëren en plakken, je hebt zelf niks gemaakt. En dat was eerst een harde slag. Zo van shit, want ik was helemaal trots op het dingetje wat ik had gemaakt en degene die alles wist van dat forum op dat moment die begon te zeggen dat ik helemaal niks had gedaan, dat het echt slecht was. Maar ja dat was ook wel weer een motivatie om dan te denken nou blijkbaar kan ik er wel meer mee. (Daderinterview 4)

Je zult volgens deze respondent moeite moeten doen om in de hackergemeenschap zelf geaccepteerd te worden en een flinke stap moeten zetten. Als je dan eenmaal toegelaten wordt, is het een kwestie van reputatie opbouwen. Het zo hoog mogelijk op 'de ladder klimmen' was voor hem persoonlijk erg belangrijk. Het hogerop willen klimmen in de hiërarchie wordt ook in enkele studies aangehaald (o.a. Aiken et al., 2016, Chiesa et al., 2009).

Enkele respondenten geven ook aan enige 'roem' wel leuk te vinden. Zo beschrijft een dader dat er op een gegeven moment allemaal geruchten de ronde gingen over hem op het internet, omdat hij heel veel had gehackt en naar eigen zeggen niemand meer veilig was. Hij geeft aan dat hij dit leuk vond en het hem ook erkenning gaf.

Of erkenning, status en bewijsdrang exclusieve motieven zijn voor cyberdaders, is wederom een punt van discussie. Gesteld kan worden dat erkenning en status ook een rol spelen bij (jeugdige en volwassen) groepen die zich met traditionele misdaad bezighouden, zoals druggerelateerde criminaliteit en geweldsdelicten. Een mogelijk verschil is wel dat de status bij cybercriminaliteit sterk(er) bepaald wordt door *wat je kunt* (je vaardigheden, de (innovatieve) werkwijze en de geleverde

prestaties) en minder door *wie je bent*. Toch is er ook op dit punt een gelijkenis te vinden met bepaalde traditionele dadergroepen. Zo beschrijven Kroese en Staring (1993) dat de status en prestige van overvallers bepaald wordt door de hoogte van de buit, de modus operandi (als de dader op een ingenieuze wijze[68] een object weet te beroven krijgt hij extra aanzien) en het type object (voor een overvaller geniet een bank meer aanzien dan een benzinepomp). Alle drie de aspecten komen op een enigszins vergelijkbare wijze terug bij cybercriminaliteit, voornamelijk bij het hacken. De buit draait voor de meeste hackers niet per se om geld, maar bijvoorbeeld om een grote of belangrijke database met gegevens.

Het aspect van bewijsdrang is mogelijk ook niet helemaal uniek voor cyberdaders. Traditionele daders moeten zichzelf vaak ook bewijzen in de groep. Mogelijk staat dit aspect wel meer op de voorgrond bij cybercriminaliteit, vanwege de nadruk op vaardigheden. Ook lijkt de bewijsdrang bij cyberdaders in meerdere contexten een rol te spelen dan bij traditionele criminaliteit. In gevallen waarbij het kunnen van de dader op de proef wordt gesteld (een persoon roept 'dat je het niet kunt') of als een persoon of bedrijf claimt de beveiliging goed op orde te hebben terwijl dat niet het geval is, wordt de bewijsdrang getriggerd. Mogelijk hangt dit samen met wat in de literatuur (en ook door hackers zelf) beschouwd wordt als iets hackerseigen, een onderdeel van hun mentaliteit (Steinmetz, 2015a, 2015b; Van der Wagen, 2018).

4.5. Geld

In de literatuur komt vooral het beeld naar voren dat geld niet of nauwelijks een motief is voor *individuele* daders van cybercriminaliteit in enge zin (Van der Wagen et al., 2016; Turgeman-Goldschmidt, 2005). Van de 54 hackers (jeugdigen en volwassenen) die Turgeman-Goldschmidt (2005) heeft geïnterviewd is er bijvoorbeeld bijna geen enkele respondent die hackte voor geld. In het onderzoek van Weulen Kranenbarg (2018) zijn financiële motieven vrijwel afwezig voor alle clusters cyberdelicten, zelfs voor delicten zoals het distribueren van malware of de verkoop van data. Cayubit et al. (2017) hebben in hun studie naar (jeugdige en volwassen) hackers wel een financieel motief gevonden, maar geven daarbij aan dat andere (meer psychologische) motieven zoals erkenning ook een rol spelen bij deze dadergroep. Sommige studies vinden dat geld pas een rol gaat spelen op een later moment in de criminele carrière. Hoek van Dijke (2016), die 20 jeugdige daders van cybercriminaliteit in enge zin heeft geïnterviewd, laat bijvoorbeeld zien dat sommige daders beginnen met hacken omdat ze de techniek willen verkennen of vanwege de kick, maar door de tijd heen vaardiger worden en ontdekken dat ze er ook geld mee kunnen verdienen. De onderzoeker spreekt in dit kader van een proces, een geleidelijke transitie. Naarmate daders professionaliseren kunnen ze ook andere (bijvoorbeeld financiële) motieven krijgen (zie ook hoofdstuk 6).

Volgens experts kunnen daders die begonnen zijn vanuit nieuwsgierigheid en enthousiasme terecht komen 'in omgevingen waarin zij in dezelfde zandbak zitten met de meer professionele daders' die er geld mee verdienen. In dat geval gaat het om rekrutering. Experts benoemen onder meer dat criminele organisaties beogen om hackers te werven om bijvoorbeeld hun communicatie te versleutelen. Volgens een expert zijn er weinig daders die gelijk bij het eerste delict een businessmodel laten draaien gericht op winst. Toch worden er door politie-experts wel voorbeelden

[68] Dit hoeft overigens niet per se om een ingewikkelde modus operandi te gaan. Kroese en Staring (1993) halen het voorbeeld aan van een overvaller die met twee pakken melk in een plastic tas de bank binnenliep en zei dat er een bom in zat. Dit werd als vermakelijk beschouwd. Ook in verschillende hackerstudies komt dit aspect terug. Een ingenieuze en inventieve hack wordt juist gekarakteriseerd door eenvoud en een beetje humor (Van der Wagen et al., 2016; Jelsma, 2017).

genoemd waarbij dat wel gelijk het geval bleek te zijn. Een voorbeeld hiervan was een collectief van jongvolwassen daders die op grote schaal online fraudeerde en daarbij vrij geavanceerde technieken gebruikte. Een ander voorbeeld is een casus van iemand die DDoS-aanvallen uitvoerde, op grote schaal bedrijven afperste en hier veel geld mee verdiende. Volgens de politie-expert die hier nauw bij betrokken was, ging het om een dader die uit een relatief arm gezien kwam. Geld stelde hem niet alleen in staat om mooie kleding te kopen, maar gaf hem ook het gevoel van "joh kijk, ik stel ook wat voor in deze maatschappij." Dit voorbeeld sluit ook aan bij de aanname van Hutchings (2016) dat een deel van de daders met cybercriminaliteit begint vanwege *strain*: het niet kunnen bereiken van de doelen (veel geld) met legitieme middelen en om deze reden de overstap maken naar (cyber)criminaliteit (zie ook hoofdstuk 6).

Studies op het gebied van georganiseerde cybercriminaliteit, waarbij het doorgaans om vermogensdelicten gaat (Choo, 2011) spreken – wat ook inherent is aan het type activiteit - wel van een financieel motief. Ook de experts geven aan dat geld of zelfverrijking bij dit soort delicten voorop staat, maar geven daarbij ook aan dat de concrete achterliggende reden om geld te verdienen wel kan verschillen. Zo zijn er cyberdaders die simpelweg een luxe levensstijl willen (wat in hun subcultuur ook status kan geven). Ook zijn er daders die vanwege schulden in de cybercriminaliteit terecht zijn gekomen of die een verslaving moeten bekostigen.

Verschillende geïnterviewde daders geven aan (ook) een financieel motief te hebben gehad of er in ieder geval iets (enkele honderden tot enkele duizenden euro's) aan te hebben verdiend. Twee daders, beiden actief in fraude gerelateerde activiteiten, hebben aangegeven aan dat materieel gewin wel meer het primaire motief was. Een van hen, die overigens het delict in groepsverband pleegde en hier ook een leidend figuur in was, geeft aan dat het voor hem voelde als een 'bedrijf' dat hij runde: "mijn dagelijks inkomen, als mijn baan, als mijn werk, bedrijfsmatig." Hij geeft aan dat er ook wel een zekere spanning aan te beleven viel, maar dat het voor hem toch voornamelijk draaide om geld. De financiële drijfveer bleef voor hem ook altijd sterk op de voorgrond staan, omdat het voor hem ook een bepaalde luxe levensstijl mogelijk maakte. Hij kon zich bijvoorbeeld een dure leaseauto permitteren die wel betaald moest worden. Ook financierde hij hiermee een drugsverslaving.

Geld was ook een heel belangrijk (maar niet het eerste en enige) motief voor een dader die onder meer betrokken was bij virtuele diefstal. Het begon voor hem voor de lol en de kick, maar op een gegeven moment ging het financiële motief steeds meer op de voorgrond staan, conform het verhaal van enkele respondenten uit de studie van Hoek van Dijke (2016). Hij speelde een online virtueel spel waarbij het de bedoeling is om zo veel mogelijk spullen te vergaren die je vervolgens kunt verhandelen in ruil voor echt geld. Hij ging samen met medespelers slimme (illegale) manieren verzinnen om snel(ler) rijk te worden, wat hem/hen uiteindelijk tot het hacken bracht en met succes. Er werden duizenden euro's verdiend aan de virtuele diefstal. Net als voorgenoemde dader geeft hij aan dat het geld hem ook in staat stelde om (dure) spullen te kopen (in zijn geval mooie kleren). Geld verdienen kwam dan ook steeds meer op de voorgrond te staan en de hacks werden volgens hem steeds meer doelgericht. Een andere dader beschrijft dat hij een tijdelijke transitie maakte van '*fame* naar financieel', wat hij ook relateert aan het feit dat hij op gesloten fora toegelaten werd die op financiële vormen van cybercriminaliteit gericht waren. Nog een andere dader geeft aan dat hij gerekruteerd was door een criminele organisatie om in opdracht klussen te doen tegen betaling. Hij kreeg hier dan wel voor betaald, maar hij deed het naar eigen zeggen voor de uitdaging en niet voor het geld. Geld was volgens hem een mooie bijkomstigheid.

Geld is uiteraard een motief dat bij veel vormen van criminaliteit in kleine of grote mate een rol speelt. De betekenis van geld (zelfverrijking en eventueel een luxe levensstijl of het oplossen van

schulden) is waarschijnlijk niet anders voor cyberdaders dan voor traditionele daders. De vraag bij dit motief is vooral of deze drijfveer wel of niet vaker voorkomt bij cyberdaders. De bevindingen suggereren dat de meer immateriële motieven zoals de kick, uitdaging en macht een grotere rol spelen dan geld, vooral waar het jonge daders (meestal hackers) betreft. Voor een subgroep hierbinnen kan geld wel op een later moment een drijfveer worden. Waar het fraude-gerelateerde delicten betreft, voornamelijk gepleegd door jongvolwassen en volwassen daders, staat geld net als bij traditionele vermogensdelicten wel meer op de voorgrond.

4.6. Wraak, frustratie of andere persoonlijke redenen

Het plegen van cybercriminaliteit vanuit frustratie en/of met als doel om wraak te nemen, wordt in verscheidene studies aangehaald als drijfveer voor cybercriminaliteit in enge zin. Vaak is er dan (net als bij traditionele criminaliteit) een emotionele factor in het spel, omdat de dader zich door iets of iemand beledigd, teleurgesteld of tekortgedaan voelt (Turgeman-Goldschmidt, 2005). Het motief kan een rol spelen bij verschillende vormen van cybercriminaliteit, waaronder virtuele diefstal (Zebel et al., 2013; Kerstens & Stol, 2012), het verspreiden van virussen (Turgeman-Goldschmidt, 2005), hacken (o.a. Rogers, 2006; Weulen Kranenbarg, 2018; Leukfeldt et al., 2010; Chiesa et al., 2009) en het uitvoeren van DDoS-aanvallen (Van der Hulst & Neve, 2008). De dader kan bijvoorbeeld iemand of een organisatie in diskrediet brengen door vertrouwelijke informatie te openbaren of aan te passen of schade toe te brengen aan de persoon of aan computerapparatuur (Brar & Kumar, 2018; Árpád, 2013). Rogers (2006) maakt binnen de motivatie wraak een onderscheid tussen een persoonlijke en institutionele wrok, evenals wraak gericht op staten. Seebruck (2015) heeft de taxonomie van Rogers verder uitgewerkt en onderscheidt persoonlijke wraak (bijvoorbeeld door ontevreden medewerkers) en grotere rechtvaardigheidskwesties (bijvoorbeeld online crowdsourcing-bewegingen).

Verscheidene onderzoeken bevestigen dat wraak of boosheid zich vaak op een persoonlijk niveau manifesteert. Leukfeldt et al. (2010) concluderen op basis van politiedossiers dat het hacken vaak in de relationele sfeer plaatsvindt, waarbij wraak wordt genomen op ex-geliefden, ex-partners of schoolvrienden. Van de 33 verdachten kon bij 12 verdachten als primaire motivatie wraak geïdentificeerd worden. Wraak of woede kan volgens de literatuur echter ook geuit worden richting andere partijen, zoals richting een docent vanwege het van school gestuurd worden (Turgeman-Goldschmidt, 2005), een 'bulletin bord' systeem[69] vanwege het verbannen zijn (Holt, 2005), een advocatenkantoor vanwege een familiegeschil over een erfenis (Odinot et al., 2017) of een bedrijf vanwege een afwijzing voor een baan (Preuß et al., 2007). Hiernaast beschrijven Chiesa et al. (2009) dat zeker de jongere hackers veel woede hebben en verlichting zoeken door middel van hacks en het neerhalen van systemen, al dan niet doelgericht.

Aanvullend wordt in de literatuur de insider of de wraakzuchtige (ex)-medewerker geïdentificeerd als een afzonderlijke categorie. Hald & Pedersen (2012) beschrijven dat het doelwit van een *insider attack* meestal de (voormalige) werkplek van de dader is. Dit geeft deze insiders een voordeel omdat ze vanwege hun werkzaamheden kennis hebben van de systemen en beveiliging (Hald & Pedersen, 2012; Li, 2008; Chiesa et al., 2009). Wraak wordt uitgeoefend als reactie op een negatieve gebeurtenis op het werk (Hald & Pedersen, 2012) zoals een gebrek aan erkenning door het management (Rogers, 2010), het mislopen van een promotie (van der Hulst & Neve, 2008), of wraak

[69] In het Engels: *Bulletin Board System* (BBS). Een prikbordsysteem is een systeem of applicatie dat het mogelijk maakt om online berichten of bestanden uit te wisselen met andere gebruikers.

vanwege ontslag (Rege, 2012; Rege-Patwardhan, 2009; Rogers, 2010; Broadhurst, Grabosky, Alazab, Bouhours & Chon, 2014; Smith, 2015).

Ook de experts hebben wraak en frustratie als drijfveren geïdentificeerd. Een expert van een lokale politie-eenheid geeft aan dat deze categorie het vaakst voorkomt als gekeken wordt naar alle verdachtenregistraties. Individuen hebben een conflict (vaak met de ex-partner), voelen zich onbegrepen door de samenleving, afgewezen of boos en willen deze frustratie tot uiting brengen. In dit verband wordt door verscheidene experts beschreven dat ofwel een DDoS-aanval of hacken wordt ingezet. Zo worden door de experts voorbeelden aangehaald van het uitvoeren van een DDoS-aanval op een concurrerend bedrijf vanwege onenigheid, het vrijgeven van informatie door een individu vanwege een conflict met een bedrijf of het aanpassen van een website van een overheidsinstantie vanwege een conflict. Hiernaast worden door de experts voorbeelden genoemd zoals het stelen van een bitcoin wallet uit jaloezie, het hacken van de e-mail of Facebook account van de ex of het stelen van informatie of naaktfoto's. In het kader van laatstgenoemde kan het delict ook meer in de zeden/(kinder)pornografische sfeer gesitueerd zijn. Zo noemt een politie-expert een voorbeeld van een casus waarbij er sprake was van een netwerk/forum waarbij op grote schaal i-Cloud accounts van jonge vrouwen werden gehackt. De afbeeldingen werden via het forum gedeeld.

Net zoals dat in de literatuur het geval is, zien de experts de gefrustreerde (ex)-medewerker als een losse categorie. De experts beschrijven overeenkomstig met de literatuur dat deze categorie kwaad is vanwege een arbeidsconflict of ontslag. Deze individuen hebben (nog) toegang tot de systemen van het bedrijf en brengen hun boosheid tot uiting in het platleggen van systemen, het wissen van databases of het stelen van bedrijfsinformatie. Er is echter nog weinig over deze categorie bekend.

Hacken uit wraak, frustratie of om persoonlijke redenen is niet vaak genoemd door de geïnterviewde daders. Eén van de daders geeft aan soms te hacken om iemand de mond te snoeren, een fenomeen dat volgens hem 'doxen' wordt genoemd. Hij legt het als volgt uit:

> Een specifiek persoon had een grote mond, dan gingen we die persoon doxen, heet dat dan, dat is dan heel veel informatie over diegene vinden. Dat is van naam tot familie tot geboortedatum tot favoriete dier, whatever. En soms deed je dan ook wel eens, als je die persoon dan echt niet mocht, dan plaatste je dat gewoon online. Vooral in die [naam virtueel spel]-wereld weet je wel, want iedereen verschuilde zich achter die gebruikersnaam en iedereen heeft een grote mond, internetgangsters zeg maar. Als je dan al die informatie over iemand kunt krijgen en je gooit het online, dan zijn ze daarna stil zeg maar. Dat deed ik op zich ook wel, meer niet. (Daderinterview 8)

Dit doxen deed hij nooit bij willekeurige mensen, maar alleen bij personen van wie hij vond dat ze het verdienden. De respondent die veroordeeld is voor het hacken van zijn ex-vriendin geeft aan onschuldig te zijn, maar vertelt in het interview wel dat er veel problemen speelden tussen hem en zijn ex, waaronder overspel.

De discussie bij het motief wraak, frustratie en persoonlijke redenen is niet zozeer of er een verschil is tussen traditionele en cyberdaders, het draait vooral om de vraag of het in deze context überhaupt om separate dadergroepen gaat. Hoewel het motief in mindere of meerdere mate een rol kan spelen bij de meer technisch vaardige daders, zoals bovenstaand voorbeeld laat zien, lijkt het motief vaker voor te komen bij traditionele (niet-technisch vaardige) daders voor wie hacken een nieuw (en toegankelijk) middel is geworden om het delict te plegen.

4.7. Ideologische motieven

In de literatuur wordt ook een groep cyberdaders onderscheiden die vooral gedreven wordt door ideologische motieven. Dergelijke daders worden in de literatuur meestal aangemerkt als hacktivisten. Deze daders streven vaak een bepaalde politieke agenda na, doorgaans gerelateerd aan vrijheid van informatie, vrijheid van meningsuiting, informatie-ethiek en mensenrechten (Dahan, 2013). Een voorbeeld hiervan is de hack van digitale bibliotheek JSTOR vanuit de overtuiging dat wetenschappelijk onderzoek openbaar en gratis toegankelijk moet zijn (Broadhurst et al., 2014). Ook zijn er hacktivistische daders met ideologische motieven die gerelateerd zijn aan extreem patriottisme en religie (Seebruck, 2015). Bij dit laatste kan gedacht worden aan het defacen van websites van religieuze organisaties in het Midden-Oosten als verdediging tegen religieus fanatisme (Chiesa et al., 2009) of terrorisme (Holt, Freilich, Chermak, 2017; Tanczer, 2017).

Hacktivisten zelf scharen hun motieven vaak onder de noemer 'burgerlijke ongehoorzaamheid' (Rogers, 2010; Tanczer; 2017). Uit een studie van Tanczer (2017) gebaseerd op interviews met 35 hackers en hacktivisten blijkt dan ook dat de hacktivisten in de veronderstelling zijn dat ze iets goeds doen voor mensen en de maatschappij. Rogers (2010) is hier echter sceptisch over. Hij stelt dat het primaire motief van de hacktivist wraak, macht, marketing of media-aandacht is en dat de ideologische motieven meer secundair zijn en/of als 'camouflage' dienen voor andere motieven. Zoals hier ook uit blijkt, kan er een discrepantie bestaan tussen zogenaamde *insider* en *outsider* accounts als het gaat om welke motieven naar voren worden gebracht (zie ook Yar, 2005).

De experts hebben weinig tot geen persoonlijke ervaring met cyberdaders met ideologische motieven, maar zijn zich wel bewust van het bestaan ervan. Een expert van de politie die jarenlang bij veel zaken betrokken is geweest, geeft aan dit type dader niet vaak tegen te komen, maar vermoedt wel dat zowel links- als rechtsextremistische groeperingen steeds meer gebruik zullen maken van hacks, omdat ze daarmee waardevolle informatie kunnen vergaren. Hacktivistische motieven worden door de experts beschreven als bereid zijn 'om strafbare feiten te plegen om de ideologie verder te brengen' of 'proberen te hacken om een boodschap te verspreiden'. Volgens een expert van het Openbaar Ministerie kan het gaan om politieke stromingen, maar kan het - in overeenstemming met de literatuur - ook om andere ideologische ideeën gaan waarbij men het niet eens is met de maatschappij en van mening is dat deze op een andere manier dient te functioneren. Voorbeelden die door de experts genoemd worden van ideologische motieven zijn de strijd voor een vrij internet of het aankaarten van misstanden in de maatschappij zoals onder andere hackerscollectief Anonymous doet. Dit kan uiteenlopen van veiligheidslekken tot genocide. Een voorbeeld van een concrete zaak die door enkele experts naar voren is gebracht betrof een collectief van hackers/hacktivisten die websites en databases hackten en ook defaceten. Hierbij waren de motieven ideologisch (slechte beveiliging willen laten zien), maar tegelijk speelde ook lol maken en media-aandacht een rol.

Het ideologische motief komt niet heel sterk uit de daderinterviews naar voren, wat mogelijk ook met de daderselectie te maken heeft. Wel hebben enkele respondenten sterke opvattingen over privacy, informatiebeveiliging en de overheid en vinden ze het belangrijk dat misstanden (zoals beveiligingslekken) aan het licht worden gebracht, ook al gebeurt dat op illegale wijze.

Net als bij de motieven geld en wraak kan gesteld worden dat ideologische motieven geen typische motieven zijn voor cyberdaders. Afgaande op de bevindingen lijkt deze groep ook divers te zijn. Het kan variëren van activistische, meer 'traditionele' (groepen) daders die een nieuw middel

hebben ontdekt om hun doelen te verwezenlijken tot daders (voornamelijk jonge hackers) voor wie hacktivisme samengaat met motieven als uitdaging, kick, plezier en macht.

4.8. Conclusie

In dit hoofdstuk is stilgestaan bij de drijfveren van cyberdaders en de beleving die daarmee gepaard gaat. Daarbij is ook bediscussieerd in hoeverre het belang en de aard van de desbetreffende drijfveer voor cyberdaders afwijkt ten opzichte van traditionele daders. De bevindingen suggereren dat de drijfveren van cyberdaders niet alleen divers zijn, maar ook dat daders vaak meerdere drijfveren hebben, die ook nog eens door de tijd heen kunnen veranderen.

De drijfveren nieuwsgierigheid, leergierigheid en (mentale) uitdaging spelen voornamelijk een rol bij jeugdige cyberdaders. Deze motieven zijn niet per definitie kwaadaardig. Ze willen de *ins and outs* van systemen leren en ontdekken hoe ver ze kunnen gaan met de techniek. Anders dan bij de meeste traditionele vormen van criminaliteit is het leren een doel of drijfveer op zichzelf en niet slechts een middel of instrument om de delicten te kunnen plegen.

Andere motieven die naar voren komen zijn de kick, spanning, plezier, verveling, verzameldrang en macht. Deze drijfveren kunnen ook bij traditionele criminaliteit spelen, maar bij cybercriminaliteit is er een meer nadrukkelijke samenhang met online vaardigheden en techniek.

Erkenning, status, *peer respect* en bewijsdrang komen als belangrijke motieven naar voren bij jeugdige daders. Ze willen bewijzen wat ze kunnen om respect of roem te verwerven of omdat zij zich uitgedaagd voelen door bijvoorbeeld bedrijven. Het verschil met traditionele misdaad is dat de focus sterker ligt op de technische vaardigheden, werkwijze en prestatie (je 'kunnen').

Financiële motieven lijken in mindere mate een rol te spelen bij jeugdige (individuele) daders. In sommige gevallen kan geld wel op een later moment in de criminele carrière een rol gaan spelen. Dit is ook afhankelijk van de activiteiten die zij ontplooien. Het financiële motief lijkt vooral voor te komen bij (volwassen) daders die actief zijn in de context van fraude en georganiseerde cybercriminaliteit. In een deel van de gevallen gaat het dan om daders die de overstap hebben gemaakt van traditionele (offline) fraude naar cybercriminaliteit.

Aanvullend kan cybercriminaliteit (voornamelijk hacken of het uitvoeren van DDoS-aanvallen) gepleegd worden uit boosheid of om wraak te nemen op vrienden, familie, ex-werkgevers of ex-geliefden waar offline een conflict mee is ontstaan. Hierbij lijkt het voornamelijk te gaan om traditionele volwassen daders die een nieuw middel hebben ontdekt om hun frustratie te uiten. Ook zijn er daders die uit ideologische motieven handelen. Laatstgenoemde twee clusters van motieven zijn relatief onderbelicht gebleven in dit onderzoek.

Hoofdstuk 5 Percepties over strafbaarheid, pakkans en schade van (gepleegde) cyberdelicten

In dit hoofdstuk wordt stilgestaan bij hoe daders aankijken tegen de strafbaarheid van cyberdelicten, de pakkans en de schade van de (gepleegde) delicten, aspecten die nauw met elkaar samenhangen. In paragraaf 5.1 besteden we aandacht aan de percepties van daders ten aanzien van de strafbaarheid van cybercriminaliteit in enge zin: in hoeverre zijn jeugdige en volwassen daders zich bewust van het feit dat ze strafbare feiten plegen of pleegden en waar hangt dit bewustzijn van af? Vervolgens wordt in paragraaf 5.2 ingegaan op de daderperceptie van de pakkans, waarbij het gaat om de vraag hoe groot daders de pakkans achten en waar ze dit op baseren alsook om de mate waarin deze perceptie invloed uitoefent op hun betrokkenheid bij cybercriminaliteit. In paragraaf 5.3 wordt stilgestaan bij de houding en perceptie ten aanzien van de schade van (gepleegde) cyberdelicten. Per deelonderwerp worden op integrale wijze de bevindingen uit de literatuur, de expertinterviews en de daderinterviews besproken.

5.1. Perceptie strafbaarheid (gepleegde) cyberdelicten

In de literatuur komt naar voren dat vooral jonge daders van cybercriminaliteit in enge zin niet altijd beseffen dat ze strafbare dingen doen en daarmee ook onwetend zijn over de (serieuze) straffen die staan op cyberdelicten, waaronder ook gevangenisstraf (Aiken et al., 2016; Smith, Grabosky, & Urbas, 2004, p. 212). De hackers die onderdeel zijn van een hackergemeenschap lijken daarentegen vaak goed op de hoogte van het doen en laten van andere hackers en van de uitkomst van hun strafproces. Hetzelfde geldt voor financieel gemotiveerde daders (Smith et al., 2004, p. 212).

Een soortgelijk beeld komt uit de expertinterviews naar voren. Waar sommige experts ervan overtuigd zijn dat het tegenwoordig heel duidelijk is waar online de grenzen liggen - dat iedereen (ook een jeugdige) weet ‘dit mag niet’ - spreekt het merendeel van de experts over een groot grijs gebied. Ze stellen dat wat online goed en fout is, niet zo zwart-wit is als in de offline wereld. De experts lijken hierbij uit te gaan van een glijdende schaal. Aan de linkerkant van de schaal heb je de meer onwetende (meestal jonge) daders, die niet of nauwelijks besef hebben van het feit dat ze strafbare dingen doen. Ze weten wel dat zij iets doen dat niet helemaal door de beugel kan of in mindere of meerdere mate ‘fout’ is, maar percipiëren het niet als een strafbaar feit waar (serieuze) juridische gevolgen aan kleven, inclusief een strafblad. Aan de rechterkant van de schaal heb je de meer ‘rationele’ of ‘berekenende’ jonge daders die zich wel degelijk bewust zijn van de strafbaarheid en ook meer kennis hebben van de straf die er op staat. Deze kennis doen ze volgens experts op via (hacker)fora. Daar wordt soms uitgebreid gesproken over straffen die volgen op hacks of het uitvoeren van DDoS-aanvallen. Als het gaat om volwassen daders wordt er door de experts vanuit gegaan dat ze zich meer aan de rechterkant van de schaal bevinden, dus zich wel bewust zijn van de strafbaarheid.

Sommige experts relateren de perceptie van de strafbaarheid ook aan het motief. De jeugdigen bij wie technische uitdaging het centrale motief is, zien niet direct in dat wat zij doen ook strafbaar is en weten niet goed waar de grenzen liggen of zoeken juist de grenzen op. Bij de meer financieel georiënteerde cyberdaders (jeugdig of volwassen) is er volgens de experts minder sprake van variatie waar het gaat om kennis van strafbaarheid. Volgens de meeste experts zijn deze daders zich ten volle bewust van de strafbaarheid van hun delicten en maken zij een rationele afweging, mede ingegeven door de (lage) pakkans, over het plegen van de delicten.

De experts dragen verschillende verklaringen aan voor het feit dat een deel van de daders (voornamelijk jeugdigen) zich niet of nauwelijks bewust is van de strafbaarheid van de cyberdelicten die ze plegen. Ten eerste kan er sprake zijn van onduidelijkheid over juridische grenzen, iets dat volgens de experts vooral bij jeugdigen speelt die hacken, waarbij het financiële gewin in mindere mate of minder vaak een rol speelt. Wanneer er geld wordt verdiend met een delict, wordt het echter een ander verhaal. Zo stelt een expert:

> Zodra je er geld mee aan het verdienen bent, kun je jezelf niet meer vertellen dat het alleen maar een lolletje en een pretje en een spelletje is. Dan snap je ook echt wel dat je met iets boevigs bezig bent. Die anderen snappen vaak ook wel dat ze een beetje boevig bezig zijn, maar dat kan je nog wegzetten als een spelletje. (Expertinterview 1, Advocaat)

Dit aspect komt ook terug in de verhalen van de geïnterviewde daders die hun delicten vooral pleegden toen ze nog minderjarig waren. Of ze nu e-mailaccounts of hun school hebben gehackt, op medespelers een DDoS hebben uitgevoerd en/of medespelers hebben bestolen in een virtueel spel, ze geven bijna allemaal aan dat zij (als jeugdige) hun cyberactiviteiten vooral als kattenkwaad of iets 'grappigs' zagen en zeker niet als het willens en wetens overtreden van de wet of als iets ernstigs. Ook het spelelement, "het was maar een spelletje" wordt frequent genoemd. Als er echter afpersing, oplichting of (aanzienlijk) financieel gewin in het spel is (geweest), dan is het voor de meeste respondenten duidelijker (ook voor jeugdigen) dat er sprake is van strafbaar gedrag.

In het kader van onduidelijkheid over de juridische grenzen komt het thema *responsible disclosure* (RD)[70] in verschillende expert- en daderinterviews aan bod. Sommige daders zouden volgens experts bijvoorbeeld in de veronderstelling kunnen zijn dat je zomaar alle systemen kunt hacken zolang je het lek achteraf maar meldt. Ze denken dan ethisch bezig te zijn, maar richten (grote) schade aan. RD staat daarnaast niet op elke website vermeld, wat het volgens sommige experts lastig in te schatten maakt voor jeugdigen of het mag en dan wel 'toch een beetje grijs' is. Ook volgens een medewerker van het OM is er nog een 'wereld te winnen' in het uitleggen van wat ethisch hacken is en wat het RD-beleid inhoudt.

Ook enkele daders geven aan dat er onduidelijkheid bestaat over RD bij henzelf en bij anderen om hen heen. Ze ervaren daarbij soms dat de overheid of de samenleving het risico van beveiligingslekken of fouten (bijvoorbeeld in websites) onderschat. Zo legt een dader uit:

> Als jij een bommelding maakt van jij hebt een bom gevonden, dan staat wel iedereen te springen, van waar is het. En een fout in je website is net als een tijdbom. Er komt een dag dat iemand het vindt en er misbruik van maakt. (Daderinterview 9)

[70] *Responsible Disclosure* (RD) betreft het "binnen de ICT-wereld (...) op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure" (NCSC, 2013, p. 5). Dit beleid is echter sinds 2018 gewijzigd, volgens de nieuwe Leidraad van het NCSC (2018) omdat RD "nog te veel nadruk legt op de verantwoordelijkheid van de melder, terwijl het uitgangspunt is dat er een gelijkwaardig gesprek ontstaat tussen melder en mogelijk kwetsbare organisatie. Dit sentiment wordt beter gevat in de huidig gangbare term *coordinated vulnerability disclosure* (CVD)".

Dit citaat laat ook heel duidelijk zien dat sommige (ethische) hackers het ontdekken van lekken van levensbelang achten en daarbij ook sterk het gevoel hebben dat de buitenwereld de ernst van beveiligingslekken flink onderschat.

Daar komt nog bij dat, ook wanneer het lek wel netjes (volgens de regels van RD) wordt gemeld, er volgens een expert (Expertinterview 4, Onderzoeker) nog geen garantie bestaat dat een hacker "geen strafzaak aan zijn broek krijgt". Het OM kan volgens een expert eigenstandig besluiten om een onderzoek in te stellen om te kijken hoe bepaalde dingen zijn verlopen. Door deze onduidelijkheid met betrekking tot de juridische grenzen kun je volgens een van de daders juist ook terughoudend worden met het melden van lekken, en *dan* juist het risico lopen om vervolgd te worden. Zo legt hij uit: *"*Wel melden of niet melden. Wel melden kan resulteren in een taakstraf of weet ik veel wat. Niet melden en als ze er dan achter zijn gekomen ben je de lul" (Daderinterview 4).

Naast de onduidelijkheid over waar in juridische zin de online grenzen liggen, spelen nog een aantal andere aspecten een rol bij de perceptie van strafbaarheid. Zo kan de perceptie van de strafbaarheid volgens de experts samenhangen met de perceptie van de schade, waar in paragraaf 5.3 nader op wordt ingegaan. Als een dader niet het gevoel heeft dat hij iemand pijn doet of grote schade berokkent, voelt het ook niet als 'criminaliteit plegen' en als iets waar een (serieuze) straf op staat. Zoals een advocaat stelt: het voelt als lol maken in plaats van dat ze beseffen "dat wat ze doen moreel verwerpelijk is" (Expertinterview 1, Advocaat).

Ten slotte wordt door de experts gewezen op het principe dat er steeds een deurtje verder open gaat. Als de dader van het een op andere moment een serieus feit zou plegen zou hij of zij zich sneller bewust zijn van de strafbaarheid, dan wanneer de dader steeds een klein stapje verder gaat en daar dan ook nog steeds mee wegkomt. Verscheidene daders wijzen in dit kader ook nog op het gemak. Een dader geeft aan dat het hem verbaast dat iets dat niet mag (althans als het gaat om de cyberdelicten waar hij bij betrokken was) zo gemakkelijk is, waardoor je er sneller instapt. Hij doelt hierbij op de eenvoudige vindbaarheid van (illegale) fora via Google en het feit dat deze publiek toegankelijk zijn, terwijl er op grote schaal discussie plaatsvindt over hoe online delicten te plegen.

Op basis van onze bevindingen kan dus worden gesteld dat om verschillende redenen nog onduidelijkheid heerst over waar de grenzen liggen van wat wel en niet strafbaar is, een aspect dat meer lijkt te spelen bij cybercriminaliteit in enge zin dan bij traditionele criminaliteit. Tegelijkertijd zien we in de daderinterviews ook terugkomen dat een deel van de daders, ook als zij de door hen gepleegde delicten als kattenkwaad bestempelen, diverse maatregelen hebben genomen om hun anonimiteit te waarborgen en/of om buiten schot te blijven (zie ook paragraaf 5.2 en hoofdstuk 6), wat lijkt te impliceren dat deze daders zich toch wel deels bewust waren van de strafbaarheid van hun gedragingen. Ook de daders zelf leggen een koppeling tussen de perceptie van de strafbaarheid/kwade intentie en het wel/niet nemen van beveiligingsmaatregelen. Zo geeft een dader aan dat hij zijn computer niet goed had beveiligd en de delicten ook onder zijn eigen naam heeft gepleegd, wat volgens hem laat zien dat hij er niet bij stilstond hoe fout het was. Een andere dader heeft door tijd heen meer maatregelen genomen naarmate zijn intentie veranderde. Zo legt hij uit:

> Ik had alles veilig gedaan behalve de eerste aanval, omdat ik toen geen intentie had. Ik had niet de intentie om het [systeem] te hacken en het helemaal te exploiten en zo. Ik had dus

geen VPN[71] gebruikt in het begin. Daarna had ik het wel gebruikt, zodat ze me nooit konden terug tracen. (Daderinterview 7)

5.2. Perceptie pakkans (gepleegde) cyberdelicten

In de literatuur wordt er veelvuldig op gewezen dat de kans om gepakt en vervolgens gestraft te worden voor cybercriminaliteit in enge zin laag is vergeleken met de pakkans bij andere soorten criminaliteit (Smith et al., 2004, p. 213). Dit heeft onder meer te maken met de juridische en technische complexiteit van de delicten, waardoor de delicten erg lastig zijn op te sporen en te vervolgen (Oerlemans, 2017). Zo kan zowel het bewijs als de dader zich in andere landen bevinden, waardoor de opsporing beperkt kan worden vanwege jurisdictieproblemen. In principe mag immers niet over de grens worden opgespoord, tenzij via – vaak langlopende – rechtshulpverzoeken een ander land toestemming geeft binnen diens territoriale grenzen bewijs te mogen verzamelen. Met de implementatie van de Wet computercriminaliteit III sinds 1 maart 2019 zou op dit vlak meer mogelijk worden (Oerlemans, 2017).

Diverse studies laten zien dat daders de pakkans laag inschatten. In het Verenigd-Koninkrijk is op basis van acht 'debrief gesprekken' met aangehouden daders van cybercriminaliteit in enge zin en tachtig *cease and desist* gesprekken geconcludeerd dat alle daders de kans klein achten opgepakt te worden (National Crime Agency, 2017). Volgens Hutchings (2016) gaan daders er vanuit dat de politie niet in staat is om de delicten op te sporen en daarnaast kunnen ze relatief eenvoudig hun identiteit verhullen. Conform de aannames uit de rationele keuzetheorie (Cornish & Clarke, 1986), veronderstelt Hutchings (2016) dat de pakkans een groter (afschrikkend) effect heeft op de dader dan de zwaarte van de mogelijke straf (zie ook Hutchings & Holt, 2017). Turgeman-Goldschmidt (2005) stelt dat zowel de pakkans als de hoogte van de straf laag is bij cybercriminaliteit, waardoor er nauwelijks sprake is van een afschrikkende werking bij de daders. Dit geldt ook voor de hackers die zij sprak, alhoewel er ook enkele respondenten waren die *wel* uitgingen van een hoge pakkans, maar zich daar niet door lieten weerhouden.

De meeste experts benadrukken dat de pakkans zeer laag is bij cybercriminaliteit in enge zin. Hoe groot de kans om opgepakt te worden is, hangt volgens de experts echter wel af van de vaardigheden waarover de dader beschikt en hoe goed de dader zich weet af te schermen. Daarnaast verschilt de pakkans per type delict. Bij het gebruikmaken van gestolen creditcardgegevens is de kans volgens een expert erg groot om tegen de lamp te lopen, omdat creditcardmaatschappijen per definitie aangifte doen. Het merendeel van de experts veronderstelt ook dat de meeste daders (behalve de jeugdigen die geen weet hebben van het feit dat ze iets strafbaars doen) zich ook heel bewust zijn van het feit dat de pakkans klein is. Het creëert volgens hen een gevoel van 'onaantastbaarheid' bij daders. Ze wanen zichzelf onzichtbaar en anoniem. De geïnterviewde experts menen voorts dat de strafhoogte in combinatie met de pakkans moet worden gezien. Als de pakkans klein is, wordt de hoogte van de dreigende straf op de koop toe genomen.

De meerderheid van de geïnterviewde daders geven ook aan dat ze de pakkans heel klein achtten toen zij zich bezighielden met het plegen van cyberdelicten en noemen hierbij ook de rol van onzichtbaarheid en anonimiteit. Zo geeft een respondent aan dat de kans veel groter is dat je wordt

[71] Een *virtual private network* (VPN) betreft een "uitbreiding van een computernetwerk over een openbaar netwerk. Via die uitbreiding kunnen gebruikers vanaf elke plek veilig gegevens delen met het computernetwerk. Voor de gebruikers is het alsof ze rechtstreeks op het netwerk zijn aangesloten. De veilige verbinding valt te omschrijven als een tunnel." (Oldengarm & Holterman, 2019).

gepakt bij een bankoverval dan voor een hack omdat je daar ook sneller weerstand kunt verwachten van de politie of mensen die proberen 'de held te spelen.' In deze quote zien we, conform de inzichten uit de routine activiteitentheorie en de rationale keuzetheorie, ook het belang van capabel toezicht terug in de belangenafweging van de dader. Bij cybercriminaliteit is er sprake van minder capabel toezicht zowel door burgers zelf als door de politie. Een andere respondent geeft aan dat hij, zodra hij thuis fysieke pakketjes ging ontvangen die aangekocht waren met gestolen creditcardgegevens, wel meer angst kreeg om opgepakt te worden. Het maakte hem paranoïde, vandaar dat hij hier ook snel weer mee is gestopt.

Waar het de anonimiteit betreft, geven de daders aan dat je diverse maatregelen kunt en moet nemen om jezelf af te schermen. Daarbij gaat het om het nemen van de juiste technische maatregelen (bijv. VPN, proxy servers), maar ook om jezelf zo onzichtbaar mogelijk te maken als het gaat om je persoonlijke informatie. Dit betekent bijvoorbeeld dat je geen sociale media gebruikt of nergens je eigen naam gebruikt. Ook hielden sommige respondenten bewust hun activiteiten verborgen voor hun naasten. Een ander aspect dat door daders genoemd worden in het kader van de pakkans is dat de kans relatief klein is dat ze net jou (uit de grotere pool van daders die actief is) er uitpikken.

De perceptie ten aanzien van de pakkans lijkt echter niet iets statisch te zijn. Zo stellen verscheidene experts dat het besef dat je gepakt kunt worden over de tijd 'wegebt' naar mate je er steeds vaker mee wegkomt, een aspect dat ook door verschillende daders naar voren wordt gebracht. Zo vertelt een respondent: "Ik was op den duur op het punt [beland] dat ik het al zo lang deed, dat ik dacht van, ze gaan me niet eens meer pakken" (Daderinterview 8).

Enkele respondenten hadden zich wel expliciet voorgenomen dat ze zouden stoppen op het moment dat ze gepakt zouden worden. Al met al suggereren de bevindingen dat het scenario om gepakt te worden wel bij de meeste daders in hun hoofd speelt, ook al schatten ze de pakkans laag in. Tegelijkertijd, zoals ook reeds in hoofdstuk 4 naar voren kwam, kan het besef dat er een risico bestaat om gepakt te worden, juist ook voor extra spanning zorgen en de adrenaline-kick vergroten.

5.3. Perceptie schade (gepleegde) cyberdelicten

Uit de literatuur komt naar voren dat de houding en perceptie ten aanzien van schade voor het slachtoffer, niet voor iedere cyberdader hetzelfde is. Zo laten studies over jeugdige cyberdaders zien dat jongeren, of ze zich nu met hacken of met cyberpesten bezighouden, de gevolgen van hun handelingen niet goed kunnen overzien en dat zij de schade bagatelliseren (o.a. Zebel et al., 2013). Ook ervaren ze de criminaliteit en de verhouding tot het slachtoffer als afstandelijk en emotieloos (Hoek van Dijke, 2016). Studies die op volwassen daders focussen gaan er vanuit dat de daders de financiële, technische of emotionele schade wel kunnen overzien, maar net als jeugdigen, gebruikmaken van neutralisatietechnieken (zie verderop in deze paragraaf).

Een soortgelijk beeld wordt geschetst door de experts. De meeste experts geven aan dat de gemiddelde jeugdige cyberdader zich tijdens het plegen van de daad niet of nauwelijks bezighoudt met de mogelijke schade die deze teweeg kan brengen. Ze stellen dat jonge daders tijdens het plegen van de daad lol ervaren of het grappig vinden, maar dat het besef van de schade ontbreekt. Volwassen daders (in het bijzonder de financieel georiënteerde daders zoals phishers) daarentegen zijn zich volgens veel experts wel goed bewust van de schade, maar lijken zich daar weinig om te bekommeren. Een advocaat geeft bijvoorbeeld aan dat deze dadergroep weleens wordt geconfronteerd met aangiftes en slachtofferverklaringen, maar beschrijft dat dit vaak boosheid oproept bij de dader omdat ze het wel weten, maar het hen niet interesseert. Een andere advocaat spreekt van een gebrek aan

empathie voor het slachtoffer, hetgeen volgens hem ook geldt voor de meeste traditionele daders van vermogensdelicten.

Daarnaast wordt er door de experts een categorie (volwassen) daders vermeld die er juist op uit is om schade te berokkenen, omdat ze bijvoorbeeld uit frustratie handelen of wraak willen nemen. In sommige gevallen beschouwen zij zichzelf als een slachtoffer en willen dan op deze manier hun daden rechtvaardigen. Ook komt het voor dat ze daadwerkelijk zelf het slachtoffer van criminaliteit zijn geweest en vervolgens een dader worden. Een reclasseringsmedewerker haalt een voorbeeld aan van een dader die onrecht was aangedaan door een familielid waar hij niet overheen kon komen en dat dit heeft geleid tot het plegen van een hack. Hacktivisten vallen volgens enkele experts ook onder de categorie daders die er bewust op uit is om schade aan te richten en daar bepaalde politieke of ideologische redenen voor heeft. De houding en perceptie ten aanzien van de schade lijkt daarmee niet alleen samen te hangen met de leeftijd, maar ook met de motivatie van de dader.

Rol van online omgeving en disinhibition

In de literatuur over cybercriminaliteit wordt steeds meer aandacht besteed aan de manier waarop de online omgeving invloed uitoefent op de perceptie van daders ten aanzien van de ernst van de delicten, maar ook de schade (zie bijv. Zebel et al., 2013). Hierbij wordt gewezen op sociale en psychologische aspecten van het internet die niet alleen voor jeugdige, maar ook voor volwassen daders van toepassing kunnen zijn. Een vaak aangehaald concept in deze context is het zogenaamde *online disinhibition effect*. Dit verwijst naar het feit dat mensen zich online anders gedragen en zich anders uitlaten dan in face to face interacties (Suler, 2004). Dit heeft volgens Suler (2004) vooral te maken met het feit dat men online anoniem is en een andere identiteit kan aannemen, waardoor bepaalde remmingen wegvallen. Ook kan hierbij sprake zijn van een zekere hyper-realiteit waarbij het onderscheid tussen fantasie en werkelijkheid niet meer scherp is. Iemand ervaart dan in een andere wereld of werkelijkheid te leven waarbij de verantwoordelijkheden die je normaliter hebt wegvallen.

Ook veel experts gaan er vanuit dat de online omgeving bepaalde remmingen wegneemt en, zoals eerder vermeld, dat de grenzen tussen goed en kwaad sneller vervagen in een online omgeving. De experts geven drie redenen waarom remmingen (zowel in emotioneel als moreel opzicht) online (deels) wegvallen.

Ten eerste is er online sprake van een andersoortige interactie met een eventueel slachtoffer. Zo is er volgens de experts geen directe confrontatie met het slachtoffer en het leed dat bij hem of haar veroorzaakt wordt (financieel of emotioneel). Dit kan ertoe leiden dat daders minder inlevingsvermogen hebben in het slachtoffer. Een van de daders benoemt in dit kader ook de anonimiteit van het slachtoffer zelf: “Je merkt niet eens wie je aan het hacken bent eigenlijk. Het is gewoon één grote oceaan en ik pak gewoon wat vissen eruit” (Daderinterview 8). Doordat het slachtoffer zo ongrijpbaar en abstract is, kan de dader relatief gemakkelijk de daad goedpraten en zich ook makkelijker van het slachtoffer distantiëren. De vraag is echter wel of dit een heel nieuw element is van de online omgeving. Een abstract slachtoffer treffen we ook aan bij traditionele vormen van criminaliteit zoals autodiefstal, waarbij de dief ook niet in aanraking komt met het slachtoffer (Morris, 2010). Mogelijk kan de online omgeving dit effect of vooral de *perceptie* van de dader van dit effect wel versterken.

Ten tweede gaan de experts er vanuit dat daders het bereik van hun handelen op het internet flink onderschatten, een aspect dat ook in de literatuur naar voren wordt gebracht. Zo stelt Hayward (2012, p. 17, in Van der Wagen, 2018) dat handelingen die online uitgevoerd klein en onschuldig lijken (in de subjectieve beleving van de dader), maar in werkelijkheid grote (fysieke) consequenties kunnen

hebben. Bij sommige delicten zoals het uitvoeren van een DDoS-aanval wordt de daad ook nog eens letterlijk gepleegd 'met een druk op de knop' terwijl dit gevolgen kan hebben voor grote aantallen individuen of bedrijven over de hele wereld. Ook de geïnterviewde daders, geven aan dat ze de schade niet goed konden overzien. Zo brengt een van de daders naar voren:

> Ik denk dat je online niet echt de schade ziet die jij veroorzaakt. Ik bedoel als jij in het echt een ruit ingooit, dan zie je het gelijk. Maar als je een DDoS-aanval uitvoert, je ziet iets dat plat gaat, maar voor de rest zie je er niks achter, wat er gebeurt achter de schermen. (Daderinterview 6)

Bovendien, als gesproken wordt over het uitvoeren van DDoS-aanvallen, wordt door verschillende daders ook niet gesproken over schade, maar vooral over iemand 'irriteren.' Daar komt bij dat het plegen van cybercriminaliteit zo gemakkelijk en goedkoop is geworden, dat het voor de dader moeilijk voor te stellen is dat de schade zo groot kan zijn en zelfs in de miljoenen kan lopen. Vermeldenswaardig in dit kader is dat experts (o.a. van de reclassering) zelf ook niet altijd precies weten wat de schade behelst (bijvoorbeeld van een DDoS-aanval), omdat slachtoffers (waaronder bedrijven) hier niet transparant over zijn. Voor deze reclasseringswerkers is dergelijke informatie in hun communicatie met de cliënt wel van toegevoegde waarde, omdat ze de daders hierdoor beter bewust kunnen maken van de schade.

Ten derde wordt door de experts gewezen op het feit dat daders in emotioneel opzicht minder geremd worden online doordat ze anoniem zijn en ze zich achter hun scherm kunnen verschuilen. Zo stelt een expert:

> Als je bijvoorbeeld een snackbar overvalt, als je geld wilt hebben, dan heb je er nogal wat voor nodig. Je hebt attributen nodig, maar je moet jezelf ook enorm oppompen. Het is namelijk een heel emotioneel iets, ook voor jou als dader. (Expertinterview 13, Officier van Justitie)

Ook enkele daders wijzen hierop en spreken in dit verband ook van een zekere 'moedwilligheid' die je voor het plegen van bepaalde offlinedelicten wel nodig hebt, maar online niet. Ook noemen zij in dit kader het gemak en de kleine pakkans. Cyberdelicten kun je vanuit thuis met enkele muisklikken voltooien, terwijl je voor een fysieke overval of woninginbraak ook naar buiten moet gaan en in 'letterlijke zin' ergens de deur moet binnen stappen.

De experts wijzen tot slot nog op het feit dat het plegen van cybercriminaliteit voor daders kan voelen als een 'spel', waardoor de perceptie van schade gering is en grenzen vervagen. Ook dit aspect wordt door diverse daders aangehaald om specifiek aan te geven dat zij en degenen om hen heen in de veronderstelling waren dat ze iets deden dat vrij onschuldig was. Hoewel het spelelement een terugkerend thema is als het gaat om de beleving van het plegen van cybercriminaliteit, kan een verwijzing hiernaar (door daders) tegelijkertijd ook een manier zijn om (achteraf) bepaalde gedragingen te bagatelliseren. Dit brengt ons bij de rol van neutralisatie.

Rol van neutralisatietechnieken

In de literatuur komt naar voren dat cyberdaders, net als traditionele daders, regelmatig gebruik maken van legitimeringen om hun gedrag te rationaliseren (Yar, 2005), ook wel neutralisatietechnieken genoemd (Sykes & Matza, 1957). Neutralisatietechnieken zijn manieren waarop daders het criminele of deviante gedrag goedpraten en zichzelf hiermee overtuigen dat ze

niet verkeerd handelen. Het feit dat cyberdaders online anoniem kunnen opereren kan dit proces volgens Aiken et al. (2016) versterken. De vijf technieken van neutralisatie die Sykes en Matza (1957) benoemen zijn: ontkenning van de verantwoordelijkheid (wat meestal impliceert dat de schuld bij iemand anders wordt neergelegd), ontkenning van de schade (de schade wordt gebagatelliseerd), ontkenning van een slachtoffer (het slachtoffer heeft verdiend wat hem of haar is overkomen), een beroep op hogere loyaliteiten (het delict wordt voor een ander veel belangrijker doel gepleegd) en veroordeling van de veroordelaar (de autoriteiten worden zelf als crimineel afgeschilderd, hetgeen de dader vrijpleit).

In bestaande studies op het terrein van cybercriminaliteit in enge zin komen al deze technieken terug (Rieb, Gurschler & Lechner, 2017; Turgeman Goldschmidt 2009). Zo claimen hackers regelmatig dat de systeembeheerders de beveiliging niet goed op orde hebben (ontkenning verantwoordelijkheid) en dat hun falen zichtbaar moet worden gemaakt (Furnell, 2009). Ook geven ze hierbij soms aan dat bedrijven vanwege hun slechte beveiliging de hack op zichzelf afroepen, waarmee de schuld dus ook (deels) bij de bedrijven zelf wordt gelegd (Van der Wagen et al., 2016). Dit betekent ontkenning van het slachtoffer. Voorts wordt de schade regelmatig ontkend door hackers. Ze geven bijvoorbeeld aan dat ze geen systemen kapot hebben gemaakt (Van der Wagen et al., 2016). Volgens Morris (2010) speelt juist het ontkennen van het slachtoffer een grote rol bij cybercriminaliteit, omdat er in cyberspace sprake is van een heel abstract en onzichtbaar slachtoffer. De dader krijgt dan al snel het gevoel dat er geen schade of slachtoffer is. Als het gaat om een beroep op hogere loyaliteiten wordt onder meer gewezen op het feit dat daders zwakheden in systemen willen blootleggen en een hack daarmee gerechtvaardigd vinden (Furnell, 2009). Een voorbeeld van de neutralisatietechniek veroordelen van de veroordelaars' is dat hackers kunnen aangeven dat bedrijven of instellingen die privacygevoelige informatie slecht beveiligen, crimineler bezig zijn hackers zelf (Van der Wagen et al., 2016).

De experts bevestigen het beeld dat cyberdaders gebruik maken van verschillende neutralisatietechnieken, maar veronderstellen dat het gebruik ervan verschilt per type dader naargelang de leeftijd en het motief. Veel experts veronderstellen, voornamelijk waar het gaat om jongere daders, dat er niet zozeer sprake is van ontkenning van de schade (als neutralisatietechniek), maar veeleer van een zekere onwetendheid. Zoals reeds beschreven, beseffen ze vaak niet dat de schade die ze aanrichten enorm kan zijn.

Daarnaast is er een categorie cyberdaders die hun daad neutraliseert door de schuld bij het slachtoffer te leggen. Bij hackers speelt volgens een expert de rechtvaardiging mee dat het slachtoffer 'dom is geweest' en het dus over zichzelf afroept. Een expert noemt in dit kader het voorbeeld van bedrijven die reclame maken voor een betaalapplicatie, maar gebruikmaken van verouderde certificaten. Juist bedrijven die claimen dat ze de beveiliging goed op orde hebben (maar in werkelijkheid niet), zijn aantrekkelijke doelwitten voor hackers.

Een vergelijkbaar sentiment heerst volgens de experts wanneer een kwetsbaarheid al lang bekend is, maar een bedrijf deze niet oplost. Ook kan er sprake zijn van een zekere wrok jegens het slachtoffer. Zo vertelt een van de experts dat er verdachten zijn die grote bedrijven als hun vijand zien, bijvoorbeeld vanwege het plaatsen van een *web block*[72] waardoor hun uitingsvrijheid wordt aangetast. De daders proberen dan vervolgens om het bedrijf 'stuk te maken'. Ook deze daders hebben dan het gevoel dat het slachtoffer krijgt wat het verdient.

[72] Waarbij bepaalde websites worden geblokkeerd.

Bij de categorie financieel georiënteerde cyberdaders is er volgens een expert ook sprake van bagatellisering van schade. Een expert stelt bijvoorbeeld dat deze daders aangeven alleen van rijke mensen te stelen omdat ze toch genoeg geld hebben. Op deze manier lijkt de daad dan gerechtvaardigd te worden. Hierbij is het vermeldenswaardig dat mensen met een middeninkomen volgens de expert ook al rijk zijn in de ogen van de dader, omdat ze een salaris hebben en spaargeld.

Tot slot is er volgens sommige experts een categorie daders die het slachtoffer ontkent door juist zichzelf als een slachtoffer te beschouwen en daarmee hun daden rechtvaardigt. Zo vertelt een reclasseringsmedewerker dat er een subgroep daders is die het gevoel heeft dat ze een slachtoffer zijn, waarbij dit slachtofferschap verschillende vormen kan aannemen. Het kan zijn dat de dader zich getreiterd voelt, bijvoorbeeld doordat gesteld wordt dat hij iets niet kan, waarbij er een link te leggen is met de in hoofdstuk 4 besproken bewijsdrang. Hiernaast stelt deze expert dat veel daders ook daadwerkelijk zelf het slachtoffer van criminaliteit zijn geweest en vervolgens zelf een dader worden.

Het gebruik van neutralisatietechnieken zien we ook terug in diverse daderinterviews. Hoewel enkele daders aangeven spijt of berouw te hebben van bepaalde dingen die ze hebben gedaan of in ieder geval aangeven hier en daar wat te ver zijn gegaan, wordt de schade door de respondenten doorgaans in mindere of meerdere mate gebagatelliseerd. Zo geven sommige daders aan dat ze wel vinden dat ze slechte dingen hebben gedaan, maar dat er toch vormen van criminaliteit bestaan die vele malen ernstiger zijn. Zo stelt een respondent die betrokken was bij het hacken van accounts om vervolgens seksuele getinte foto's te verkrijgen: *"*Ik ben geen moordenaar of zware crimineel. Ik heb slechte dingen gedaan, dat zal consequenties hebben. Maar ja, je hoeft het ook niet erger te maken dan dat het is natuurlijk" (Daderinterview 3).

Enkele andere daders geven meer in algemene zin aan dat ze cybercriminaliteit een minder ernstige vorm van criminaliteit vinden dan bijvoorbeeld moord of verkrachting, omdat je daarmee het slachtoffer "niet onmiddellijk raakt". Ze kunnen zich wel voorstellen dat er vormen van cybercriminaliteit zijn waarbij dat anders is. Een dader haalt hierbij het voorbeeld aan van het platleggen van een kerncentrale, omdat je dan extreem belangrijke systemen beschadigt.

Een ander deel van de daders legt de schuld (gedeeltelijk) bij het slachtoffer neer, waarbij voornamelijk gewezen wordt op de extreem of 'belachelijk' zwakke wachtwoorden die de slachtoffers gebruikten en/of op het feit dat mensen overal dezelfde wachtwoorden gebruiken. Zo zegt een van de respondenten: "Ze hebben het er een beetje naar gemaakt. Ze hebben praktisch gezegd: welkom, kom binnen" (Daderinterview 7).

Sommige daders vinden ook om deze specifieke reden, het feit dat het zo simpel was om een individu of bedrijf in kwestie te hacken, dat het onterecht is dat ze er zo'n zware straf voor hebben gekregen. Daders kunnen ook een soort sentiment hebben van 'je roept het kennelijk over jezelf af' jegens het slachtoffer.

Ook zijn er enkele respondenten die de schade ontkennen, omdat ze naar eigen zeggen alleen gegevens hebben gekopieerd en niets hebben vernield of gestolen. Om deze reden veronderstellen ze dan ook niet dat ze iemand er kwaad mee hebben gedaan. Turgeman-Goldschmidt (2005) spreekt in deze context dan ook van *intangible offenses* (niet-tastbare delicten), omdat er niet zoals bij reguliere diefstal in fysieke zin dingen weggenomen worden en dat het dan ook niet als diefstal ervaren wordt. Ook wordt nog genoemd dat het slachtoffer het geld toch wel terugkrijgt van de bank of dat een bedrijf een beetje geld wel kan missen, wat wederom een klassiek voorbeeld is van ontkenning van de schade als neutralisatietechniek.

Rol van eigen moraal

Zoals in de vorige paragraaf uiteengezet is, zien we verschillende neutralisatietechnieken terugkomen die ook door traditionele daders worden gebruikt. Een interessant discussiepunt hierbij is of de betekenis van deze rationalisaties voor beide soorten daders identiek is. Het oorspronkelijke idee van neutralisatie zoals voorgesteld door Sykes en Matza (1957) is het principe van een 'morele vakantie.' De dader weet wel dat hij iets doet wat niet mag, maar zet de normen die in de samenleving gelden tijdelijk buitenspel. Tijdens en/of achteraf gaat hij het gedrag goedpraten. Hoewel neutralisaties ook deze functie kunnen hebben voor cyberdaders, is het wel de vraag of er altijd sprake is van het tijdelijk naast zich neerleggen van bestaande normen. Zo komt uit verschillende studies over hacken naar voren dat hackers zich vaak expliciet verzetten tegen bestaande normen en in plaats daarvan hun *eigen* normen hanteren. Ze denken zelf beter te weten waar de grens tussen goed en kwaad ligt en zien zichzelf soms ook als een soort moraalridders (Van der Wagen et al., 2016; Steinmetz, 2015b). Volgens Xu et al. (2013) is er bij hackers sprake van een *moral disengagement*. Hacken wordt als acceptabel beschouwd zolang er geen schade is.

De observatie dat cyberdaders, vooral waar het hackers betreft, een sterke eigen moreel hebben, dus voor zichzelf duidelijke grenzen hebben opgesteld van wat wel en wat niet kan en zich daarbij weinig lijken aan te trekken van de strafrechtelijke grens, wordt ook door verschillende experts vermeld. Een cybersecurityexpert haalt als voorbeeld een dader aan die van mening was dat het hem wel toegestaan was om een systeem binnenkomen, maar dat het stelen van creditcardgegevens of foto's voor hem een stap te ver zou zijn. Ook diverse geïnterviewde daders, lijken eigen grenzen te stellen als het gaat om goed en kwaad. Uit de interviews komen vier soorten grenzen naar voren, namelijk financieel gewin, misbruik maken van gegevens, privacy/vertrouwelijkheid van gegevens en het vernietigen/veranderen van gegevens. Een eerste grens die getrokken wordt is het financiële aspect. Zodra er sprake is van aanzienlijk financieel gewin of afpersing, wordt hacken als criminaliteit of stelen gezien. Daarbij is er voor sommige respondenten wel een verschil tussen geld wegnemen van een bedrijf of van individueel persoon. Zo legt een respondent uit:

> Ik heb in het verleden dan wel die [website] hosting gratis gekregen, dat ik dacht van nou dat is wel heel makkelijk, ik kan gewoon een random [bank]nummer invullen en ik krijg gewoon gratis hosting. Ik wou dan niet dat het dan bij iemand anders wordt afgeschreven, daar ligt wel de grens. (Daderinterview 11)

Een tweede grens, die door meerdere daders wordt getrokken, ligt bij het daadwerkelijk misbruik maken van de gegevens die je middels hacken verkrijgt, wat ook nauw verwant is aan het financiële aspect. Bij misbruik gaat het bijvoorbeeld om oplichting, spullen kopen met verkregen gegevens of gegevens verkopen of verspreiden. Volgens een van de daders bestaat er een groep hackers (waar hij ook toe behoorde) die wel heel graag (op grote schaal) wachtwoorden binnenhaalt, omdat het hen een kick en macht geeft, maar deze niet daadwerkelijk misbruikt. Hij schaart deze categorie onder de noemer *grey hat* hackers, omdat ze op de grens opereren. Een andere respondent spreekt in deze context van een verantwoordelijkheidsgevoel. Op het moment dat je toegang weet te verkrijgen tot gevoelige informatie, wil je dat volgens hem niet uit handen geven, omdat je dan niet weet wat ermee gaat gebeuren.

Een derde, hiermee nauw verbonden grens die wordt getrokken, ligt meer in de sfeer van de vertrouwelijkheid van gegevens en de privacy. Verschillende respondenten geven aan dat ze het te

ver vinden gaan op het moment dat persoonlijke gegevens op straat terecht komen. Zo legt een dader uit:

> Ik weet wel een beetje de grens of zo. Ik heb ook wel veel mensen gehackt natuurlijk, dan kom je ook wel dingen tegen waarvan je zeker wel weet dat die persoon dat privé wilt houden. Zulke dingen zet ik dan ook niet online. Ik heb wel een bepaalde grens, ik ga niet iemands leven helemaal kapot maken of zo. (Daderinterview 8)

Een vierde grens die wordt genoemd, die eerder ook al bij de bespreking van de neutralisatietechnieken aan bod kwam, ligt bij het wel of niet kapotmaken van systemen of het veranderen van gegevens. Als daar sprake van is, wordt volgens verschillende respondenten een grens overschreden. Met andere woorden, als je het 'voor de techniek doet' is het niet crimineel.

5.4. Conclusie

In dit hoofdstuk is achtereenvolgens stilgestaan bij hoe daders van cybercriminaliteit in enge zin aankijken tegen de strafbaarheid van cyberdelicten, de pakkans en de schade van de (gepleegde) delicten. Als het gaat om de perceptie ten aanzien van strafbaarheid lijkt sprake te zijn van een glijdende schaal. Aan de ene kant van de schaal bevinden zich (veelal jonge) daders die zich niet of nauwelijks bewust zijn van de strafbaarheid en aan de andere kant daders die dat wel zijn en bijvoorbeeld via fora goed op de hoogte zijn van de straffen die ze riskeren.

De gebrekkige perceptie van strafbaarheid, die aanwezig is bij een deel van de dader komt deels voort uit de onzichtbaarheid van de aangerichte schade. Ook bestaat er bij sommige daders onduidelijkheid over de juridische grenzen.

De pakkans schatten daders over het algemeen erg laag in vanwege beperkte politiecapaciteit en mogelijkheden voor anonimisering. De bevindingen laten tevens zien dat daders het risico om gepakt te worden over tijd, naarmate men vaker ongezien wegkomt, steeds lager gaat inschatten.

Ten aanzien van de perceptie van de schade is naar voren gekomen dat daders, vooral jonge daders, de omvang en ernst van de schade als gering inschatten alsook de schade bagatelliseren of ontkennen (neutralisatie). Hoewel ontkenning van het slachtoffer of de aangerichte schade ook bij daders van traditionele criminaliteit voorkomt, wordt dit online versterkt door de afstand tot slachtoffer, de hyperrealiteit waarin het gedrag tot stand komt (het voelt als spel), de normalisering die ontstaat door gamen (waar het routine en normaal is om elkaar te DDoSsen of te hacken) en door het gemak waarmee bepaalde delicten (in hoge frequentie) gepleegd kunnen worden. Tevens zorgt de online omgeving voor minder remmingen vanwege afwezigheid van het oordeel van anderen of andere gevreesde consequenties. Tegelijkertijd is het een discussiepunt of de functie van deze neutralisatietechnieken identiek is aan die van traditionele daders, vanwege het feit dat er bij een deel van de daders, sprake is van een sterk eigen moraal.

Hoofdstuk 6 Criminele carrière

Als het gaat om de criminele carrière van (cyber)daders wordt in de literatuur doorgaans gesproken over *pathways* (Aiken et al., 2016; Xu et al., 2013) of *trajectories* (Hutchings, 2016). Een focus op paden of trajecten impliceert dat men in kaart wil brengen hoe het delinquente gedrag van een dader zich ontwikkelt door de tijd heen, van initiatie tot stoppen (*desistance*), en welke factoren daar invloed op uitoefenen. Dergelijke inzichten zijn van groot belang voor de vraag welke interventies wanneer passend kunnen zijn. Er zijn slechts vijf (empirische) studies gevonden waarbij de criminele carrières van daders van cybercriminaliteit in enge zin zijn onderzocht (Aiken et al., 2016; Brewer et al., 2018; Hutchings, 2016; Kao et al., 2009; National Crime Agency, 2017; Xu et al., 2013). Hierbij kan een onderscheid gemaakt worden tussen studies die alleen op de paden van jongeren focussen (Aiken et al., 2016; Kao et al., 2017; National Crime Agency, 2017) en studies die (ook) naar de paden van volwassen daders kijken (Hutchings, 2016). In deze studies is vooral gebruik gemaakt van expertinterviews en/of dossieronderzoek (Aiken et al., 2016; National Crime Agency 2017) en zelfrapportage (Brewer et al., 2018) en in sommige gevallen zijn ook daders geïnterviewd (o.a. Hutchings, 2016; Kao et al., 2013). In dat laatste geval gaat het doorgaans wel om zeer kleine daderpopulaties (N=6).

In dit hoofdstuk wordt niet zozeer beoogd verschillende paden uit te stippelen, maar vooral om op basis van de literatuur, expert- en daderinterviews, inzichten te geven in de factoren die van invloed zijn op de criminele carrière van cyberdaders. Daarbij wordt zowel ingegaan op het ontstaan en de ontwikkeling van de criminele carrière als op de vraag wat daders (los van de interventie) doet stoppen. De rol die interventies kunnen spelen bij het stoppen bespreken we in hoofdstuk 7 en 8.

Zoals reeds naar voren is gekomen, is de groep cyberdaders nogal divers qua leeftijd, delicten, motieven en vaardigheden, wat ook maakt dat de factoren die tot het delictgedrag leiden verschillend kunnen zijn voor verschillende (type) daders. De nadruk ligt in dit hoofdstuk voornamelijk op de factoren die een rol spelen bij jonge en jongvolwassen daders en in mindere mate bij de wat oudere daders en 'late starters.' De eerste reden hiervoor is dat we relatief meer te weten zijn gekomen over jeugdige daders. Zo pleegde het merendeel van de door ons geïnterviewde daders hun delicten toen ze nog niet volwassen waren. De tweede reden, wat tegelijkertijd een bevinding is van dit onderzoek, is dat het bij de groep late starters van cybercriminaliteit vaak om traditionele daders lijkt te gaan die de overstap hebben gemaakt naar cybercriminaliteit (voornamelijk phishing) en/of dit combineren met traditionele delicten. Deze daders maken dus een late start met specifiek cybercriminaliteit, maar zijn geen late starter als het gaat om traditionele vormen van criminaliteit. Aangezien zij naar alle waarschijnlijkheid qua profiel niet heel sterk afwijken van de traditionele dader, beperken we ons in dit hoofdstuk tot die factoren die een rol spelen bij het feit dat zij in hun criminele carrière een (gedeeltelijke) overstap hebben gemaakt naar cybercriminaliteit.

Daders die betrokken zijn bij hacken in de conflictsfeer, waarbij het doorgaans niet om zeer geavanceerde hacks gaat (zoals het raden van het wachtwoord) of daders die betrokken zijn bij hacken in de zedensfeer (waarbij het soms wel en soms niet om geavanceerde technieken gaat), behandelen we om soortgelijke redenen ook niet in dit hoofdstuk. Ons inziens kunnen we hun criminele carrière en de factoren die daarbij een rol spelen beter situeren in respectievelijk het domein van conflict-gerelateerde delicten en zedendelicten, ook al plegen zij in formele zin ook cybercriminaliteit in enge zin. Dat betekent ook dat de bevindingen uit enkele daderinterviews minder prominent aan bod zullen

komen in dit hoofdstuk.

Het hoofdstuk bestaat uit drie delen. In paragraaf 6.1 wordt ingegaan op de factoren die een rol spelen bij de initiatie. Paragraaf 6.2 focust op de ontwikkeling en (eventuele) rijping van de criminele carrière en in paragraaf 6.3 worden factoren besproken die invloed uitoefenen op *desistance*.

6.1. Initiatie

Op basis van de literatuurstudie, expert- en daderinterviews kunnen verschillende criminogene factoren aangewezen worden die een rol spelen bij de initiatie. Afhankelijk van verschillende andere factoren, zoals de leeftijd en motivatie, hebben ze in mindere of meerdere mate impact op het ontstaan en de verdere ontwikkeling van de criminele carrière. Deels gaat het om factoren die veranderlijk (dynamisch) zijn, waarmee ze vanuit de *What Works* benadering ook belangrijk zijn in het kader van de vraag waarop de interventie zich moet richten.

6.1.1. Rol van *maturity gap*

Zoals reeds beschreven, lijkt daderschap van cybercriminaliteit in enge zin zich in veel gevallen te beperken tot de adolescentie. Als gevolg daarvan wordt in bestaande studies over cybercriminaliteit (o.a Yar, 2005; Aiken et al., 2016) vooral naar (traditionele) verklaringen gekeken op het terrein van jeugdcriminaliteit, waaronder het twee paden-model van Moffitt (1993). Daders die vooral tijdens de adolescentie delinquent gedrag vertonen, worden door Moffitt *adolescence-limited (*AL) daders genoemd. Het verloop van hun criminele carrière wordt verklaard door de zogenaamde *maturity gap*: een discrepantie tussen fysiek (biologisch) en maatschappelijk (in de ogen van anderen) volwassen zijn. Adolescenten streven in deze turbulente periode onafhankelijkheid na, willen zich onttrekken aan het ouderlijk gezag of controle en zijn eveneens op zoek naar de eigen identiteit. De bevestiging van *peers* is daarbij erg belangrijk (Warr, 2002). Volgens Moffitt (1993) ontstaat delinquent gedrag dan doordat het een statusverhogend effect heeft. Het gedrag wordt volgens haar afgekeken van zogenaamde *life-course-persistent* (LCP) delinquenten, delinquenten die al op jonge leeftijd (ernstig) delinquent gedrag vertonen en die zich niks aan lijken te trekken van regels en verboden en daarmee volwassen privileges verkrijgen (bijv. geld). Door al deze factoren is de AL-dader tijdens de adolescentie vatbaarder voor delinquent gedrag. Wat daarbij ook nog meespeelt is dat jeugdigen in deze fase vaak nog over onvoldoende cognitieve of psychosociale inzichten beschikken in normatieve kwesties (Eisenberg, Sadovksy, Spinrad, Fabes & Losoya, 2005; Moffitt, 1993; Warr, 2002), ook wel aangeduid met de term *ethical deficit* (DeMarco, 2001). Toch weten AL-daders volgens Moffitt (1993) wel in welke situaties pro-sociaal gedrag meer oplevert dan antisociaal gedrag, hetgeen ook weer verklaart dat ze op een gegeven moment weer stoppen.

Alhoewel cyberdaders, zoals aangegeven in hoofdstuk 3, in sommige gevallen al vanaf hun tiende starten met het plegen van delicten, kunnen we er vanuit gaan dat de *maturity gap* en de hiermee gepaard gaande factoren ook grotendeels op hen van toepassing zijn (Aiken et al., 2016). De vroege(re) start kan (in ieder geval deels) verklaard worden door het feit dat jeugdigen op jonge leeftijd al gamen en online zijn en via die kanalen worden blootgesteld aan cyberdelinquent gedrag (zie ook 6.1.2 en 6.1.4). Het patroon en de kenmerken van de LCP-dader (o.a. lage zelfcontrole en ernstige persoonlijkheidsstoornissen) lijkt op basis van onze bevindingen in mindere mate van toepassing te zijn op cyberdaders of in ieder geval niet één op één van toepassing te zijn. Zo bleek onder meer in hoofdstuk 3 dat een deel van de cyberdaders (ook daders die veel/ernstige delicten

plegen), anders dan traditionele daders, juist over een hoge zelfcontrole beschikt. Ook suggereren onze bevindingen (voornamelijk de literatuur en expertinterviews) dat er mogelijk andere soorten problematiek een rol kunnen spelen bij (een deel van de) cyberdaders, bijvoorbeeld problemen die voortvloeien uit een autisme spectrum stoornis. In dat opzicht sluiten we niet uit dat er ook een LCP-variant bestaat van de cyberdader.

Door de experts wordt vooral een relatie gelegd tussen de adolescentiefase (het AL-patroon) en het ontstaan en de ontwikkeling van de criminele carrière van cyberdaders. Hierbij worden aspecten aangehaald zoals autoriteitsproblemen, impulsiviteit en gevolgen van handelingen niet goed kunnen overzien. Ook de geïnterviewde daders leggen geregeld zelf, wat in sommige gevallen ook een neutralisatietechniek zou kunnen zijn, een verband tussen hun jonge leeftijd en het plegen van delicten, wat zichtbaar is in uitspraken als: “ik was nog een kind”, “ik was een jochie”, “ik was kinderlijk bezig”, “het was onvolwassen”“als tiener dacht ik zo.” Ook worden door hen aspecten aangehaald die met *de maturity gap* in verband kunnen worden gebracht zoals autoriteitsproblemen, impulsiviteit en behoefte aan bevestiging van *peers* (zie verder 6.1.4). In combinatie met deze *maturity gap* spelen ook meer technische en online factoren een rol, waar hieronder verder op wordt ingegaan.

6.1.2.Interesse in computertechnologie en/of gamen

Voor een deel van de cyberdaders, voornamelijk jongeren en jongvolwassenen, geldt dat er al van jongs af aan, voordat er überhaupt sprake is van een criminele carrière, veel interesse en fascinatie is voor en affiniteit met ICT en/of gamen (o.a. Aiken et al., 2016; National Crime Agency, 2017; Dupont, 2014; Holt, Burruss & Bossler, 2010; Xu et al., 2013). Waar het interesse in ICT betreft, gaat dit gepaard met het graag willen ontdekken en exploreren van nieuwe dingen en het willen begrijpen van hoe elementen van computersystemen met elkaar interacteren (Holt et al., 2010; Van der Wagen, 2018). De in hoofdstuk 4 besproken nieuwsgierigheid en leergierigheid komt hier dan ook in terug. Overeenkomstig de literatuur stellen de experts dat deze interesse in ICT zich bij een deel van de daders al op jonge leeftijd manifesteert, wat overigens ook voor ‘reguliere’ IT-ers kan gelden die nooit een cyberdelict hebben gepleegd. Ook een deel van de daders (voornamelijk de hackers) die wij hebben gesproken geven aan al van jongs af aan interesse in IT/computers te hebben. In de meeste gevallen begon de interesse in IT tussen zes en acht jaar, maar ook was er een respondent die aangaf al op driejarige leeftijd met de computer van zijn vader bezig te zijn en al op zesjarige leeftijd leerde hoe computerprogramma’s opgebouwd zijn.

Ook geven enkele geïnterviewde daders aan dat ze zelf gehackt zijn in een spel en dat het hier allemaal mee begon. Het gehackt worden triggerde niet zozeer een wraakgevoel, maar vooral interesse in hoe het in zijn werk gaat. Zo vertelt een respondent:

> De eerste ervaring met hacken was toen ik zelf gehackt werd, dat was op Habbo Hotel, ik had daar best wel wat geld in gestoken als kind en toen werd ik gehackt, dat was niet zo leuk. Ik ben toen gaan uitzoeken hoe dat gekomen is… Daar begon mijn interesse, toen begon ik het uit te zoeken en kwam ik op onzin als illegaaltje.nl. Toen ik langzaam die kennis begon te vergaren, kwam ik er achter dat het best lastig was. Dat is hoe het begonnen is. (Daderinterview 12)

Een interesse voor IT of gamen is uiteraard geen op zichzelf staande criminogene factor voor cybercriminaliteit, maar is zeker wel van belang om te duiden hoe jongeren in de cyber(criminele) wereld verzeild kunnen raken. Volgens Xu et al. (2013) (zie ook Árpád, 2013) speelt een gebrek aan

uitdaging op school een belangrijke rol bij daders met veel affiniteit voor computers. Deze groep is intelligent, maar heeft een hele specifieke interesse in ICT-vakken (die er niet of nauwelijks zijn of van slechte kwaliteit zijn). Andere (niet-IT) vakken vinden ze niet interessant of kunnen ze met gemak halen. Ze raken dan verveeld en komen met hacken in aanraking. Zoals in hoofdstuk 4 besproken is, zijn er verschillende experts die deze bevinding ondersteunen en ook is het in verschillende daderinterviews terugkomen. Het lijkt dus zeker een factor van betekenis te zijn als het gaat om het ontstaan van de criminele carrière.

Indien iemand veel gamet, kan men, zoals hierboven besproken, ook met cybercriminaliteit in aanraking komen. Interesse hebben in ICT is hierbij niet altijd aan de orde. De nieuwsgierigheid voor cybercriminaliteit kan hier wel gestimuleerd worden omdat het tamelijk gebruikelijk is om elkaar in games te hacken of een DDoS-aanval uit te voeren. Zo beschrijft een van de daders het spel dat hij speelde als 'maffiapraktijken voor kinderen', omdat er van elkaar gestolen werd en er gehackt en gegokt werd. Een dader die betrokken was bij het uitvoeren van DDoS-aanvallen gaf aan dat hij via gamen met DDoS-aanvallen te maken kreeg. In het desbetreffende spel was dit een normale en veelvoorkomende praktijk en hij deed daar ook aan mee. Op een gegeven moment is hij dit ook buiten de spelcontext gaan doen. Het spelen van deze games lijkt derhalve ook een zekere normalisering of normvervaging te weeg te brengen. Daar komt bij dat het plegen van sommige delicten ook wel erg eenvoudig kan zijn, wat onder meer samenhangt met de beschikbaarheid van kant-en-klare tools.

6.1.3. Beschikbaarheid van (kant-en klare) tools

Er lijkt in toenemende mate door hackers en andere daders gebruik gemaakt te worden van kant-en-klare tools. Wat dit betekent voor de criminele carrières van de daders is niet eenduidig te beschrijven. In de eerste plaats blijkt voor een deel van de daders de beschikbaarheid van en de gemakkelijke toegang tot kant-en-klare tools een belangrijke katalysator te zijn geweest bij hun instap in cybercriminaliteit. Dit is een ontwikkeling van de laatste jaren (Brewer et al., 2018; National Crime Agency, 2017; Van der Wagen, 2018) die zowel bij de jeugdige als volwassen daders zichtbaar is. Bij jeugdigen wordt dan vaak gesproken over scriptkiddies, (tiener)hackers die over de minste vaardigheden beschikken en gebruik maken van bestaande geautomatiseerde hacktools (Broadhurst et al., 2014; Kirwan & Power, 2013). Sommige auteurs scharen niet alleen hackers, maar ook uitvoerders van DDoS-aanvallen onder deze categorie (o.a. Hoek van Dijke, 2016). Experts doen dat over het algemeen ook. Als reden geven ze aan dat je een DDoS-aanval relatief gemakkelijk online kunt bestellen en met een paar muisklikken kunt uitvoeren. Een van de experts noemt deze groep daders dan ook '*plug-and-play* criminelen' om het gemak te bedrukken. Ook daders zelf leggen in eerste instantie de nadruk op de eenvoud. Ze geven aan het uitvoeren van een DDoS-aanval zo simpel en kinderlijk te vinden, dat je het geen cybercriminaliteit kunt noemen. Bij cybercriminaliteit denken ze toch meer aan de 'slimme' criminaliteit en iets waar je vaardigheden voor nodig hebt. Zo stelt een respondent:

> DDoS is voor sukkels. Het is ook niet hacken, het is gewoon letterlijk, je betaalt aan een website geld en je vult een IP-adres in en ze liggen plat. Dat vind ik niet hacken, daar was ik altijd zwaar tegen. Het is zo simpel, maar het is ook zo fucked up gewoon. (Daderinterview 8)

Tegelijkertijd wordt aangegeven dat het ook een kwestie is van het op een slimme manier inzetten van bestaande tools. Het wel of niet gebruiken van bestaande tools is dus niet per definitie een

afspiegeling van iemands kunnen. Zo beschrijft een van de daders dat het uitvoeren van een DDoS-aanval dan wel kinderlijk eenvoudig is, maar dat je het wel op een slimmere manier kunt inzetten. Hij heeft naar eigen zeggen meerdere stressers[73] gekocht en vervolgens zelf een applicatie geschreven die de stressorfunctie herhaalt, waardoor hij een krachtig soort van botnet had gemaakt van stressers. Een politie-expert haalt ook een voorbeeld aan van een uitvoerder van DDoS-aanvallen die klein begon, maar op een gegeven moment ook botnets wist te bouwen. Hij spreekt in dit kader van een ontwikkelpad. De dader begon als een beginneling die een beetje aan het inlezen was op fora, ging zelf dingen beginnen te bouwen en groeide uit tot een relatief 'grote cybercrimineel.' Met andere woorden, het gebruik van bestaande tools kan in veel gevallen als een beginfase beschouwd worden van de criminele carrière, of ze nu wel of niet verder professionaliseren.

Experts leggen sterk de link tussen technische vaardigheden en het zelf kunnen schrijven van scripts, vaardigheden die volgens de experts verkregen worden via instructies op fora, YouTube en Google en eventueel met hulp van anderen. Verscheidene daders denken hier anders over. Ook als je in staat bent om zelf tools te *maken* ben je volgens de daders niet per definitie een goede hacker. Zo stelt een dader dat het juist voordelen kan hebben om niet je eigen tools te programmeren, omdat je dan op een andere manier naar systemen en kwetsbaarheden kijkt.

> Ik denk dat, soms heeft het een soort van bonus als je het [programmeren] niet kan. Ik weet niet of dat logisch is, maar als je heel goed weet hoe je tooling kunt gebruiken en hoe je flaws [weet te ontdekken] en je weet hoe die systemen opgebouwd zijn, dan kan je er soms meer mee dan dat je scriptjes kunt schrijven. (Daderinterview 12)

Sommige daders geven aan het gewoon fijner te vinden om met eigen tools te werken en weer anderen doen allebei, bijvoorbeeld omdat ze niet steeds "het wiel opnieuw willen uitvinden". Deze bevindingen bevestigen ook de aanname van Holt en Kilger (2008) dat hackers die gebruik maken van bestaande tools niet per se minder vaardig zijn dan hackers die zelf tools schrijven. Het is meer een kwestie van een keuze of mentaliteit.

Bij de groep daders die de overstap maakt van traditionele criminaliteit naar cybercriminaliteit worden kant-en-kant klare tools (ook) beschouwd als een essentiële factor die hen in staat stelt om deze overstap te maken. In dit kader wordt zowel in de literatuur als door de experts van *crime as a service* gesproken. De experts beschrijven diverse casussen waarin dat zichtbaar is. Een politiemedewerker geeft een voorbeeld van een fraudezaak waarbij er geen enkele dader was die IT-vaardig was. Het waren oudere beroepscriminelen die helemaal geen verstand hadden van IT. Ze hadden alleen geld nodig om het kant-en-kant klare phishing pakket te kopen en hoefden het alleen maar te installeren en 'het trucje' te leren. Ook zijn er voorbeelden van casussen waarbij slechts een lid van de groep IT-vaardig is en waarbij de rest traditionele beroepscriminelen zijn. Uit bestaand onderzoek op basis van politiedossiers (o.a. Leukfeldt et al., 2017b; Odinot et al., 2017) komen deze daders met elkaar in contact komen via werkconnecties, rekrutering online of via het bestaande sociale netwerk.

Ook bij deze groep is het onderscheid tussen wel en niet-vaardig zijn, niet altijd zwart-wit. Sommige daders hebben volgens de experts bijvoorbeeld wel de kennis en vaardigheden om hun identiteit af te schermen, maar bezitten voor het plegen van het delict zelf geen technische kennis.

[73] Een IP-stresser is een tool om de robuustheid van een netwerk of server te testen en kan gebruikt worden voor het uitvoeren van een DDoS-aanval.

Tot slot moet ook het belang van *social engineering* als vaardigheid, zowel bij jeugdige als volwassen daders, niet onderschat worden, waarbij de dader middels deceptie gegevens beoogt te verkrijgen van slachtoffers zoals wachtwoorden of pincodes. Eén van de geïnterviewde daders die betrokken was bij identiteitsfraude en phishing gaf aan niet te kunnen hacken (hij had zich daar ook niet in verdiept), maar dat hij wel goed in staat was om (nep)websites te maken, die er 'gelikt' uit te laten zien en ook manieren wist te bedenken om zoveel mogelijk slachtoffers naar dergelijke websites toe te lokken.

6.1.4. Invloed (online) *peers*

Cyberdaders opereren over het algemeen niet solistisch. Ze maken vaak deel uit van online gemeenschappen, waar ze informatie, ideeën en tools uitwisselen (Nycyk, 2016), partners vinden en soms ook vriendschappen vormen (Hutchings, 2016). Goldsmith en Brewer (2015) spreken in dit kader van sociale *affordances*, wat verwijst naar het feit dat de toegankelijkheid tot de 'juiste' mensen zoveel makkelijker is dan in de offline wereld, wat op zijn beurt de schaal en het bereik van de criminaliteit kan vergroten.

Waar het jeugdigen betreft, wordt in de literatuur gewezen op de essentiële *sociale* rol van hackerfora en/of gamefora bij de initiatie en ontwikkeling (Holt, 2005; Hutchings, 2016; National Crime Agency, 2017). Voor veel jonge daders bieden dergelijke fora het gevoel ergens bij te horen en ze geven hen ook de kans om zichzelf te bewijzen (Aiken et al., 2016; National Crime Agency, 2017). Dergelijke fora fungeren dan als een virtuele *peer group* waarbij gelijkgestemde peers elkaar kunnen vinden (Morris & Blackburn, 2009). Tevens is het de plek waar normen, waarden en pro-criminele attitudes worden overgedragen, gevormd en bekrachtigd (Van Merkom, 2017). Hutchings (2016) verklaart dit proces in het licht van de differentiële associatietheorie van Sutherland (1947). Deze theorie gaat ervan uit gaat dat delinquent gedrag (en de daarmee gepaarde technieken, normen en waarden, attitudes en neutralisaties) aangeleerd wordt in hechte groepen. Dergelijke leerprocessen komen ook op online fora terug (Van Merkom, 2017). Ook de experts zien hack/gamefora als platformen die een sturende rol kunnen hebben in het al dan niet starten van een cybercriminele carrière. Het is volgens experts niet alleen het elkaar opjutten (zoals bij traditionele jeugdcriminaliteit), maar (misschien nog wel meer) de behoefte om jezelf *achteraf,* nadat je iets hebt gedaan, te bewijzen en daarvoor erkenning te krijgen. Erkenning krijgen op fora wordt ook in verschillende daderinterviews aangehaald, soms omdat ze deze erkenning in de offline wereld misten. Een dader beschrijft bijvoorbeeld dat er op school wel eens tegen hem werd gezegd dat hij 'geen ruggengraad heeft' en 'er niet komt'. Hij postte zijn hack ook op een forum omdat hij de aandacht die dat genereerde fijn vond.

Dat grenzen vervagen en dat er pro-criminele attitudes worden aangeleerd en bekrachtigd op fora, wordt ook door enkele daders onderkend. Zo stelt een van hen:

> Er zitten duizenden mensen op zo'n forum en die geven allemaal goedkeuringssignalen voor allemaal dingen: iedereen doet het, niemand vindt het erg, je kunt er niet voor gepakt worden, wie heeft er nou echt last van. Na een tijdje dat soort dingen lezen is er sprake van een onbewuste acceptatie. (Daderinterview 14)

Deze dader beschouwt het forum dan ook als een belangrijke factor voor zijn betrokkenheid bij cybercriminaliteit. Het had hem geholpen als het forum er gewoon niet was geweest, net zoals we "niet een drugsdealer op straat willen hebben staan." Een interessant discussiepunt is of pro-criminele

attitudes online nu sneller worden overgedragen dan offline. Hoewel het mechanisme hetzelfde kan werken, zou het wel zo kunnen zijn dat de intensiteit van de blootstelling aan dergelijke attitudes wel groter kan zijn. Zo beschrijft een politie-expert op basis van wat hij tegenkomt op online fora, hoe enorm intensief de interacties daar kunnen zijn.

> Als je ziet in wat voor kringen dader X chat en doet, zitten heel veel mensen in, dan denk je hoe bestaat het dat je zoveel berichten kunt lezen en sturen waar dan een man of 30/40 inzit, je kan niet eens bijhouden hoe snel dat gaat, dan denk je van gast, hebben jullie niks beters te doen? Er zitten mensen bij die een baan hebben, die zitten dan in die groep, ja geen idee, als ik het zou doen zou ik niet aan mijn werk toekomen, zoveel berichten kijken en reageren. (Expertinterview 25, Politie)

Los van virtuele *peers*, waar in de literatuur vooral op wordt gefocust, kunnen ook offline *peers* een belangrijke rol spelen bij de initiatie. Door verschillende experts worden voorbeelden genoemd waarbij vooral jeugdigen door offline *peers* aangemoedigd worden om cybercriminaliteit in enge zin te plegen. Het hacken van of het uitvoeren van DDoS-aanvallen op de eigen school is hier wel het duidelijkste voorbeeld van, wat hen ook bij offline *peers* status en erkenning kan opleveren. Twee van de door ons geïnterviewde daders passen ook in dit beeld. Ook het hebben van 'verkeerde vrienden' wordt een paar keer genoemd door de experts, eveneens in relatie tot jongvolwassen daders. Tot slot beschrijven enkele daders dat hun offline *peers* het delinquente gedrag goedkeurden of in ieder geval niet afkeurden.

6.1.5. Persoonlijke problemen

Zoals reeds in eerdere hoofdstukken aan bod is gekomen, is er in de literatuur aandacht voor verschillende soorten problematiek die een rol spelen bij de initiatie, zowel in het sociale-, gezins- en psychologische domein. Een aspect dat relatief vaak wordt genoemd, is dat een deel van deze daders in een sociaal isolement zit en dat deze factor een relatief grote impact heeft op het delictgedrag. Verschillende experts onderschrijven dat deze daders in de fysieke wereld eenzaam zijn, hun ei niet kwijt kunnen of niet populair op school zijn. In de online wereld zijn ze *wel* in staat om personen te vinden met dezelfde interesses, van wie ze bevestiging kunnen krijgen of die hen het gevoel geven dat ze er bij horen. Ze kunnen dan buitenproportioneel veel tijd online gaan spenderen, waardoor er ook een disbalans in het dag- en nachtritme kan ontstaan. Zoals reeds naar voren kwam, ondersteunen de bevindingen uit de daderinterviews het belang van erkenning zoeken, maar in mindere mate de invloed van een sociaal geïsoleerd bestaan. Dit kan mogelijk deels verklaard worden door de selectie daders die we gesproken hebben. Wel zijn er enkele daders waarbij een (tijdelijk) sociaal isolement of teruggetrokkenheid deel uit maken van een groter complex aan problemen die er toe leidden dat ze zijn gaan hacken.

> Heel vaak ruzie, op school bijvoorbeeld vaak vechten, eenzaam, depressief ook wel, ik wil er niet teveel op ingegaan, maar het was een redelijk negatieve periode. Het forum was een beetje mijn wereldje waar ik me wel thuis voelde. Het was een ontsnapping. (Daderinterview 11)

> Het was een beetje een periode waarin ik klaar was met alles en iedereen. Het was zeg maar een periode dat ik mijn telefoon twee weken had uitgezet en dat ik mijn werk twee weken

volledig genegeerd had, dat ik alles genegeerd had. Toen dacht ik: laat me proberen om te hacken en dat soort dingen. (Daderinterview 7)

Ook zijn er daders die veel nachtelijke uren achter de computer spenderen of spendeerden, waarbij de een dit normaal en fijn vindt en de ander aangeeft dit wel enigszins problematisch te vinden.

6.1.6 Opportunisme/gelegenheid

Zoals eerder naar voren kwam bestaat er een categorie daders die een (gedeeltelijke) switch heeft gemaakt naar cybercriminaliteit en op latere leeftijd een start maakt met een carrière in de cybercriminaliteit. De meest gangbare verklaring voor een dergelijke transitie is opportunisme. Hutchings (2016) betitelt dergelijke daders als *innovators* die hun doelen (geld verdienen) willen bereiken ongeacht de middelen. Het feit dat cybercriminaliteit tal van nieuwe mogelijkheden biedt om relatief gemakkelijk geld te verdienen in combinatie met lage risico's om gepakt te worden, verklaart grotendeels dat ze het cybercriminele pad opgaan. Ook de toegang tot een grote pool potentiële slachtoffers lijkt grotendeels de switch te kunnen verklaren (zie ook Leukfeldt, 2014). Ook de experts zien opportunisme als de belangrijkste verklaring voor de (gedeeltelijke) overstap die sommige traditionele daders maken. Phishing en hacken zijn voor dit type dader voornamelijk een nieuw 'gereedschap' en de digitale wereld is een verlengstuk van hun werkterrein. Cybercriminaliteit kan volgens politie-experts zowel een aanvulling op als uitbreiding van bestaande criminele activiteiten zijn, maar het kan ook de volledige focus worden. De opportunistische daders worden door sommige experts als *streetwise* betiteld om aan te geven dat ze niet zozeer hoogopgeleid zijn, maar wel slim genoeg en innovatief zijn om nieuwe mogelijkheden aan te grijpen en desnoods nieuwe vaardigheden aan te leren.

6.2. Ontwikkeling en rijping

In navolging van de eerder aangehaalde literatuur, beschrijven diverse experts de criminele carrière als een gradueel proces of ontwikkelingspad waarbij er steeds een klein stapje verder wordt gegaan. Een (jonge) dader gaat volgens verschillende experts meestal niet van het ene op het andere moment zware of serieuze delicten plegen, maar stap voor stap. Doordat het een gradueel proces is, wordt men minder snel gehinderd door zijn of haar moreel kompas. Bovendien, zoals reeds in hoofdstuk 5 naar voren is gekomen, kan het niet gepakt worden het gevoel geven ontastbaar te zijn, waardoor men zich maar blijft doorontwikkelen. De meeste daders onderschrijven ook zelf hun betrokkenheid bij cybercriminaliteit als iets dat klein en onschuldig begon (simpelweg kijken 'of het werkt' of 'uitproberen') en zich van daaruit verder ontwikkelde. In deze paragraaf gaan we hier nader op in.

Xu et al. (2013) beschrijven op basis van hun onderzoek een ontwikkelingspad van vier fasen. Deze fasen zijn een bruikbaar uitgangspunt om stil te staan bij de ontwikkelingspaden die we in onderhavig onderzoek zijn tegengekomen. Allereerst is er volgens de auteurs sprake van een periode waarin de affectie voor computers/IT ontstaat ('affectie voor computers'). Vervolgens komt er een ontdekkingsfase *(*'nieuwsgierige exploratie'), waarin er langzamerhand ook een interesse voor hacken wordt ontwikkeld. Daarna volgt een periode van groei waarbij illegale activiteiten worden geëxploreerd en ook een start gemaakt wordt met het plegen hiervan ('illegale excursie') en daarna volgt een periode van rijping ('criminele exploitatie') waarin op grote(re) schaal cybercriminele delicten worden gepleegd.

Ons onderzoek laat zien dat er sprake is van variatie zowel als het gaat om welke fasen door verschillende (groepen) daders worden doorlopen als wat zich binnen dergelijke fasen afspeelt. Zoals

in eerdere paragrafen naar voren is gekomen, begint de criminele carrière wel vaak, maar niet bij iedere dader met een affectie voor computers/IT (op jonge leeftijd). Vooral jeugdige daders die voornamelijk (maar niet alleen) gedreven worden door nieuwsgierigheid (in de werking van IT), leergierigheid en mentale uitdaging doorlopen deze fase. De criminele carrière kan ook beginnen bij de fase van 'nieuwsgierige exploratie'. Dit geldt bijvoorbeeld voor daders wiens interesse voor cybercriminaliteit specifiek tijdens het spelen van games getriggerd wordt. Ook in het rapport van de NCA wordt een dergelijk pad onderscheiden (National Crime Agency, 2017). Hacken en het uitvoeren van DDoS-aanvallen zijn normale praktijken in het spel en men wordt nieuwsgierig over hoe dit werkt en wil dit ook zelf proberen en exploreren, eventueel buiten de setting van het spel. De gemakkelijke toegang tot kant- en klare tools faciliteert dit proces ook. Daders die gelijk in deze fase beginnen lijken over het algemene gedreven te worden door nieuwsgierigheid (meer op het niveau van ontdekken of en hoe de tools werken) en lol/plezier. Motieven zoals spanning, kick en macht lijken zowel een rol te spelen bij daders die de eerste en tweede of alleen de tweede fase doorlopen.

Beide groepen daders komen vervolgens in de fase van de 'illegale excursie' terecht, waarbij er een of meer cyberdelicten worden gepleegd. Hoe jeugdige daders zich in deze fase ontwikkelen lijkt deels afhankelijk te zijn van de mate waarin men in online fora participeert. Actieve deelname op fora zorgt, zoals eerder in dit hoofdstuk besproken, dat daders niet alleen meer vaardigheden ontwikkelen om cyberdelicten te plegen, maar mogelijk ook pro-criminele attitudes aanleren. Vooral indien motieven als erkenning, status en *peer respect* een belangrijke rol spelen voor de dader, kan het forum de criminele carrière aanwakkeren en worden de grenzen steeds verder verlegd. De criminele carrière beperkt zich in sommige gevallen tot deze fase, wat ook bij enkele van onze respondenten het geval was. Men heeft bijvoorbeeld een keer de school gehackt (soms ook door invloed van offline vrienden) en de lol/uitdaging was er daarna ook af (zie ook paragraaf 6.3). Daarbij is het dan ook de vraag of van een 'criminele carrière' gesproken kan worden. Ook zijn er mogelijk daders die dan wel niet in de fase van 'criminele exploitatie' terecht komen, maar wel verder professionaliseren en daarbij grenzen blijven opzoeken tussen het legale (en/of ethische) en het illegale en dus nog met een been in de fase van 'illegale excursie' blijven steken. In het geval van het laatste lijkt het vaak om jeugdige daders te gaan met een sterk eigen moraal en zichzelf als *grey hat* hacker zien. Ook hierbij is het de vraag of je echt van een 'criminele carrière' kunt spreken.

De illegale excursie kan, wat waarschijnlijk geldt voor een kleiner deel van de jeugdige daders, ook verder gaan en uiteindelijk uitmonden in de fase van 'criminele exploitatie', waarbij het plegen van cyberdelicten grote(re) of ernstige vormen aanneemt. De transitie hier naartoe lijkt gepaard te gaan met diverse factoren die eerder al besproken zijn, namelijk de mate waarin vaardigheden worden ontwikkeld, de mate waarin men een positie/status verwerft op een forum en, wellicht nog belangrijker, het motief of de combinatie van motieven. Voornamelijk indien er sprake is van een transitie naar een financieel motief, waarbij de dader 'ontdekt' dat hij veel geld kan verdienen met cybercriminaliteit en/of eventueel gewend raakt aan een bepaald bestedingspatroon, is de kans reëel dat de dader in de fase van 'criminele exploitatie' terecht komt en daar enige tijd in blijft hangen.

In het kader van hoe daders, die in deze fase terecht komen, zich specifiek ontwikkelen en doorgroeien, lijkt afgegaan op de expert- en daderinterviews, wederom variatie te bestaan. Uit onze bevindingen blijkt dat er ten eerste sprake kan zijn van een toename van de frequentie/schaal in het plegen van delicten. Een dader gaat bijvoorbeeld steeds vaker of op grotere schaal hetzelfde delict plegen. Hierbij moet wel rekening gehouden worden met de aard van de delicten: bij het uitvoeren van een DDoS-aanval bijvoorbeeld, kan een dader binnen beperkte tijd wel 100 aanvallen lanceren. Frequentie heeft daarmee een andere betekenis dan bij traditionele criminaliteit. Schaalvergroting is

ook op andere manieren terug te zien. Eén van de daders geeft bijvoorbeeld aan dat hij bezig was om een grote databank op te bouwen met inloggegevens van derden. Het betrof een combinatie van databases die je online kunt downloaden en databases die hij zelf had gehackt, zodat hij privégegevens had waar anderen niet over beschikten. Mocht hij dan iemand willen hacken, dan was de kans groot dat ergens in die database het wachtwoord wel te vinden was (ook met het oog op dat mensen vaak hetzelfde wachtwoord gebruiken). Het opbouwen van een eigen databank beschouwde hij als een soort investering om zoveel mogelijk gegevens te verzamelen, die hij vervolgens kon gebruiken/misbruiken. “Het was eigenlijk gewoon steeds meer een soort piramide of zo, steeds meer opbouwen en hoe meer je hebt, in hoe meer dingen je kunt komen” (Daderinterview 8).

In het kader van de schaal waarop delicten worden gepleegd lijkt er sprake te zijn van een onderscheid tussen daders die gericht zijn op kwaliteit (bijvoorbeeld specifieke doelen hacken, specifieke buiten binnenhalen, steeds andere doelen willen hacken om uitgedaagd te kunnen worden) en daders die gericht zijn op kwantiteit (bijvoorbeeld zoveel mogelijk databases hacken). Dit laatste zou mogelijk te maken kunnen hebben met de in hoofdstuk 4 besproken verzameldrang naar informatie. Motieven als de kick en uitdaging lijken, op basis van onze daderinterviews zowel bij op kwaliteit als kwantiteit gerichte daders een rol te spelen.

Een tweede ontwikkeling die we hebben aangetroffen is dat de dader andersoortige cyberdelicten gaat plegen, iets waar in de literatuur nog niet veel over bekend is. Volgens Khey, Jennings, Lanza-Kaduce en Frazier (2009) spitsen cyberdaders zich vaak toe op een soort delict en beperken zij zich tot het soort delict waar ze het meest bekend mee zijn. Het is volgens experts lastig om bij cyberdaders te spreken van specialisten, dat wil zeggen daders die zich beperken tot één delict, werkwijze, locatie of soort doelwit. Veel experts beschrijven namelijk dat de daders een technische ontwikkeling doormaken waarbij ze verschillende dingen ondernemen. Dit kan gepaard gaan met verschillende cyberdelicten, die ieder hun eigen werkwijze hebben en ook andere vaardigheden en kennis vereisen. De mate van specialisatie varieert bij de geïnterviewde daders. Sommige daders beperkten zich tot een soort delict en een ander deel van de daders pleegde over tijd meerdere soorten cyberdelicten. Dit laatste lijkt vooral aan de orde te zijn bij de daders wiens criminele carrière langer voortduurde. Men wilde bijvoorbeeld nieuwe dingen leren of uitproberen. Een van de daders die we hebben gesproken lijkt met alle soorten cybercriminaliteit ervaring te hebben, zoals met hacken, het uitvoeren van DDoS-aanvallen, *defacing*, het opzetten van botnets en fraude. Ook hangt een verandering in het soort delict samen met veranderingen in drijfveren, bijvoorbeeld van roem naar financieel.

Voor de late starters, daders die de transitie van traditionele delicten naar cybercriminaliteit hebben gemaakt, geldt in de meeste gevallen een andersoortig ontwikkelpad. Terugkomend op de hierboven gesproken 4 fasen van een cybercriminele carrière, lijken deze daders (mogelijk na een korte verkenning) vrijwel direct in de fase van criminele exploitatie terecht. De interesse is niet zozeer voortgekomen uit het willen verkennen en exploreren van de techniek, maar wordt vooral bepaald door de nieuwe kansen die deze vorm van criminaliteit biedt als het gaat om het verdienen van geld.

6.3. *Desistance*: Stoppen of doorgaan?

Aan het stoppen (alsook aan het doorgaan) kunnen verschillende redenen ten grondslag liggen. Deze kunnen enerzijds te maken hebben met de keuzes die cyberdaders zelf maken en/of beïnvloed worden door omstandigheden die er voor zorgen dat ze stoppen (of doorgaan). Hieronder wordt stilgestaan bij de factoren die uit de literatuur, expert- en daderinterviews naar voren zijn gekomen.

6.3.1. Volwassenwording

Volgens de typologische verklaring van Moffitt (1993) bestaat er een grote groep daders die, conform het patroon van de AL-dader ook weer stopt met het plegen van criminaliteit alsook een kleinere meer persistente groep (LCP-dader) die in de volwassenheid doorgaat en waarbij dus sprake is van een zekere rijping (Xu et al., 2013). De verklaring waarom de eerste groep stopt wordt gezocht in het feit dat de eerder besproken *maturity gap* kleiner wordt. Men realiseert zich dat het niet-plegen van delicten meer kansen biedt op begerenswaardige zaken (bijvoorbeeld werk) en zodoende stopt men met het delinquente gedrag.

Ook door verschillende experts wordt het plegen van cybercriminaliteit beschreven als een fase waar de meeste daders weer uitgroeien naarmate zij ouder worden en een beter moreel besef ontwikkelen. Ook gaan ze er vanuit dat veel jeugdigen naar mate ze ouder worden alsnog een moreel kompas ontwikkelen die meer correspondeert met de juridische grens. Dit gaat gepaard met het ontgroeien van de pubertijd, minder impulsiviteit en een beter inlevingsvermogen in anderen.

Enkele daders lijken dit standpunt te ondersteunen en denken dat volwassenwording meer invloed heeft gehad op het feit dat ze stopten dan de aanhouding en de bestraffing. Zo stelt een respondent: “Wat ik zelf denk is gewoon dat ik gewoon meer volwassen ben geworden qua leeftijd. Ik bedoel het is maar een jaartje, maar in dat jaartje vind ik zelf dat er wel veel veranderd is qua gedrag zeg maar” (Daderinterview 6).

Een andere dader geeft aan dat het illegaal hacken maar kort heeft geduurd en dat hij zichzelf daar in heeft geremd vanwege een groeiend verantwoordelijkheidsgevoel:

> Ik denk dat het in een periode van drie, vier, vijf weken was. Het is niet iets waar ik heel druk mee ben geweest, dat was pure initiële interesse, wat ik zei, ik ben daar wel in geremd. Met geremd bedoel ik niet de politie, ik bedoel dat ik mezelf daarin heb geremd, dat ik zelf ook wel door had van he. Je hebt een soort van… kijk, je kunt bijna zeggen je hebt een soort van power toch, daar komt ook *responsibility* mee. Die nam ik op dat moment niet en die nam ik daarna wel. (Daderinterview 12)

6.3.2. Veranderingen in kosten-batenafweging

Volgens Hutchings (2016) maken daders niet alleen een kosten-batenafweging als het gaat om het plegen van criminaliteit, maar ook als het gaat om het stoppen. Zo wijst ze op het feit dat cyberdaders vaak in de veronderstelling zijn dat ze toch niet gepakt worden en om deze reden dus doorgaan. Zoals in hoofdstuk 5 naar voren is gekomen, is hierbij ook sprake van een tijdsdimensie. Hoe langer en vaker men delicten pleegt en daarmee wegkomt, hoe lager de risicoperceptie wordt en dus hoe lager de kosten worden ingeschat. Mogelijk speelt deze factor ook een rol bij het feit dat een deel van de daders stapsgewijs in de fase van ‘criminele exploitatie’ terecht komt. Naast de toename van eventuele kosten spelen ook de afname van bepaalde baten een rol bij het wel of niet stoppen. Als de dader niet langer bepaalde voordelen ervaart of er geen voldoening meer uithaalt (bijvoorbeeld plezier en prestaties), zal hij of zij sneller stoppen. Het wegvallen van baten komt ook in de daderinterviews naar voren. Daarbij benoemen de daders allereerst dat de lol of spanning er op een gegeven moment van afgaat en dat het plegen van cyberdelicten niet meer interessant is.

> Op een gegeven moment is ook de nieuwsgierigheid, of de spanning, eraf. Zo van ja, goed we hebben het bereikt en ik wilde het toch niet misbruiken, ja wat moet ik er verder mee. Gewoon er niks meer mee doen, en dan door met je leven zeg maar. (Daderinterview 10)

De factor spanning of adrenalinekick lijkt dan zowel een factor te zijn die het delictgedrag kan aanwakkeren als (uiteindelijk weer) kan afremmen. Dezelfde uitdaging waar het ooit mee begon is er niet meer en men gaat op zoek naar andere (legale) uitdagingen en/of krijgt andere prioriteiten. Dit brengt ons automatisch bij het punt dat er ook andersoortige kosten en baten meespelen op het gebied van werk en gezin.

6.3.3. Werk en wederhelft

In de literatuur over *desistance* wordt het belang van zogenaamde *turning points* benadrukt. Daarbij gaat het om het belang van *life events* zoals een nieuwe baan vinden, trouwen en kinderen krijgen (Sampson & Laub, 2005). Dergelijke keerpunten kunnen een identiteitsverandering in gang zetten die van belang is om niet terug te vallen in de criminaliteit. In dit kader wordt ook wel van secundaire *desistance* gesproken (o.a. Maruna & Farrall, 2004; Maruna & Toch, 2005). Primaire *desistance* verwijst alleen naar het stoppen van het plegen van delicten. Er is weinig literatuur waarbij de rol van *turning points* bij cyberdaders is onderzocht. Weulen Kranenbarg et al. (2018) hebben (zoals ook in hoofdstuk 3 besproken) in een kwantitatief onderzoek naar cybercriminaliteit in enge zin gevonden dat werk en opleiding, anders dan bij de meeste traditionele daders, *niet* als protectieve factoren gelden voor cybercriminaliteit. Het hebben van een baan in de IT-sector kan zelfs de kans op het plegen van cybercriminaliteit verhogen (hoewel dit verband niet significant is). Een niet-IT gerelateerde baan kan de kans op het plegen van cybercriminaliteit daarentegen wel verlagen.

Het belang van *turning points* is ook aan de orde gekomen tijdens verschillende expertinterviews. Zo wordt het vinden van een legale baan beschouwd als een factor die *desistance* kan bevorderen. Eén van de reclasseringsmedewerkers beschrijft het als een intrinsieke motivatie. Een van de daders stopte bijvoorbeeld omdat hij een baan kreeg en zelf ook niet zou willen dat zijn geld van zijn rekening zou worden gehaald door een crimineel, omdat hij er hard voor heeft gewerkt.

Sommige geïnterviewde daders, voornamelijk de hackers, benadrukken ook het belang van een baan vinden om op het rechte pad te blijven en geven aan een carrière in de IT-sector te ambiëren, maar zeggen hierin wel bemoeilijkt te worden door hun strafblad (zie verder 6.3.5). Sommige daders geven aan legitieme manieren te hebben gevonden om heel veel geld te verdienen op het internet en geven aan dat dat toen de nieuwe focus werd. *Responsible disclosure* en het verdienen van *bug bounties* (een beloning die je krijgt als je een lek meldt) zien verscheidene respondenten als een mooi alternatief. Ze signaleren echter wel dat dit gepaard gaat met onzekerheid over zowel de beloning als wat er met de melding gaat gebeuren. Ook komen *turning points* gerelateerd aan gezinsvorming aan de orde. Een van de daders geeft aan dat hij vanwege zijn vriendin en kind graag op het rechte pad wil blijven.

6.3.4. Factoren die *desistance* bemoeilijken

Vanuit de *desistance* benadering is *desistance* vele malen complexer dan een simpele kosten-batenafweging. Volgens deze benadering gaat het om een complex proces wat gepaard kan gaan met vallen en opstaan (*trial and error*) (Sampson & Laub, 2005). Het is, op basis van de literatuur nog onbekend in hoeverre dit ook voor cyberdaders geldt. Zoals uit de vorige paragraaf naar voren is gekomen, wordt vaak verondersteld dat zij gunstige toekomstperspectieven hebben, wat zou kunnen betekenen dat er nieuwe kansen op de loer liggen en men mogelijk minder snel terug gaat vallen in de illegaliteit. Op basis van de daderinterviews zien we weinig aanwijzingen voor een echte ‘struggle’.

Er wordt gesproken van een langzame transitie waarbij men gestaag stopt, bijvoorbeeld door andere prioriteiten en interesses en veranderingen in het moreel kompas. Wel komen er, zowel in de expert- als daderinterviews aspecten aan de orde die het proces van *desistance* bemoeilijken.

Allereerst komt naar voren sommige daders in de wereld van cybercriminaliteit worden 'opgezogen' en dat het dan zelfdiscipline vergt om er weer uit te komen. Deze worsteling wordt door verschillende experts aangehaald. Zo beschrijft een politie-expert:

> Op het moment dat je daar verder in terecht komt vergt het steeds meer zelfdiscipline om er weer uit te stappen. Het werkt wel als een soort verslaving op het moment dat je je contacten hebt, je dingetjes lukken, je verdient een keertje wat geld, je krijgt wat meer status hier en daar en je wordt belangrijker, dan wordt het wel steeds lastiger om er uit te komen. (Expertinterview 29, Politie)

Een van de geïnterviewde daders geeft om deze reden aan nooit meer fora te bezoeken, zodat hij er niet meer aan blootgesteld wordt. Na zijn zaak is hij naar eigen zeggen nooit meer op 'grijze' of 'zwarte' fora geweest, ook al is hij wel benieuwd of die fora opgerold zijn of dat het verder gaat. Hij heeft zijn connecties via Skype verwijderd (veel contact ging via Skype). Hij voelt niet echt een drang, maar hij ziet het ook niet meer. Als je het niet ziet kun je er ook niet in terecht komen, aldus de dader. Tegelijkertijd denkt hij niet dat hij erin mee zou gaan als hij het weer zou tegenkomen.

Een andere belangrijke factor die genoemd wordt in het kader van *desistance*, is het hebben van een strafblad en de consequenties daarvan. Net als bij traditionele daders kan dit belemmerend werken in het kader van het stoppen met criminaliteit. De kansen op de arbeidsmarkt kunnen bijvoorbeeld (flink) ingeperkt worden indien daders geen Verklaring Omtrent het Gedrag (VOG) kunnen krijgen (Van 't Zand, 2017). Er zijn vrijwel geen studies te vinden die dit aspect bij cyberdaders hebben onderzocht. Wel wordt er door sommige auteurs vanuit gegaan dat hackers minder problemen ondervinden om een baan te vinden omdat ze essentiële vaardigheden hebben (o.a. Turgeman-Goldschmidt, 2008), zoals ook is aangehaald door de experts.

De experts veronderstellen dat daders met veel IT-talent een betere uitgangspositie op de arbeidsmarkt hebben, omdat zij vaardigheden hebben waar in de maatschappij veel behoefte aan is. Tegelijkertijd wordt er ook van uitgegaan dat een strafblad beperkingen kan opleggen. Volgens verschillende experts zal een aantal banen niet meer toegankelijk zijn met een strafblad, maar andere banen nog wel. Dit hangt er onder andere van af of het delict is gepleegd uit jeugdige nieuwsgierigheid en of een leidinggevende daar begrip voor heeft. Ook banen die een vertrouwensfunctie betreffen kunnen vanwege het strafblad lastig toegankelijk worden, omdat daar een screening voor nodig is.

Ook enkele daders die een strafblad hebben, geven aan problemen te hebben ondervonden bij het vinden van werk door hun strafblad. Zo vertelt een respondent:

> Een bedrijf wil niet met iemand in zee die een crimineel verleden heeft. En ja weet je, zie dan maar eens uit te leggen aan hun dat je geen crimineel bent als je wel een strafblad hebt. Al word je veroordeeld voor het stelen van een lolly dan heb je wel een strafblad. En iemand met een strafblad wordt gezien als een crimineel... Zo heb ik mijzelf niet gezien, dat drong pas door toen ik de ene afwijzing na de andere ging krijgen. Dus ik ging zoeken naar een manier om mijn integriteit terug te winnen. Van hoe kan ik nou, hoe kan ik nou aantonen dat ik wel degelijk te vertrouwen ben. (Daderinterview 9)

Met andere woorden, ook al hebben cyberdaders mogelijk meer kansen op de arbeidsmarkt, ze kunnen nog steeds hinder ondervinden van hun strafblad, wat het proces van *desistance* kan vertragen of bemoeilijken.

6.4. Conclusie

In dit hoofdstuk is stilgestaan bij verschillende facetten van de criminele carrière van cyberdaders. In dit kader zijn niet zozeer wederzijds uitsluitende ontwikkelingstrajecten uiteengezet, maar inzichten geleverd over criminogene factoren die van invloed zijn op het verloop van de criminele carrière van daders. Deze inzichten kunnen in combinatie met de inzichten uit voorgaande hoofstukken aanknopingspunten bieden voor passende interventies: wanneer en bij wie deze het beste kunnen worden ingezet. In het hoofdstuk is zowel ingegaan op het ontstaan (de initiatie), de ontwikkeling van de criminele carrière als op de vraag wat daders (los van de interventie) doet stoppen.

Als het gaat om de initiatie zijn factoren aan bod gekomen die zowel een rol spelen bij traditionele- als bij cybercriminaliteit. Zo zijn aspecten als de *maturity gap*, de invloed van delinquente *peers* en bepaalde drijfveren (bijvoorbeeld geld) bij beide soorten daders van belang. Wel zien we hierbij ook verschillen die te maken hebben met de online omgeving waarin deze daders (vaak vele uren per etmaal) spenderen. Zo suggereren de bevindingen dat blootstelling aan pro-criminele definities kan worden aangewakkerd door de vele tijd die op fora wordt gespendeerd alsook door het belang van prestatie, erkenning en status op dergelijke fora. Daarnaast zijn er criminogene factoren naar voren gekomen die specifiek een rol spelen bij cyberdaders zoals interesse voor/affiniteit met ICT, gamen en/of gemakkelijke toegang tot tools. In het kader van de ontwikkeling van de criminele carrière is uitgegaan van vier fasen die daders deels of allemaal doorlopen (‘affectie voor computers’, ‘nieuwsgierige exploratie’, illegale excursie’ en ‘criminele exploitatie’). Uit het hoofdstuk blijkt dat er veel variatie is met betrekking tot welke fase(n) worden doorlopen. Dit kan variëren van daders die alle fasen doorlopen tot daders die niet verder komen dan nieuwsgierige exploratie waarbij het ook te betwijfelen of er echt sprake is van een ‘criminele carrière’. Ook is er een categorie (doorgaans volwassen) daders die vrijwel gelijk in de fase van ‘criminele exploitatie’ terecht komt, waarbij het meestal gaat om opportunistische daders die de overstap naar cybercriminaliteit hebben gemaakt.

Ook bij daders die dezelfde fasen doorlopen bestaat variatie als het gaat om hoe de ontwikkeling van het delictgedrag er uit ziet en welke factoren daarop van invloed zijn. Deze variaties hangen grotendeels samen met factoren die een rol spelen bij de initiatie alsook met de motieven en vaardigheden/mate van professionalisering. Tegelijkertijd spelen andere processen mee als het gaat om wat het verloop van de criminele carrière bepaalt, waaronder veranderingen in morele percepties (ofwel richting pro-crimineel ofwel richting pro-sociaal), veranderingen in motieven (bijvoorbeeld van erkenning naar financieel) en ook speelt verandering in de risicoperceptie een rol. Zoals ook reeds in hoofdstuk 5 naar voren is gekomen, worden daders door de lage pakkans niet afgeremd en wanen ze zich ontastbaar.

Als het gaat om *desistance* zien we dat diverse factoren een rol spelen. Ook hier kan het gaan om factoren die bij traditionele daders van invloed zijn zoals volwassenwording en de rol van werk en wederhelft. Verondersteld wordt hierbij wel dat daders juist meer kansen hebben op een goede baan, hetgeen niet altijd bevestigd wordt door de respondenten. In het geval van dit laatste gaat het dan om de beperkingen die een strafblad opleveren. Ook laten de bevindingen zien dat er door de tijd heen, wat ook weer samenhangt met leeftijd en sociale bindingen, andere kosten en baten een rol kunnen gaan spelen. Daarbij zien we ook terug dat de motieven die aanvankelijk ervoor zorgden dat de daders deze delicten gingen plegen (bijvoorbeeld kick/spanning) er ook weer voor zorgen dat ze er

mee stoppen. In het kader van stoppen wordt ook gewezen op factoren die *desistance* bemoeilijken. Los van het strafblad wordt in dit kader gewezen op het feit dat men helemaal is opgegaan in de wereld, zowel in termen van status als (het snelle) geld, waardoor er nog te veel baten zijn om door te gaan.

DEEL 2: Interventies voor daders van cybercriminaliteit in enge zin

In paragraaf 1.6 is kort beschreven hoe vanuit de het rationele keuzeperspectief, de *What Works* literatuur en in de *desistance* literatuur aangekeken wordt tegen de mogelijkheden om met interventies de kans op (recidive van) criminele delicten en meer in het algemeen de ontwikkeling van de criminele carrières van daders van traditionele criminaliteit te beïnvloeden. In deze literatuur worden regelmatig, vooral bij de laatste twee benaderingen, specifieke doelgroepen zoals zedendelinquenten, geweldplegers of plegers van drugsgerelateerde criminaliteit en hun criminogene factoren onderscheiden. We hebben betrekkelijk weinig studies gevonden waarin het *What Works* model of de *desistance* benadering specifiek toegepast worden op daders van cybercriminaliteit in enge zin. Wel zijn de benaderingen impliciet of expliciet uit de interviews naar voren gekomen. Zoals zichtbaar wordt in hoofdstuk 7, zijn er relatief veel studies waarin de theorie van afschrikking wordt toegepast op daders van cybercriminaliteit.

Ook heeft de zoektocht naar literatuur, zoals beschreven in paragraaf 2.1.2, opvallend weinig (effect)onderzoek naar interventies voor daders van cybercriminaliteit in enge zin opgeleverd. Het meeste onderzoek was ofwel *beschrijvend* van aard, bijvoorbeeld ten aanzien van het type en de hoogte van opgelegde straffen, ofwel *theoretisch* van aard, op basis waarvan het *verwachte* effect van interventies wordt beschreven. Daarnaast heeft de zoektocht zeer weinig Nederlands onderzoek opgeleverd en vooral onderzoek uit de Verenigde Staten. Derhalve beschouwen wij de expert- en daderinterviews van belangrijke waarde voor het bepalen van wat werkzame mechanismen zouden kunnen zijn van interventies zoals wij deze kennen in Nederland.

In hoofdstuk 7 wordt stilgestaan bij interventies die direct ingrijpen op de perceptie van de kosten-batenverhouding van het plegen van cybercriminaliteit (rationele keuzebenadering), waaronder interventies gericht op generale of speciale afschrikking en situationele criminaliteitspreventie. In hoofdstuk 8 wordt gefocust op zowel *risk-based* interventies (interventiedoel: het targeten van criminogene behoeften) als *strength-based* interventies (interventiedoel: versterken van protectieve factoren en ondersteuning bieden aan het *desistance* proces). Zoals in paragraaf 1.6 is aangegeven, kan een interventie elementen bevatten van verschillende benaderingen.

Hoofdstuk 7 Interventies die aansluiten bij afschrikking en situationele criminaliteitspreventie

In dit hoofdstuk staan interventies voor cyberdaders centraal die aansluiten bij de theorieën van afschrikking en situationele criminaliteitspreventie. Dit betekent dat de interventies in beginsel uitgaan van een calculerende dader en gericht zijn op het beïnvloeden van de balans van kosten en baten, waarop de keuze voor crimineel gedrag wordt gebaseerd. De reden om hier in dit hoofdstuk bij stil te staan, is dat zowel in de literatuur als in de interviews, vooral door experts, veel gesproken wordt over de vraag welke straffen voldoende zouden afschrikken en rationeel calculerende cyberdaders ervan zouden kunnen weerhouden (nogmaals) tot crimineel gedrag over te gaan. In dit hoofdstuk zullen wij allereerst ingaan op theorieën gerelateerd aan de rationele keuze, waaronder het klassieke afschrikkingsperspectief en het perspectief van situationele criminaliteitspreventie (paragraaf 7.1). Vervolgens worden de bevindingen uit de literatuur en praktijk over interventies gericht op het beïnvloeden van de rationele keuze besproken. In paragraaf 7.2 wordt eerst een algemeen overzicht gegeven over hoe er vanuit de praktijk wordt aangekeken tegen de voorwaarden *zeker, streng en snel*, waaraan interventies gericht op afschrikking volgens de klassieke theorie dienen te voldoen. Daarna worden steeds verschillende typen interventies besproken. Allereerst de reactieve interventies gevangenisstraf en financiële consequenties (paragraaf 7.3). Vervolgens preventieve interventies waarmee de rationele keuze kan worden beïnvloed, waaronder *knock and talk*, voorlichting op scholen, *online policing* en verstoring (paragraaf 7.4). In paragraaf 7.5 wordt een conclusie gegeven.

7.1. Straffen volgens de klassieke theorie

De klassieke theorie gaat uit van de rationele, calculerende mens en stelt daarom dat interventies effectief zijn indien er sprake is van voldoende afschrikking (Bentham, 1789). Er kunnen twee vormen van afschrikking worden onderscheiden, namelijk generale en speciale afschrikking. Generale afschrikking verwijst naar het afschrikkende effect van een straf in algemene zin. Zowel gestraften als niet-gestraften worden dan door de dreiging van straf weerhouden om criminaliteit te plegen. Bij speciale afschrikking gaat het om afschrikking van een gestrafte. Een persoon wordt dan door de aan hem of haar opgelegde straf ervan weerhouden om te recidiveren. De theorie van afschrikking gaat uit van de volgende causale aanname: hoe groter de zekerheid (*certainty*), zwaarte (*severity*) en snelheid (*swiftness*) van de straf, hoe lager de criminaliteit (Gibbs, 1975; Kleck, Sever, Li & Gertz, 2005). Om voldoende afschrikwekkend te zijn, moeten interventies dus *zeker* en *snel* volgen op crimineel gedrag en voldoende *streng* zijn; aspecten waar in dit hoofdstuk op ingegaan wordt.

De theorie van afschrikking is onder andere gebaseerd op het rationele keuze-perspectief (Cornish & Clarke, 1986), die er vanuit gaat dat daders een rationele kosten-batenanalyse maken en zij, wanneer de verwachte opbrengsten hoger zijn dan de verwachte kosten, tot het plegen van criminaliteit zullen overgaan. De theorie gaat er daarbij vanuit dat deze analyse van de dader wel enigszins subjectief is omdat deze beperkt wordt door tijd, cognitieve vaardigheden en beschikbare informatie. Conform deze theorie moeten kosten worden verhoogd door enerzijds de strafdreiging te verhogen, dat wil zeggen de sanctie waarmee volgens de wettekst een strafbare gedraging wordt bedreigd, en anderzijds het risico om opgepakt te worden (de pakkans) te vergroten. Deze twee elementen hoeven niet per se even zwaar te wegen (Clarke, 1997, in Hutchings, 2016). Ook zijn er gerelateerde theorieën die meer nadruk leggen op het verminderen van de gelegenheid en het

beïnvloeden van de daarmee verbonden (rationele) keuze van de dader. Clarke en Felson (1993) hebben bijvoorbeeld een specifiek model van situationele criminaliteitspreventie ontwikkeld, waarbij zij een vijftal hoofdstrategieën onderscheiden, namelijk: 1) het risico verhogen, 2) de moeite verhogen, 3) de opbrengsten verlagen, 4) het verminderen van provocaties, en 5) het reduceren van mogelijkheden voor excuses. Omgevingsgerichte interventies zouden mogelijk niet alleen voor de fysieke maar ook voor de digitale omgeving kunnen werken (Leukfeldt & Yar, 2016). Hierop wordt in paragraaf 7.4.4 verder ingegaan.

Om daadwerkelijk afschrikking te genereren, moeten potentiële daders dus in de veronderstelling zijn c.q. de perceptie hebben dat ze gestraft of gepakt kunnen en zullen worden. Hierin schuilt volgens Kleck et al. (2005) ook een probleem. Dit wordt in de hierna volgende paragrafen verder uitgewerkt.

7.2. Het belang van zeker, snel en streng nader bekeken

7.2.1 Zeker

Zoals uit hoofdstuk 5 blijkt, wordt de pakkans door cyberdaders over het algemeen als erg klein ingeschat, kleiner dan bij traditionele criminaliteit. Dit is vanuit de theorie van afschrikking problematisch omdat het vooral de *kans* om gepakt te worden is die afschrikwekkend werkt en niet zozeer de strafhoogte, ook wel *perceptuele afschrikking* genoemd (Moerland, 1991). Bij de zekerheid over of er straf volgt op cybercriminaliteit gaat het, zo blijkt uit de literatuur, bovendien niet zozeer om hoe hoog de pakkans daadwerkelijk is (de reële pakkans), maar hoe hoog potentiële daders *denken* dat deze is (de gepercipieerde pakkans) (Turgeman-Goldschmidt, 2005; Hutchings & Holt, 2017). Door de lage pakkans zou volgens experts de hoogte van de mogelijk op te leggen straf door cyberdaders 'op de koop toe' worden genomen.

Uit de literatuur komt verder naar voren dat *publiciteit* een van de voorwaarden is om afschrikkingsstrategieën van de overheid succesvol te laten zijn (Goldman & McCoy, 2016). Daarom zou een zekere mate van publiciteit over de cyberacties en capaciteiten van de politie noodzakelijk zijn. Het gaat bij afschrikking namelijk niet om de capaciteiten van de overheid om bijvoorbeeld op te sporen of te verstoren, maar om het *geloof* van anderen dat de overheid zulke capaciteiten bezit. Daarnaast wordt in de literatuur gesteld dat het nodig is dat de boodschap van afschrikking naar de juiste personen wordt gecommuniceerd (attributie). Immers, als men niet zeker weet wie de beoogde ontvangers van de afschrikkingsboodschap dienen te zijn, kan onvoldoende maatwerk worden geleverd (Goldman & McCoy, 2016).

Volgens enkele experts moeten zowel de daadwerkelijke capaciteiten van de overheid als het geloof van anderen in deze capaciteiten omhoog. Een van de geïnterviewde cybersecurityexperts verwacht bijvoorbeeld dat als de politie laat zien welke hackbevoegdheid ze hebben en wat ze op dat gebied daadwerkelijk voor elkaar krijgen, dit afschrikwekkend zou kunnen werken, omdat het de perceptie van de pakkans vergroot. Mede bezien vanuit de lage (gepercipieerde) pakkans, spreken experts erover dat het opgepakt worden op zichzelf een ingrijpende ervaring kan vormen die duidelijk impact heeft. Dit geldt vooral voor experts die persoonlijk betrokken zijn bij jonge cyberdaders. De meeste jeugdigen hebben absoluut niet stilgestaan bij het idee dat ze opgepakt zouden kunnen worden en schrikken enorm. De impact is niet alleen gelegen in het moeten verschijnen op het politiebureau of een nacht in de cel moeten doorbrengen, maar in dat de daders hierdoor de gevolgen van hun gedrag zijn gaan inzien; niet alleen voor zichzelf, maar ook voor het slachtoffer of de familie van de dader. In aansluiting hierop beschouwen meerdere experts het effect van de aanhouding wel

degelijk als substantieel, omdat het een *hook for change* zou vormen op basis waarvan wordt besloten te stoppen met criminaliteit (Giordano, Cernkovich & Rudolph, 2002). Hierin zien experts een duidelijk verschil met traditionele daders, omdat recidive na de eerste aanhouding bij cyberdaders lager lijkt te liggen. Zo stelt een advocaat:

> Ik denk wel dat als die jongens gepakt worden eenmaal, dat de kans op recidive heel klein is... Dat ze daadwerkelijk geen criminele dingen meer doen. Ik denk dat maakt op deze jongens, zeker op zo'n jonge leeftijd, zoveel indruk. Gewoon aangehouden worden, vastgezet worden, dat doet ze echt pijn, het doet de familie pijn. Ik kom heel weinig recidive tegen bij mijn cliënten. (Expertinterview 1, Advocaat)

Het gegeven dat cyberdaders minder vaak recidiveren wordt ook naar voren gebracht door politie-experts die al tientallen zaken hebben behandeld. Een groot deel van de daders – voornamelijk jeugdige niet-financieel gerichte daders - zien ze niet in de opsporingsonderzoeken terugkomen. Daders (meestal volwassenen) die betrokken zijn bij fraude-gerelateerde vormen van cybercriminaliteit ziet men vaak wel terugkomen. Verschillende (ook andere) experts verwijzen hierbij naar phishers: die accepteren volgens hem eenvoudigweg dat ze een paar jaar moeten gaan zitten en leren in de gevangenis vervolgens nieuwe manieren om criminaliteit te plegen die ze direct gaan uitproberen zodra ze vrijkomen.

Een deel van de geïnterviewde daders zegt door de arrestatie of als gevolg van de strafzaak te zijn gestopt, hoewel ook een deel expliciet benoemt, zoals in hoofdstuk 5 is toegelicht, dat ze op eigen initiatief zijn gestopt en niet vanwege de aanhouding. Voor sommigen kwam de aanhouding inderdaad onverwacht, bijvoorbeeld omdat ze dachten er (wederom) mee weg te kunnen komen. Een andere respondent verwachtte de aanhouding juist wel: hij zei verbaasd te zijn dat de politie niet al veel eerder voor de deur stond. Verwacht of onverwacht, de aanhouding wordt over het algemeen als een zeer onprettige ervaring beschreven voor henzelf en voor hun familie. Verschillende respondenten uiten tijdens het interview onvrede over het proces van vervolging en de bejegening door politieagenten.

Op sommige jeugdige daders maakt het voldoende indruk dat zij door allerlei andere partijen op het matje worden geroepen om vervolgens te stoppen met crimineel gedrag, bijvoorbeeld wanneer een aanhouding mede leidt tot boze reacties van ouders en van de school. Een respondent die niet is aangehouden door de politie, maar wel op school op het matje is geroepen, vertelt dat de *dreiging* met politie al voldoende voor hem was om te stoppen:

> Het maakte ook best wel indruk als ze gaan dreigen met de politie en de directeur komt erbij en dit en dat, als je 13 bent. Dus ik had toen wel zoiets van nou ik vind het wel mooi geweest. (Daderinterview 10)

Op basis van expert- en daderinterviews kan dus voorzichtig worden gesteld dat van aanhouding alleen al een mogelijk afschrikwekkend effect uitgaat voor jeugdige daders, die niet eerder zijn opgepakt en voor wie criminaliteit niet hun bron van inkomsten vormt. Dit geldt zodoende niet voor degenen die voor financieel gewin cybercriminaliteit plegen. Ten slotte moet worden opgemerkt dat het veronderstelde afschrikwekkende effect dat enkel van de aanhouding zou uitgaan, tot op heden niet wetenschappelijk is onderzocht. Daarnaast geldt dat de meeste experts beperkte ervaring met cyberdaders hebben (zowel in aantallen als in looptijd), wat kan betekenen dat het effect (stoppen of

doorgaan met criminaliteit) simpelweg nog onvoldoende zichtbaar is. Ten slotte kan het zo zijn dat de geïnterviewde daders geen representatief beeld geven van de gehele populatie, maar relatief vaker zijn gestopt met criminaliteit.

7.2.2 Snel

"*Bam, je doet iets fout en klats*." (Expertinterview 25, Politie)

Met bovenstaande uitspraak drukt een politieagent het belang uit van een snelle reactie op regelovertredend gedrag. De noodzaak van snel straffen, geldt volgens hem specifiek bij *jonge* cyberdaders, omdat hun langetermijndenken evenals het kunnen reflecteren op gedrag uit het verleden nog onderontwikkeld is. Een reclasseringswerker die enkel (jong)volwassen daders heeft begeleid zegt dat de impact van het aangehouden worden na verloop van tijd wegebt. Het is daarom volgens hem erg belangrijk om cyberdaders in de tussenliggende periode (tussen de aanhouding en het opleggen van de straf) reeds aan hun verandering te laten werken. Daar kunnen schorsende voorwaarden waarbij verdachten verplicht moeten meewerken aan reclasseringstoezicht aan bijdragen.

Van een snelle reactie lijkt echter in de meeste gevallen geen sprake, daar het volgens de geïnterviewde experts en daders vaak lang duurt voordat er überhaupt een verdachte in het vizier komt. Meer dan bij traditionele criminaliteit lijkt het opsporingsonderzoek veel tijd in beslag te nemen Zo stelt een advocaat: "Die zaken lopen heel lang in eerste aanleg omdat er ook redelijk veel onderzoeken zijn op technisch vlak en het gewoon sowieso grotere onderzoeken zijn met een ontkennende verdachte." (Expertinterview 16, Advocaat)

Meerdere experts noemen het ontkennen van het plegen van een delict door een verdachte als een complicerende factor, omdat het bewijs dat de verdachte het daadwerkelijk was die op een bepaald moment achter een bepaalde computer zat en online verantwoordelijk was voor een bepaalde handeling, lastig te leveren is. Zo kan een verdachte volgens een expert bewust 'zand in de machine strooien' door allerlei vragen op te werpen, zodat het Nederlands Forensisch Instituut dat moet gaan uitzoeken (waarbij ook wachttijden gelden) om vervolgens áls de zaak eenmaal voorkomt strafkorting te krijgen vanwege de lange tijd die verstreken is. Dit geldt volgens hem specifiek voor de 'oude rotten', die precies weten hoe het werkt, van de termijnen op de hoogte zijn en daarom niets zeggen en niet meewerken. Bij jeugdigen kan het zo zijn dat ze wel direct bekennen zodra ze worden aangehouden en worden geconfronteerd met het bewijs. Er zijn echter ook jeugdigen voor wie dat niet geldt, bijvoorbeeld de jeugdigen die ook drugs verhandelen via het darknet en dus het hardcore criminele pad opgaan. Volgens deze respondent komt het erop neer dat de overheid snel moet handelen om geloofwaardig te zijn: "Je kan niet tegen zo'n jeugdige zeggen: twee jaar later kom je nog eens op zitting." (Expertinterview 25, Politie)

Sommige cyberdaders vertellen dat zij pas werden opgepakt op het moment dat het gepleegde delict al een jaar of langer geleden was. Verschillende daders geven aan dat voor hen de justitiële interventie die uiteindelijk volgde veel te laat kwam en daardoor eigenlijk geen effect, functie of nut meer had. Vaak hadden zij al besloten te stoppen met criminaliteit en hun leven een andere wending weten te geven.

De snelheid van het ontdekt en aangehouden worden kan aldus van grote invloed zijn op het verloop van het delictgedrag. Immers, zoals in paragraaf 7.2.1 is beschreven, heeft het moment van opgepakt worden voor in het bijzonder jeugdige, *first offenders*, op zichzelf en los van een eventuele straf, reeds grote impact.

7.2.3 Streng

Over wat een passende reactie is op cybercriminaliteit bestaan zowel in de literatuur als in de praktijk veel vragen. Omdat grenzen van tijd en ruimte wegvallen, kan de impact van cybercriminaliteit veel groter zijn dan van offline criminaliteit. Zo kan de schade enorm groot zijn maar is tevens de omvang ervan niet altijd duidelijk vast te stellen, waardoor onduidelijkheid bestaat over wat een passende reactie is (Marcum, Higgins & Tweksbury, 2012). Smith et al. (2004) schreven dat officieren van justitie in de VS zich hierdoor in een lastig parket bevinden: aan de ene kant wil men in serieuze gevallen, waarin bijvoorbeeld op wereldwijde schaal forse schade is aangericht aan infrastructuren, een duidelijk afschrikkende reactie geven, zowel naar de dader als naar de samenleving als geheel (p. 96). Aan de andere kant, indien een dergelijke delict door jeugdigen en *first offenders* is gepleegd, lijkt juist een milde aanpak aangewezen. Bovendien lijkt volgens deze auteurs een afschrikwekkende reactie meer gepast bij bijvoorbeeld ransomware dan bij delicten die gepleegd zijn uit nieuwsgierigheid of om sociaal-politieke redenen, zoals een 'vrij' internet of het aanwijzen van kwetsbaarheden (Smith et al., 2004). Immers, wanneer de dader beweert het delict te hebben gepleegd uit nieuwsgierigheid, zonder kwade bedoelingen en zonder het idee dat wat hij deed illegaal was, accepteert deze mogelijk niet dat hij of zij fout bezig was, zodat een reactie gericht op afschrikking dan een beperkt effect zou kunnen sorteren (Smith et al., 2004, p. 214). Alternatieve aanpakken zijn dan mogelijk passender. Waar dus de ernst van het delict tot een zware straf zou nopen, geeft de aard van de verdachte en eventuele strafverminderende omstandigheden zoals *first offender* zijn aanleiding tot een lichte straf. Voor rechters is het een uitdaging hiertussen een balans te vinden, aldus Smith et al. (2004, p. 264).

Ook volgens de geïnterviewde experts dient bij daders die uit nieuwsgierigheid of baldadigheid een (eerste) cyberdelict plegen en die bij aanhouding direct bekennen en spijt betuigen, eerder naar *alternatieve* afdoeningsmogelijkheden te worden gezocht. Bij deze groep wordt meer dan een standje niet nodig geacht. Overeenkomstig de literatuur wordt vermeld dat met het effect van een straf op het verdere leven van een jonge dader rekening wordt gehouden. Indien echter geldelijk gewin of bewuste vernieling (o.a. door ransomware) het hoofdmotief is en er sprake is van een semiprofessionele of georganiseerde dader, dan menen experts dat eerder een *traditionele* strafrechtelijke afdoening zou moeten plaatsvinden.

Los van het specifieke afschrikwekkende effect voor individuele daders menen vooral de experts die werkzaam zijn als (proces)partij binnen het strafproces dat het *generaal preventieve effect* van straffen over het algemeen te laag is. Er worden volgens hen dermate lage straffen uitgedeeld dat hiervan weinig afschrikking zal uitgaan. Mede gezien de combinatie met de lage pakkans is het volgens een rechter denkbaar dat de opgelegde straffen uiteindelijk omhoog zullen gaan juist om generale afschrikking te bereiken. Er zouden volgens experts momenteel onvoldoende voorbeeldcasussen worden gepresenteerd waarbij van de opgelegde straf een signaalfunctie kan uitgaan. Ook de rechter meent dat een dergelijke signaalfunctie kan uitgaan van voorbeeldzaken:. Een voorbeeld zou volgens een advocaat in het bijzonder gesteld kunnen worden met 'grote vissen' die opgepakt worden:

> Ik denk dat generale preventie echt belangrijk is. […] De pakkans blijft nihil, dus ik denk dat die straf gewoon een stuk omhoog moet voor de serieuze daders. Want het zijn vaak wel echt rationele dadertypen. […] Anders denkt iedereen die ook iets stukmaakt 'nou prima, de pakkans is nul, en de één-op-de-miljoen díe gepakt wordt, krijgt toch een pisstrafje. (Expertinterview 1, Advocaat)

Deze advocaat doelt hierbij niet zozeer op de strafdreiging (maximum straf) die op een cyberdelict staat, maar op het feit dat op dit moment de maximaal op te leggen straf in de door het OM geëiste straf nauwelijks wordt benaderd. Hij noemt het voorbeeld van een strafbaar feit waarvoor het wettelijke strafmaximum van één jaar gevangenisstraf geldt, maar waarvoor – zelfs wanneer men 'de grootste vis aller tijden' te pakken heeft – hooguit twee maanden wordt geëist, hetgeen volgens hem totaal niet afschrikwekkend werkt. Deze mening wordt gedeeld door een politieagent:

> Als ze het er op social media onderling over hebben, is het zo van 'DDoSsen, je moet even vegen en je krijgt misschien een boetetje, that's it'. Er staan gewoon geen hoge straffen op. Het wetboek zegt vijf jaar hè, voor een aanval op een vitale infrastructuur. Als je het betalingsverkeer platlegt in Nederland, volgens mij zit je dan wel in de vitale hoek. Als je zegt het is niet vitaal maar een gewone DDoS, is het nog steeds twee-drie jaar; en dan krijg je alleen een taakstraf? […] Het is een signaal van niks als ze vervolgens wegkomen met een taakstraf. (Expertinterview 25, Politie).

In de literatuur wordt erop gewezen dat criminelen zich vaak bas**e**ren op ervaringen van andere criminelen (Kleck et al., 2005). Uit de interviews kan worden opgemaakt dat dit naar alle waarschijnlijkheid niet heel anders is voor cyberdaders. Aangezien daders, en dus ook cyberdaders, zich vooral lijken te baseren op verschillende (niet officiële) bronnen, waaronder de media, is het van minder belang hoe groot of klein de reële strafdreiging is, maar draait het uiteindelijk om de perceptie die iemand heeft (Kleck et al., 2005). Derhalve kan in de literatuur steun gevonden worden voor de door experts benadrukte 'signaalfunctie' van zaken waarmee een voorbeeld kan worden gesteld. Uit de interviews met experts komt net als uit de literatuur het beeld naar voren dat er nog veel onduidelijkheid bestaat over wat een passende straf zou vormen. Een aantal aspecten die meegewogen dienen te worden bij het bepalen van de ernst van het delict, en vervolgens de ernst van de straf, zijn bij cyberzaken minder eenduidig dan bij offline criminaliteit. Te denken valt aan het aantal slachtoffers, de frequentie van het delict, de potentiële schade van het delict en de impact van het delict op samenleving en slachtoffers. De vraag is hoe al deze factoren dienen mee te wegen bij het bepalen van een passende straf.

Naast het bepalen van de zwaarte van het delict, is het volgens experts ook ten aanzien van andere aspecten lastig tot een passende straf te komen. In de eerste plaats gaat er vaak een veelheid aan delicten achter een zaak schuil. Dan is het de vraag welk feit primair ten laste wordt gelegd. Een rechter noemt het voorbeeld van phishing, waaronder misschien wel zeven verschillende delicten schuilgaan, waaronder diefstal, oplichting, valsheid in geschrifte, witwassen, het vervaardigen van malware of het deelnemen aan een criminele organisatie. Dan is het van belang dat het delict dat het meest kenmerkend is voor het gedrag of het delict dat de hoogste straf kent, primair ten laste wordt gelegd. De maximale strafhoogte kan per delict weleens de helft schelen. Wordt oplichting ten laste gelegd, dan geldt een gevangenisstraf van ten hoogste vier jaren. Wordt witwassen ten laste gelegd, dan kan een gevangenisstraf van ten hoogste acht jaren gelden.

Sommige experts menen dat de impact van het delict voor met name slachtoffers niet serieus genoeg wordt genomen. Volgens een advocaat loopt de opsporing van cyberzaken in Nederland voorop, maar maken cyberofficieren er vervolgens alleen een serieuze zaak van als er sprake is van drugshandel of kindermisbruik. Dit zou volgens een politie-expert ook kunnen komen doordat, wat

ook bij daders zelfs dus speelt, het als minder ernstig wordt gezien dan traditionele criminaliteit, terwijl de schade feitelijk groter is:

> Het strafrecht zou iets meer moeten focussen op wat voor uitwerking heeft nu eigenlijk zoiets als dat je rekening in een keer wordt leeggeplunderd.[…] Ik denk dat op het moment dat je fysiek een overval pleegt, dat het veel zwaarder wordt gezien nog dan wanneer je iemand van 20.000 euro digitaal berooft. (Expertinterview 25, Politie)

Op grond van deze bevindingen lijkt het er dus nog onvoldoende duidelijkheid te bestaan over wat een passende straf is, niet alleen voor partijen binnen het strafproces en verdachten, maar ook voor de samenleving als geheel, nu een duidelijk generaal afschrikwekkend effect vanwege de lage pakkans in combinatie met soms lage straffen lijkt te ontbreken.

7.3. Reactieve interventies die de rationele keuze kunnen beïnvloeden

7.3.1. Gevangenisstraf

Uit de literatuur blijkt dat er nauwelijks onderzoek is gedaan naar gevangenisstraffen voor cyberdaders. In ieder geval zijn er geen Nederlandse studies hieromtrent gevonden. Twee studies uit de VS beschrijven dat ongeveer de helft tot 65% van de vervolgde cyberdaders (voor allerlei vormen van computergerelateerde criminaliteit) een gevangenisstraf opgelegd heeft gekregen (Marcum et al., 2012) en dat voor cybercriminaliteit in enge zin minder lange gevangenisstraffen werden opgelegd dan voor cybercriminaliteit in ruime zin (Smith et al., 2004). Uit deze studies zijn een aantal kenmerken te destilleren die mogelijk ook bij Nederlandse cybercriminaliteitzaken een rol spelen. Ten eerste dat cyberdaders in vergelijking met daders van traditionele vormen van criminaliteit, minder vaak een gevangenisstraf opgelegd krijgen (Marcum et al., 2012). Ten tweede dat de kans om een gevangenisstraf opgelegd te krijgen groter wordt in geval van een eerdere veroordeling voor een geweldmisdrijf (Marcum et al., 2012). Ten derde dat bij cybercriminaliteitzaken waarbij sprake is van kinderpornografie of ander obsceen materiaal, de gevangenisstraffen hoger zijn dan bij cybercriminaliteit in enge zin (Smith et al., 2004). Ten vierde dat bij cybercriminaliteit in enge zin, in vergelijking met cybercriminaliteit in ruime zin, er meer variëteit in de opgelegde interventies is, en dus minder vaak sprake is van een gevangenisstraf (Smith et al., 2004).

Uit de Nederlandse praktijk komen verschillende beelden naar voren over de toepassing van hechtenis of een gevangenisstraf bij daders van cybercriminaliteit. Een strafrechtadvocaat merkt op dat hij, in tegenstelling tot zijn collega's, niet de hele dag op en neer hoeft naar de gevangenis om cliënten te bezoeken, omdat voor cybercriminaliteit in enge zin geen gevangenisstraffen worden opgelegd (Expertinterview 5). Deze expert geeft aan dat het vaak voorkomt dat de officier van justitie een gevangenisstraf eist, maar dat de rechter voor een taakstraf gaat. Vooral bij *first offenders* lijkt een gevangenisstraf weinig te worden opgelegd. Volgens de meeste experts is dit ook niet (meer) nodig in die gevallen waarin het in voorarrest zitten al voldoende afschrikwekkend werkt (speciale preventie). "Vaak worden ze echt wel wakker geschud door een nachtje cel. […] Als je het daarna seponeert maakt niet eens meer uit, dan is het opeens heel echt" (Expertinterview 1, Advocaat).

Echter, ook bij zaken die de 'bovengrens van de ernst van zaken' betreffen, zoals bekende bitcoinwitwaszaken, ziet een advocaat dat het voorkomt dat de veroordeelde ondanks een gevangenisstraf van drie jaar, waarvan een jaar voorwaardelijk, uiteindelijk zijn hele gevangenisstraf in een open kamp heeft uitgezeten en zodoende 'gewoon' thuis kon zitten met een enkelband en kon werken. Een andere advocaat herkent dit beeld echter niet, en ziet dat zaken van verdachten die op

grotere schaal delicten plegen en veel verschillende slachtoffers hebben gemaakt, wel heel vaak uitmonden in een gevangenisstraf. Voor phishers of de 'echte darkwebjongens' lijken experts het erover eens te zijn dat wel standaard gevangenisstraffen worden opgelegd. Dit type dader heeft volgens een respondent reeds (veel) ervaring met 'zitten'.

7.3.2. Financiële gevolgen

Andere interventies gericht op afschrikking zijn de geldboete (als straf) en financiële maatregelen, zoals de schadevergoeding en het verbeurd verklaren van goederen. Mits deze gevolgen voldoende zwaarwegend (*streng*) zijn, kunnen ze een dader afschrikken nogmaals een delict te plegen. Deze interventies passen tevens bij het rationele keuzeperspectief en bij het situationele criminaliteitspreventiemodel dat criminaliteit eveneens wil voorkomen door maatregelen die de opbrengsten verlagen.

Ook over financiële gevolgen is weinig onderzoek gevonden. Volgens een uit de VS afkomstige studie worden schadevergoedingsmaatregelen geregeld opgelegd, juist in zaken waarin sprake is van financieel georiënteerde cybercriminaliteit, zoals fraude, diefstal of het aanpassen van data. Daarbij geldt als uitdaging om de exacte omvang van de schade vast te stellen (Smith et al., 2004). Tevens geldt daarbij als vraag of de daders de schadebedragen, zeker als deze in de honderdduizenden euro's lopen, überhaupt wel kunnen terugbetalen (Smith et al., 2004).

De geïnterviewde experts benoemen ook dergelijke dilemma's bij het opleggen van financiële consequenties. Veel respondenten zijn niet erg uitgesproken over de wenselijkheid van forse financiële consequenties. Zij lijken dit af te wegen tegen de draagkracht van de dader. Sommige experts vinden dat het momenteel te weinig gebeurt dat een dader bewust wordt gemaakt van alle, dus ook de financiële, consequenties, door iemand financieel "echt te laten bloeden". Vooral voor daders die met cybercriminaliteit geld hebben verdiend, zou erop moeten worden ingezet dat misdaad niet mag lonen, althans volgens een medewerker van de politie. Het afpakken van verdiend geld of spullen die met dit verdiende geld worden aangeschaft, zou vooral bij jongeren en jongvolwassenen 'pijn' (moeten) doen. Bij verschillende geïnterviewde cyberdaders is gebleken dat de inbeslagname van hun computerapparatuur voor hen als de zwaarste 'straf' gold, ook als daarna nog een officiële straf volgde:

> Dat de politie m'n computer had meegenomen en dat ik alles kwijt was. Dat is gewoon jaren aan dingen die je hebt geprogrammeerd en honderden en misschien wel duizenden uren wat er allemaal in zit. En ja, ook allemaal websites die ik door de jaren heen heb gehackt en de database van heb opgeslagen. Dat was ik allemaal kwijt. (Daderinterview 8).

Hoewel herstel van de schade een belangrijk onderdeel van de straf zou moeten zijn, blijkt dat in de praktijk echter vaak onmogelijk omdat daders relatief weinig vermogend zijn en de schade groot is. Bovendien zouden hoge schadevergoedingen in het geval van jeugdigen de dader voor de rest van zijn leven met een zware financiële last opzadelen. Dat is volgens een expert "een molensteen die je hem niet gunt." Hoewel het volgens experts een goede optie is daders een deel van de schade te laten vergoeden, blijkt het in de praktijk lastig een evenwicht te vinden tussen het financieel 'pijn doen' en het niet omhangen van een 'molensteen'. Een advocaat beschouwt de (lage) schadevergoedingen die bij jeugdigen worden opgelegd vooral als een *symbolische* maatregel. Volgens verschillende experts zijn het bovendien vaak de ouders die, soms vanuit schaamte, de portemonnee trekken. Dit roept de

vraag op in hoeverre de financiële consequenties door jeugdigen persoonlijk worden gevoeld om daarmee het gewenste afschrikwekkende effect te kunnen sorteren.

Ten slotte is het verhalen van schade afhankelijk van het indienen van een schadevergoedingsverzoek door slachtoffers. Dit zou per type delict verschillen. Volgens een rechter dienen lang niet alle slachtoffers een vordering tot schadevergoeding in. Een bedrijf wil bijvoorbeeld geen negatieve publiciteit. Daarnaast hebben bedrijven volgens een van de geïnterviewde daders niet altijd weet van het feit dat ze zijn opgelicht, indien het om kleinere bedragen gaat (Daderinterview 14). Deze dader, die online spullen had besteld zonder ervoor te betalen, wilde na zijn aanhouding schoon schip maken door met de gedupeerde bedrijven in gesprek te gaan en het geld terug te betalen, maar uiteindelijk kwam het neer op het betalen van een schadevergoeding aan de overheid.

7.4. Preventieve interventies die de rationele keuze kunnen beïnvloeden

7.4.1. Knock and talk

Knock and talk is een waarschuwingsgesprek dat de politie houdt met (potentiële) verdachten aan huis, waarbij met hen in gesprek wordt gegaan over de strafbaarheid van hun online gedrag (Politie, 2018). Het doel van het waarschuwingsgesprek is bewustwording te creëren ten aanzien van de risico's en gevolgen van online (strafbaar) gedrag en tevens af te schrikken door het signaal af te geven dat niemand er vanuit kan gaan anoniem te zijn (Politie, 2018). Omdat er vaak voor een dergelijke interventie wordt gekozen wanneer er onvoldoende reden is tot aanhouding over te gaan, wordt een dergelijk gesprek hier onder de preventieve interventies geschaard. Een voorbeeld betreft de actie die de politie in 2018 hield tegen gebruikers van DDoS-aanvallen via de (illegale) website Webstresser.org. Bij een aantal verdachten heeft de politie, nadat de verdachten met het bewijs waren geconfronteerd, besloten het bij een dergelijke waarschuwing te laten:

> De jongens vertelden de politie dat ze niet hadden gedacht dat dossen zo makkelijk was. Ze zeiden dat ze niet goed wisten of het nu wel of niet illegaal was. Jonge verdachten die bijvoorbeeld alleen maar tegenstanders in hun game 'DoSten', willen we niet direct een strafblad bezorgen. (Vermaas, 2018)

In de (internationale) literatuur is geen onderzoek naar dit soort interventies gevonden. Wel verscheen in 2017 een rapport van de National Crime Agency (2017) in het Verenigd-Koninkrijk, waarin zij verslag doen van *cease and desist* bezoeken. Dit houdt in dat een politieagent een persoonlijk bezoek brengt bij personen die 'op het randje verkeren' van het plegen van cybercriminaliteit. De agent bespreekt de potentiële link van de persoon met criminele activiteiten en spoort diegene aan met deze activiteiten te stoppen, omdat er anders consequenties zullen volgen. Het gaat om personen die zich in de periferie van cybercriminaliteit begeven maar (nog) niet daadwerkelijk verdacht worden van het plegen van delicten (National Crime Agency, 2017). De werkzame mechanismen van zowel de Engelse als de Nederlandse variant van huisbezoeken door de politie zijn dus afschrikking, door enerzijds anonimiteit te verbreken en te laten weten dat deze personen in beeld zijn bij de politie en anderzijds te wijzen op de risico's en gevolgen als zij niet stoppen met het (strafbare) gedrag. Vanuit het afschrikkingsperspectief draagt dit bij aan bewustwording van de mogelijke ernst van de gevolgen of kosten van criminele gedragingen (*streng*). Ook draagt het bij aan de perceptie van het risico opgepakt te worden, nu men weet bij de politie in beeld te zijn (*zeker*).

De geïnterviewde experts hebben wisselende verwachtingen. Vooral politie-experts die zelf ervaring hebben met dit soort gesprekken en OM-medewerkers hebben positieve verwachtingen van

knock and talks. Een officier van justitie was vooral verwachtingsvol over deze interventie bij jeugdigen:

> Het is effectief omdat het handelen van zo'n, vaak adolescent, uit het anonieme gehaald wordt en zichtbaar gemaakt wordt, in ieder geval in zijn directe omgeving. Zijn ouders zien dat er wat aan de hand is. Het feit dat er politie aan de deur staat, of in de gang staat, dat zelf is al echt een enorm schrikmoment voor veel van deze. Dat zie je niet elke dag, dat is nogal heftig en ze komen ook om te praten over iets wat ik heb gedaan, met mijn ouders erbij. Dat heeft echt wel impact. (Expertinterview 13, Officier van Justitie)

Mechanismen die in de literatuur worden genoemd komen ook terug in de interviews met de experts. Volgens een cybersecurityexpert is voldoende "dat ze weten dat ze gezien zijn". Ditzelfde werkzame mechanisme – het uit de anonimiteit halen – wordt door politie-experts genoemd die dit vooral voor pubers als een effectief middel zien. Als bij die doelgroep niet op tijd wordt ingegrepen zou het namelijk, wanneer zij steeds verder in hackerskringen terechtkomen, steeds meer zelfdiscipline vragen om er weer uit te stappen.

Daarnaast is vroeg ingrijpen te prefereren, omdat daarmee iemand uit het klassieke strafrechtelijke traject wordt gehouden. Volgens een officier zijn *knock* and *talks*, mede daardoor, ook erg efficiënt. Het bespaart capaciteit doordat mensen die een strafrechtelijke grens over dreigen te gaan, maar er nog net niet helemaal over zijn, tijdig geïnformeerd kunnen worden. Een politieagent spreekt in de dit kader van een 'draai om de oren.' Ook kan bijvoorbeeld illegale software in beslag worden genomen. Daardoor kunnen mogelijk verdere maatregelen uitblijven. Juist omdat dit volgens hem een grote groep mensen betreft, zou het een efficiënt en effectief middel kunnen zijn. Een van de geïnterviewde politie-experts ziet ook meerwaarde in een variant met doorzoeking en inbeslagname van apparatuur, waarbij verder niet tot aanhouding wordt overgegaan tenzij de persoon ermee door gaat.

De officier ziet echter ook dat een dergelijke interventie twee verschillende kanten kan opwerken. Aan de ene kant kan een potentiële dader het risico te hoog vinden of het de moeite niet meer waard vinden. Dat laatste is bijvoorbeeld als de ouders de computer van de kamer van hun kind hebben afgehaald of de telefoon hebben afgenomen. Aan de andere kant kan het ertoe leiden dat de potentiële dader juist de *operational security* opvoert zodat men hem nooit meer kan vinden. In dit verband verwacht een advocaat zelfs een mogelijk risicoverhogend effect van dit soort gesprekken omdat volgens hem geldt: hoe lichter je eerste interventie, hoe groter de kans op (herhaalde) criminaliteit. Daarnaast stelt deze advocaat:

> Ik sluit dan ook niet uit of dat iets tofs wordt. Dat ze dan zeggen "Joh ik heb net een knock and Talk gesprek gehad hierbinnen". Weet je, ik zet nog vijf proxies tussen mezelf en de volgende actie. Nee, ik denk dat daar misschien toch niet voldoende dreiging vanuit gaat. (Expertinterview 1, Advocaat).

Dit sluit aan bij verschillende theoretische perspectieven dat interventies juist deviant of crimineel gedrag kunnen stimuleren omdat het als statusverhogend wordt gezien (Smith et al., 2004) of juist de uitdaging en spanning (*thrill*) bieden waar hackers naar op zoek zouden zijn (Steinmetz et al., 2017). Een *knock and talk*-interventie zou dan eerder de beloning vergroten dan de kosten verhogen,

waardoor per saldo de balans om criminaliteit te plegen er niet op de gewenste manier door beïnvloed wordt.

7.4.2. Voorlichting op school

Een vorm van generale afschrikking is het op school geven van voorlichting aan jeugdigen over de gevolgen van het plegen van cybercriminaliteit. In hoofdstuk 3 is beschreven dat het toezicht van ouders op online gedrag vaak beperkt is, wat het belang van de rol van de school hierin benadrukt. Bovendien is ten aanzien van de initiatie van criminele carrières van cyberdaders beschreven hoe bij jongeren binnen de context van games een zekere normalisering kan optreden, omdat het normaal is om elkaar te DDoSsen of te hacken. Dit wordt erkend door een politiemedewerker: "Jongeren ontwikkelen zich super snel en er zijn nergens rode vlaggen; je weet niet dat het niet mag, niemand heeft toezicht, je ouders corrigeren je niet. Je kunt zo makkelijk die criminele stappen doorlopen".

Hoewel er geen (evaluatie)onderzoek naar voorlichting naar voren kwam in het literatuuronderzoek, onderstrepen verschillende auteurs het belang van hiervan. Door middel hiervan zou bewustwording kunnen worden gecreëerd over de gevolgen van online strafbaar gedrag, wat generale afschrikking onder jeugdigen kan bewerken. Zo wijst Bae (2017) erop dat scholen geregeld lessen moeten bieden over correct computer- en internetgebruik, de normen en regels in cyberspace en de consequenties van delinquent online gedrag. Dit zou onderdeel moeten uitmaken van het formele en informele curriculum van de school, zoals ook Cassidy, Faucher en Jackson (2013) stellen.

In aansluiting op deze literatuur, geldt volgens experts ook in Nederland dat er te weinig voorlichting wordt gegeven op scholen en worden er ook weinig preventieve interventies voor jeugdigen ontwikkeld. Scholen zouden zich onvoldoende bewust zijn van de online mogelijkheden en gevaren en zien ze dit niet als een urgent probleem of gevaar. Volgens een expert nemen scholen pas de verantwoordelijkheid om aan preventie te werken als zij zelf slachtoffer zijn geworden (bijvoorbeeld van een DDoS-aanval). In aansluiting op de literatuur is het volgens experts belangrijk dat voorlichting op scholen gaat over welk gedrag strafbaar is (de strafbaarheid), want daarvan zouden kinderen vaak (nog) geen benul hebben. Zo stelt een expert:

> Hoe jonger je begint met die bewustwording, hoe makkelijker je kan voorkomen dat het mis gaat en dat ze later alsnog [een webshop] ofzo gaan hacken. Ik denk dat dat als preventieve factor wel heel goed werkt maar dat is zeer recent, pas sinds een jaar ofzo aan het opkomen. (Expertinterview 14, Cybersecurityexpert).

Daarnaast moeten de strafrechtelijke consequenties, dus wat voor straf er opgelegd kan worden als je de fout ingaat (de strafdreiging), duidelijk worden gemaakt. Ze moeten daadwerkelijk gewezen worden op de juridische implicaties van het plegen van een strafbaar feit. Ten slotte moet duidelijk worden welke schade berokkend wordt aan bedrijven of individuen, omdat jeugdigen dat niet kunnen inschatten. Dit gebeurt echter volgens experts nog veel te weinig en zou bovendien al op de basisschool moeten beginnen, omdat kinderen op zeer jonge leeftijd al beginnen met gamen.

Net zoals bij *knock and talk* gesprekken zien experts ook bij voorlichting op scholen dat de interventie twee kanten op kan werken. In plaats van bewustwording en afschrikking kan het averechts werken, doordat de nieuwsgierigheid van jeugdigen wordt geprikkeld. Volgens een advocaat zou voorlichting over strafbaarheid en strafrechtelijke gevolgen - mede gezien de lage pakkans - niet het gewenste afschrikwekkende effect sorteren:

> De meeste van de mensen zijn jonge jongens, die doen informatica, die gaan een beetje tegen elkaar opsnijden en ik denk dat als de leraar zegt dat het niet mag, ja… […] Ik denk dat die jongens nu gewoon denken joh wat voor kwaad kan het ook, omdat ze gaan zien dat de straffen nihil zijn en de pakkans nihil. (Expertinterview 1, Advocaat)

Voorlichting op scholen zou volgens deze advocaat dus afschrikwekkend kunnen werken, mits crimineel gedrag voldoende *zeker* en *streng* wordt bestraft. Een rechter heeft dezelfde bedenkingen bij het optuigen van voorlichtingscampagnes en zegt niet te kunnen inschatten of dat een generaal preventieve werking heeft, omdat het juist ook mensen op ideeën kan brengen. Al met al lijkt voorlichting over de strafbaarheid van online grensoverschrijdend gedrag vooral van waarde voor jongeren van zeer jonge leeftijd dan wel bij wie drijfveren als interesse en nieuwsgierigheid niet van invloed zijn. Voor jeugdigen die wel worden getriggerd door de uitdaging en spanning die dergelijke gedragingen met zich brengen, zou voorlichting mogelijk, mede vanwege de lage pakkans, een averechts effect kunnen hebben.

7.4.3. Online policing

Online policing zou een bijdrage kunnen leveren aan de afschrikking van cyberdaders, bijvoorbeeld in de vorm van online zichtbaarheid, online reageren en online opsporingsbevoegdheden. Van *online policing* zijn diverse voorbeelden gevonden in de internationale literatuur. Aiken et al. (2016) zien een belangrijke preventieve rol weggelegd voor de politie op meerdere fronten, waarbij vooral de politieaanwezigheid online zichtbaar moet zijn. Juist omdat er geen online aanwezigheid is van de 'sterke arm', zoals op straat wel het geval is, zien jeugdigen mogelijk de risico's van hun gedrag niet in. In dit verband verwijzen zij naar allerlei termen die hiervoor gebruikt worden: '*web constable*', '*web patrouille*', '*policing in cyberspace*' en '*online community policing*'. Het gaat er volgens deze auteurs om dat niet alleen het opsporingswerk, maar ook het meer alledaagse politiewerk, zoals preventie, bewustwording en algemeen advies op het gebied van cybersecurity online plaatsvindt. Hiervoor zouden jonge politieagenten kunnen worden ingezet die zich fulltime bezighouden met een rondgang rond fora en chatrooms waarbij ze zichzelf kenbaar maken, aanspreekbaar zijn en een positieve invloed proberen uit te oefenen (Aiken et al., 2016, p. 18).

Warning banners

Een andere manier waarop de politie haar online zichtbaarheid kan vergroten, is door het plaatsen van *warning banners*. Dat zijn digitale waarschuwingsberichten om te voorkomen dat iemand online delictgedrag vertoont. Dit is de enige preventieve interventie waarnaar een viertal quasi-experimentele studies is verricht. Hierbij zetten de onderzoekers *honeypot* computers[74] in om hackers te 'lokken', waarmee men de acties die worden uitgevoerd nauwkeurig kan volgen en zodoende het verschil kan meten bij hackers die wel en geen waarschuwingsbericht te zien krijgen. De studies, allen afkomstig uit de VS, laten wisselende resultaten zien. Zo blijkt dat het gebruik van *warning banners* het aantal gevallen van (illegaal) binnendringen van een computer niet vermindert, maar wel de *duur* van het binnendringen significant vermindert (Maimon, Alper, Sobesto & Cukier, 2014). Ook andere onderzoekers vonden slechts een gedeeltelijk effect van *warning banners* (Wilson, Maimon, Sobesto

[74] Een computersysteem dat met opzet niet goed beveiligd is, met als doel het te laten aanvallen, zodat men deze aanval kan analyseren.

& Cukier, 2015; Testa, Maimon, Sobesto & Cukier, 2017). Zo bleek het variëren met verschillende type *warning banners* met 1) een altruïstische boodschap gericht op morele overtuiging, 2) dreiging met een officiële sanctie, 3) een ambigue dreiging, geen significante uitkomsten op te leveren (Howell, Cochran, Powers, Maimon & Jones, 2017). Op basis van deze bevindingen kan dus slechts beperkt steun worden gevonden voor het afschrikwekkende effect van *warning banners*.

Steinmetz (2017) biedt een verklaring voor het beperkte afschrikwekkende effect van *warning banners*: voor sommige hackers zou het risico van gepakt kunnen worden juist een vorm van spanning (*thrill*) bieden. Dit maakt deel uit van het avontuur waarnaar zij op zoek zijn (Steinmetz et al., 2017; Steinmetz, 2017). Bijgevolg kunnen *warning banners* cybercriminaliteit dus juist *stimuleren*, doordat de dreiging van straf onderdeel wordt van het plezier of de beloning die hacken oplevert, een soort van *sneaky thrill* (Katz, 1988; Steinmetz et al., 2017). Bezien vanuit de kosten-batenafweging die hackers volgens de rationele keuzetheorie maken, zouden zij hierdoor dus mogelijk juist aangemoedigd in plaats van afgeschrikt worden.

Ook de experts hebben wisselende verwachtingen ten aanzien van het nut van *warning banners*. Volgens een officier zou het bij bepaalde hackers werken een online waarschuwingsbericht te krijgen ("I know! I see you!") en zou dat meer afschrikken dan een gesprek met 'Jan de Agent' (Expertinterview 13, Officier van Justitie). Volgens een politiemedewerker zouden dergelijke waarschuwingen ook op hackersfora of in games getoond kunnen worden, vooral om het proces van normaliseren van illegaal gedrag tegen te gaan. Een ethische hacker die aanwezig was bij de expertmeeting verwacht dat het wel effect kan hebben als jongeren een pop-up te zien krijgen van de politie wanneer zij googelen op DDoS maar niet weten dat het illegaal is. Het merendeel van de experts is sceptischer hierover. Zo verwachten sommige experts dat een dergelijke interventie vooral voor bepaalde doelgroepen zou werken. Bijvoorbeeld wel voor kinderen, maar niet voor personen die al langer actief zijn. Een politie-expert verwacht dat het door hackers gewoon zal worden weggelachen en advocaten stellen vraagtekens bij het nut van een dergelijke interventie.

7.4.4. Verstoring

Verstoring is een strategie die gesitueerd kan worden in het kader van afschrikking, in het bijzonder sluit het aan bij de strategieën van situationele criminaliteitspreventie (Hutchings & Holt, 2017). Hieronder vallen het *vergroten van de te nemen moeite*, het *verhogen van het veronderstelde risico* en het *verlagen van de opbrengsten* van criminaliteit. Verstoring is specifiek gericht op het opwerpen van barrières in (verschillende fases) van de uitvoering van delicten. Daarmee is het dus ook gericht op het beïnvloeden van de kosten/batenafweging van financieel gemotiveerde daders (Goldman & McCoy, 2016).

Een aantal bij de opsporing betrokken experts noemen vormen van verstoring waarvan zij geloven dat deze kunnen bijdragen aan de afname in criminaliteit. Door een cybersecurityexpert wordt in dit kader bijvoorbeeld het toepassen van overheidsregulering op bitcoin wisselkantoren genoemd (Expertinterview 21). Zo noemt hij het voorbeeld van de FIOD die een bitcoin mixer[75] offline haalde die in Nederland werd gehost. Een ander voorbeeld van verstoring is het aanpakken van *facilitators*, die diensten verlenen aan cyberdaders, zoals het aanbieden van software en netwerken, omdat die niet zouden vinden dat ze crimineel bezig zijn. Daarbij noemt deze cybersecurityexpert de

[75] Ook wel *cryptocurrency mixing service* genoemd. Dit betreft een dienst die de herkomst van bitcoins of andere cryptovaluta kan verhullen en gebruikt kan worden om cryptovaluta wit te wassen (Zie ook https://www.fiod.nl/fiod-en-om-halen-witwasmachine-voor-cryptovaluta-offline/)

Ennetcom-zaak[76] als voorbeeld (Expertinterview 21). Verschillende experts geloven dat het aanpakken van de criminele dienstverleningsindustrie, dus websites waarop pakketten of bijvoorbeeld DDoS-aanvallen besteld kunnen worden, bijdraagt aan een afname van cybercriminaliteit. Als voorbeeld wordt hier een recente internationale actie aangehaald waarbij een grote website, op dat moment de grootste criminele dienstverlener waarop men DDoS-aanvallen kon kopen, is neergehaald (dezelfde actie als waarbij *knock and talk* gespreken, zoals hierboven beschreven, zijn gehouden): "Als de meest laagdrempelige dienstverlener niet meer bereikbaar is, kun je opzoek naar een andere of bedenken dat het niet meer de moeite is. Dus het kan wel effect hebben" (Expertinterview 13, Officier van Justitie).

Dergelijke vormen van verstoring zouden mogelijk effect kunnen zijn, omdat ze aansluiten bij de bevindingen omtrent de *perceptie van strafbaarheid* en de *initiatie van* de criminele carrière van cyberdaders. Door daders wordt het *gemak* waarmee online delictenonlinedelicten kunnen worden gepleegd als drempelverlagend beschouwd om er in te stappen. Hierbij werd gedoeld op het gemak waarmee websites en fora kunnen worden gevonden waar het plegen van cybercriminaliteit wordt uitgelegd of gefaciliteerd. De toegang tot kant-en-klare tools of pakketten om cybercriminaliteit te plegen (het *crime-as-a-service* principe) bleek voor zowel jeugdige als volwassen daders een factor van betekenis bij de initiatie. Verstoringmaatregelen zouden zich juist op dit soort platformen kunnen richten, waardoor daders minder snel en gemakkelijk de opstap naar cybercriminaliteit kunnen maken.

Een ander voorbeeld van een verstoringsmaatregel die is genoemd is het neerhalen van de Hansa Market. Een dergelijke interventie zou volgens een cybersecurityexpert bijdragen aan het wegnemen van *onderling vertrouwen* online, waar men op inzette bij het sluiten van deze (drugs)markt[77] (zie verder Van Wegberg & Verburgh, 2018). Een expert die zich naar eigen zeggen te midden van hackerskringen begeeft, geeft aan dat de Hansa Market-actie tot goede online zichtbaarheid van de politie heeft geleid en 'echt wel indruk heeft gemaakt' en 'respect heeft afgedwongen' bij hackers over de hele wereld.

7.5. Conclusie

In deze afsluitende paragraaf wordt kort stilgestaan bij welke interventies volgens de literatuur en de interviews worden verwacht het meest zinvol te zijn. Ten eerste wordt vaak aangesloten bij het klassieke afschrikkingsperspectief, dat ervan uitgaat dat hoe groter de *zekerheid*, *ernst* en *snelheid* van de straf, hoe minder criminaliteit er zal worden gepleegd (Kleck et al., 2005). Uit de interviews kan worden opgemaakt dat ten aanzien van deze drie voorwaarden nog veel winst valt te behalen. Zowel de gepercipieerde als de daadwerkelijke pakkans wordt als zeer laag beschouwd door experts evenals door daders. Daarnaast is verbetering in de doorlooptijden van opsporing, vervolging en berechting mogelijk indien men het grootst mogelijke afschrikwekkende (speciaal preventieve) effect wil sorteren. Het antwoord op de vraag hoe streng of zwaar de straffen dienen te zijn, hangt volgens experts vooral af van de motivatie van de dader, waarbij een onderscheid wordt gemaakt tussen daders die een financieel motief hebben en jonge *first offender*s die door nieuwsgierigheid worden gedreven. Voor de laatstgenoemde groep daders zou het opgepakt worden door de politie vaak al voldoende afschrikwekkend werken, zo blijkt uit zowel de expert- als daderinterviews. Het moment

[76] Het bedrijf Ennetcom faciliteerde een versleutelde berichtenservice waar cybercriminelen gebruik van maakten.

[77] Hansa Market betrof een markplaats op het darkweb (zie ook https://www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html)

van betrapt en opgepakt worden, zou door dit type cyberdader vaak worden aangegrepen om te stoppen met het online delictgedrag. Anderzijds zou volgens verschillende experts bij serieuze cyberzaken, nu de kans dat daarvoor iemand wordt aangehouden überhaupt laag is, een voorbeeld kunnen worden gesteld naar de samenleving toe, waarvan een generaal preventief effect kan uitgaan. Een dergelijke signaalfunctie wordt ook in de literatuur onderschreven (Kleck et al., 2005). Echter, over wat een passende (zware) straf is, bestaat in de literatuur (Marcum et al., 2012) evenals onder experts en daders op dit moment onzekerheid.

Ten aanzien van de preventieve interventies gericht op afschrikking die in dit hoofdstuk naar voren zijn gekomen, zijn de bevindingen minder eenduidig. Hoewel van preventieve interventies door de politie – zoals *knock and talks* en vormen van *online policing* – inderdaad een afschrikwekkend effect lijkt te kunnen worden verwacht, zijn er tegelijkertijd ook experts die hierbij een averechts effect verwachten. Daders gaan zich bijvoorbeeld beter beveiligen (anonimisering) om niet gepakt te worden. Over *verstoring* zijn de verwachtingen van experts over het algemeen positief (Hutchings & Holt, 2017; Goldman & McCoy, 2016). Uit Nederlands onderzoek blijkt dat van dergelijke – op situationele criminaliteitspreventie gebaseerde – strategieën een criminaliteit verminderend effect kan uitgaan (Van Wegberg & Verburgh, 2018). Ten aanzien van andere preventiemaatregelen die uitgaan van het maken van een (rationele) een kosten-batenafweging door (potentiële) daders worden ook averechtse effecten verwacht, omdat de baten bij cyberdaders divers zijn en niet enkel gericht hoeven te zijn op financieel gewin. Zo kunnen voorlichting op scholen en online waarschuwingsberichten (*warning banners*) de nieuwsgierigheid van jeugdigen prikkelen en hacken juist spannend maken. En een *knock and talk* met een agent aan huis zou bijvoorbeeld ook statusverhogend kunnen werken onder jonge hackers (*peer respect*). Hoewel over het algemeen zeer weinig onderzoek is gedaan naar dergelijke interventies, lieten enkele van de weinige quasi-experimentele onderzoeken die in de VS zijn gedaan naar *warning banners* weinig tot geen significante uitkomsten zien, zodat van een duidelijk afschrikwekkende werking niet kan worden gesproken (Testa, Maimon, Sobesto & Cukier, 2017; Steinmetz, 2017). Nu onderzoek naar preventieve, op afschrikking gerichte interventies, althans in Nederland, nog niet is gedaan om de effecten en bijeffecten van dergelijke preventieve interventies te meten, zou in ieder geval vooralsnog met de genoemde mogelijk averechtse effecten rekening kunnen worden gehouden in de praktijk.

Hoofdstuk 8 Interventies die aansluiten bij *What Works* en *Desistance*

In dit hoofdstuk staan interventies centraal die aansluiten bij de *What Works* of de *desistance* benadering of een combinatie van beide. Vanuit beide benaderingen wordt kritisch aangekeken tegen interventies die primair vanuit een rationele keuzeperspectief of afschrikking ingestoken worden. De kritiek is dat daarbij onvoldoende ruimte wordt geboden om aan achterliggende criminogene of pro-sociale behoeften van daders te werken. Deze kunnen onder andere van belang zijn naast kale straffen omdat (traditionele) criminelen vaak over persoonlijkheidskenmerken blijken te beschikken die er voor zorgen dat ze minder responsief zijn voor strafdreiging. Daarbij gaat het bijvoorbeeld om kenmerken zoals impulsief zijn, snel afgeleid zijn, een korte termijn-focus hebben en gericht zijn op een snelle beloning ongeacht risico's op de lange termijn (Vold, Bernard & Snipes, 2002, in: Kleck et al., 2005). Zoals in hoofdstuk 3 naar voren kwam, worden deze kenmerken minder vaak aangetroffen bij daders van cybercriminaliteit in enge zin, wat zowel met de aard van het delict als de persoon van de dader te maken kan hebben. Voor het deel van de daders dat niet impulsief is en over meer zelfcontrole beschikt dan de traditionele dader, geldt dat ze wellicht gevoeliger zijn voor (een toename in) de straf. Voor het overige deel zouden interventies gericht op afschrikking mogelijk niet effectief zijn omdat andere (criminogene) behoeften en persoonlijke eigenschappen een rol spelen.

Bovendien is een van de kritiekpunten uit de *What Works*-literatuur dat vrijheidsbeperkende straffen mogelijk de criminele vaardigheden of het criminele netwerk vergroten. Deze kritiek is terug te horen bij sommige experts. Er wordt bijvoorbeeld gesuggereerd dat jonge jongens juist geen baat hebben bij detentiestraf omdat zij er 'slimmer' weer uitkomen, gerekruteerd kunnen worden door criminelen en er in ieder geval niet als een beter persoon uitkomen. Een detentieperiode kan in negatieve zin inspelen op criminogene behoeften doordat er relaties kunnen worden gelegd met andere (traditionele) criminelen. In hoofdstuk 6 kwam naar voren dat juist invloed van (niet alleen online, maar ook offline) *peers*, in de vorm van erkenning of het bekrachtigen van pro-criminele attitudes een belangrijke rol lijkt te spelen bij de initiatie en ontwikkeling van cybercriminaliteit.

Tevens kwam in hoofdstuk 6 naar voren dat in het proces van *desistance*, (pro-)sociale bindingen, zoals het hebben van een baan, partner en/of kind, bevorderend kunnen werken. Detentiestraf kan in dit opzicht nadelig uitwerken, omdat sociale bindingen (met familie, vrienden of maatschappij) kunnen worden verbroken en sociaal kapitaal, zoals een inkomen, baan of opleiding, verloren kan gaan. Volgens experts (zie ook hoofdstuk 3) gaat het bij cyberdaders vaak om personen die een opleiding volgen en een bepaald toekomstperspectief hebben waar zij naartoe aan het werken zijn. In die gevallen zou een gevangenisstraf, ook voor meerderjarige daders, minder passend zijn. Voor jongeren geldt dat een gevangenisstraf er niet voor zou moeten zorgen dat zij hun opleiding niet kunnen vervolgen. Experts hebben dus aandacht voor het feit dat een detentiestraf sociale bindingen, met familie en vrienden, en sociaal kapitaal, werk of opleiding, kan verstoren en cyberdaders zouden op dat gebied meer te verliezen hebben dan traditionele daders.

In aansluiting op de *What Works* en *desistance* benadering zal de focus in dit hoofdstuk niet alleen liggen op interventies die gericht zijn op het laten afnemen van criminogene behoeften. Het kan ook gaan om alternatieve interventies, die behulpzaam kunnen zijn voor potentiële, beginnende of zich ontwikkelende cyberdaders, juist door het versterken van protectieve factoren. De interventies die in dit hoofdstuk worden besproken, betreffen interventies die uit de expertinterviews naar voren zijn gekomen als mogelijk behulpzaam of wenselijk. Het gaat dus niet enkel om bestaande, justitiële interventies.

Allereerst worden in dit hoofdstuk de uitgangspunten van de *What Works* benadering (paragraaf 8.1) en de *desistance* benadering (paragraaf 8.2) behandeld. Daarna wordt ingegaan op het belang van het juiste instrumentarium om criminogene factoren en behoeften te kunnen meten (paragraaf 8.3). Vervolgens wordt ingegaan op diverse reactieve en preventieve interventies die uit de literatuur en de praktijk naar voren komen en die aansluiten op een of meer criminogene behoeften uit de *What Works* benadering of bijdragen aan het proces van stoppen met criminaliteit volgens de *desistance* benadering. Achtereenvolgens betreffen dit cognitieve en sociale problemen en mogelijkheden (paragraaf 8.4), het ombuigen van pro-criminele attitudes (paragraaf 8.5), het vergroten van IT-vaardigheden en carrièreperspectieven (paragraaf 8.6), en tot slot de specifieke Hack_Right interventie (paragraaf 8.7).

8.1. *What Works*

De *What Works* literatuur heeft een belangrijke rol gespeeld in de ontwikkeling van effectieve interventies gericht op het terugdringen van recidive bij daders van traditionele criminaliteit (Andrews, Bonta, & Wormith, 2006; Lipsey & Cullen, 2007). Deze op de *Psychology of Criminal Conduct* gebaseerde benadering (Andrews et al., 1990) heeft een aantal principes geformuleerd die van belang zijn bij het tot stand komen van effectieve interventies voor wat betreft recidivevermindering. De empirische literatuur waarin deze benadering een rol speelt, laat op een overtuigende wijze zien dat uitsluitend punitieve interventies, dus straffen zonder specifieke op gedragsverandering en resocialisatie gerichte programma's, voor de individuele dader geen of zelfs een recidiveverhogend effect hebben (Lipsey & Cullen, 2007). Het afschrikwekkende effect dat van deze straffen uit zou moeten gaan, weegt dus kennelijk niet op tegen de schade (door o.a. labeling, verlies van sociale bindingen en toename in criminele vaardigheden en netwerken) die door detentie of een andere vrijheidsbeperkende maatregel wordt veroorzaakt. In plaats van afschrikking ligt bij de *What Works* benadering daarom de nadruk op het wegnemen van criminogene factoren en actief aanzetten tot pro-sociaal gedrag.

De *What Works* literatuur benoemt specifieke principes, tezamen ook wel het RNR-model genoemd, die van belang zijn voor interventies om effectief te kunnen zijn, oftewel aangrijpingspunten bieden voor gedragsverandering (*hook for change principe*). Deze betreffen zowel de inhoud van de interventies als de wijze van uitvoering.

In de eerste plaats speelt het *risicobeginsel* een rol. Inhoudelijk is het volgens de *What Works* benadering van belang dat de intensiteit van de interventie past bij het risico op en de ernst van herhaald delictgedrag. Meer intensieve interventies passen bij hoog-risico daders (Andrews et al., 1990; Lowenkamp et al., 2006) terwijl voor laag-risico daders minder intensieve interventies effectiever zijn.

In de tweede plaats moeten interventies gericht zijn op criminogene behoeften (*needs-beginsel*). Dit houdt in dat omstandigheden of gedrag die direct samenhangen met een verhoogde kans op criminaliteit *en* die potentieel veranderbaar (dynamisch) zijn de focus van de interventie moeten zijn (Andrews et al., 1990). In dit kader worden zeven criminogene behoeften onderscheiden als het gaat om *traditionele* criminaliteit, namelijk: 1) antisociale persoonlijkheidspatronen (bijv. impulsief, avontuurlijk en plezier-zoekend zijn), 2) pro-criminele attitudes (criminaliteit rationaliseren, negatieve houding hebben richting de wet), 3) sociale steun voor criminaliteit (bijvoorbeeld het hebben van delinquente vrienden), 4) verslaving (drugs of alcohol), 5) problemen in familiesfeer (slechte band ouders, gebrek ouderlijk toezicht), 6) problemen op school (slechte prestaties, ontevredenheid), 7) gebrek aan pro-sociale vrijetijdsbesteding. Ook definiëren Bonta en Andrews

(2007) enkele niet-criminogene behoeften (*non-criminogenic needs*), zoals zelfvertrouwen en fysieke en mentale gezondheid, die volgens hen minder veelbelovend zijn als het gaat om effectieve interventies. Als je bijvoorbeeld inzet op het versterken van iemands zelfvertrouwen zonder dat je daarbij ook pro-sociaal gedrag aanleert loop je het risico dat de interventie resulteert in het 'creëren' van een zelfverzekerde crimineel. Op basis van de vorige hoofdstukken hebben we een beeld gekregen van de *needs* die in meer- of mindere mate aanwezig zijn bij cyberdaders. Ons startpunt is dat, waar het gaat om de criminogene behoeften die overeenkomen met die van traditionele daders, bestaande interventies soelaas kunnen bieden. Waar het gaat om criminogene behoeften die afwijkend zijn of juist alleen bij deze dadergroep spelen, kunnen bestaande interventies worden aangepast of nieuwe interventies worden ontwikkeld.

In de derde plaats is het volgens *What Works* en het RNR-model van belang dat de interventie rekening houdt met de mogelijkheden, vaardigheden, leerstijlen en kracht (*strength*) van het individu, ofwel het *responsiviteitsbeginsel*. Daarbij spelen cognitieve en emotionele eigenschappen een rol (Andrews et al., 1990). Veel effectieve interventies gericht op daders van traditionele criminaliteit gaan uit van cognitieve gedrags- of sociale leertherapieën (Andrews et al., 2006), omdat daders (ongeacht het type criminaliteit) in het algemeen responsief blijken te zijn voor deze methoden (dit wordt ook wel *algemene responsiviteit* genoemd). Daarbij is een belangrijke factor voor het tot stand komen van houding- en gedragsverandering de aanwezigheid van motivatie voor de verandering (McMurran & Ward, 2010). Daarnaast is het belangrijk aandacht te hebben voor de individu specifieke responsiviteit die sterk tussen daders kan verschillen (*specifieke responsiviteit)*. Zo kunnen daders verschillende leerstijlen of intelligentie hebben of andere motivaties voor het delictgedrag. Het is belangrijk dat de interventie ook aansluit bij die specifieke responsiviteit. Specifieke responsiviteit kan worden vergroot door o.a. bewustwording en het stellen van doelen die voor de dader van belang zijn. In dit onderzoek ligt de nadruk vooral op de vraag hoe interventies kunnen inspelen op de behoeften en responsiviteit van cyberdaders.

8.2. *Desistance* benadering

Op de *What Works* benadering is veel kritiek gekomen vanuit de *desistance* literatuur. Door sterk de nadruk te leggen op de 'behandeling' van criminogene factoren en het voorkomen van recidive zou door deze benadering te weinig rekening worden gehouden met de dynamiek die hoort bij het *desistance* proces. Daarin stellen mensen eigen doelen en vindt een proces van vallen en opstaan plaats waarin zij leren hoe zij die doelen met niet-criminele middelen kunnen bereiken (Hampson, 2018; McNeill, Farrall, Ligtowler & Maruna, 2012). Het ontwikkelen van een nieuwe, pro-sociale identiteit is daarbij essentieel. Belangrijk daarbij zijn hoop op verandering en zicht op een toekomst na het stoppen met criminaliteit. Zoals geformuleerd door McNeill, Anderson, Colvin, Overy, Sparks en Tett (2011, p. 8) is het belangrijk dat mensen *'desist into something'*, waarbij het belang van niet-crimineel sociaal kapitaal wordt benadrukt. Dit proces zou met interventies ondersteund kunnen worden waarbij positieve rolmodellen, kansen, en positieve bekrachtiging van mogelijkheden (*strength-based* benadering) belangrijke elementen zijn (McNeill et al., 2012).

De empirische evidentie voor de effectiviteit van op deze benadering gebaseerde interventies is nog beperkt. Dit komt deels doordat de benadering nog relatief jong is en de uitwerking ervan in specifieke interventies nog niet wijdverspreid. De aard van de interventies, die multidimensionaler en langduriger zijn en niet direct gericht op recidivebeperking maakt het isoleren van effecten van de specifieke interventie ook lastig. Daardoor zijn er nog weinig evaluatiestudies van dergelijke *strength-based* interventies.

Desalniettemin vormt het *desistance* perspectief een waardevolle aanvulling op de wijze waarop naar interventies en de daarin werkzame elementen kan worden gekeken. Waar *What Works* zich vooral richt op het veranderen van criminogene behoeften, richt de *desistance* benadering zich op de vraag hoe middels interventies ondersteuning geboden kan worden aan verschillende processen die met *desistance* gepaard gaan (o.a. ontwikkelen pro-sociale identiteit, zelfbeeld en relaties). Waar *What Works* rekening houdt met de responsiviteit van individuen – waaronder mogelijkheden, vaardigheden, leerstijlen, kracht en motivatie – door de interventie daarop aan te passen, vormen bij de *desistance* benadering deze persoonlijke aspecten het uitgangspunt. Daarom wordt in dit kader van een *strength-based* benadering gesproken.

8.3. Het juiste instrumentarium

Om tot de keuze voor een geschikte interventie te komen, dienen volgens de *What Works* benadering zowel criminogene factoren en protectieve factoren als de responsiviteit in kaart te worden gebracht. Uit de expertinterviews blijkt dat hier echter nog weinig inzicht in bestaat, terwijl de experts er wel van overtuigd zijn dat die kennis hard nodig is om tot gerichte interventies te kunnen overgaan. Het volgende citaat maakt duidelijk dat experts zich hardop afvragen welke criminogene behoeften een rol spelen: *"*Is dat nou sociaaleconomische achtergrond? Is dat nou verveling? Is dat onzekerheid? Wordt diegene misschien gepest?" (Expertinterview 5, Advocaat).

Bijgevolg zijn de ideeën die er onder de experts bestaan over aanwezige criminogene behoeften divers. Om een goed beeld te krijgen van de criminogene factoren bij een specifieke dader worden reclasseringsadviezen, gedragsrapportages en, voor minderjarigen, rapportages van de Raad voor de Kinderbescherming (RvdK) genoemd als de geschikte bronnen om hier zicht op te krijgen. Het blijkt echter af te hangen van het type zaak of er zulke adviezen worden aangevraagd door het OM of de rechter. Een van de geïnterviewde advocaten heeft nagenoeg geen ervaringen met reclasseringsadviezen in cybercriminaliteit zaken, zowel in ruime als enge zin, en geeft ook aan deze zelf nooit op te vragen. Volgens een geïnterviewde rechter komen reclasseringsrapportages geregeld voor in cyberzaken, maar gedragsrapportages niet. Hij zegt zelf persoonlijkheidsstoornissen niet met daders van cybercriminaliteit (in enge zin) te associëren. Om die reden horen gedragsrapportages wat hem betreft niet thuis in dit domein, evenmin wordt er volgens hem door de verdediging op aangestuurd.

Uit de focusgroep met reclasseringswerkers komt echter naar voren dat zij menen dat er wel degelijk sprake kan zijn van psychische problematiek, maar dat dit nu niet wordt gediagnosticeerd. Zij bevestigen het beeld van de rechter dat opvallend weinig psychiatrische rapporten worden opgemaakt voorafgaand aan een strafzaak. Dit verklaren zij deels door het feit dat verdachten simpelweg weigeren mee te werken aan een onderzoek door het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP). Medewerkers van de RvdK laten weten dat zij in hun risicotaxatie altijd de criminogene factoren in kaart brengen met behulp van het Landelijk Instrumentarium Jeugd (LIJ). Hierin worden tien leefdomeinen beschreven om uiteindelijk tot een dynamisch profiel van criminogene- en protectieve factoren te komen waarop geïntervenieerd kan worden.

De mate waarin er zicht komt op achterliggende criminogene factoren hangt, behalve van het beschikbare instrumentarium, af van de samenwerking tussen allerlei bij het strafproces betrokken instanties. Medewerkers van de RvdK laten weten vooralsnog geen zicht te hebben op hoe vaak zij in beeld komen en worden ingeschakeld binnen het totaal aan cyberzaken. In principe worden zij

ingeschakeld als een jeugdige op ZSM komt; een aanpak die volgens het OM staat voor zorgvuldig, snel en op maat met betrekking tot het afdoeningstraject. Op een ZSM-overleg wordt vervolgens bekeken wat qua 'routering' het beste zou zijn voor een jeugdige, waarbij de RvdK onderzoek zal doen. Als een zaak in handen is bij een jeugdofficier zal deze, volgens de RvdK-medewerkers, makkelijk de route naar ZSM bewandelen. Maar als de zaak in handen is bij een cyberofficier, komt de zaak niet altijd op ZSM terecht en wordt niet altijd overlegd om tot een routeringsbesluit (waar moet deze jeugdige heen, wat gaan we ermee doen, enzovoorts) te komen. Cyberzaken vallen volgens de RvdK medewerkers vaak in de categorie midden tot zwaar, terwijl zij alleen standaard onderzoek doen in zware zaken. Vaker onderzoek doen zou volgens de RvdK-medewerkers wenselijk zijn, omdat dan meer zicht ontstaat op de achterliggende problematiek. Eenzelfde geluid laten reclasseringswerkers horen. Volgens hen zou de reclassering meer om advies kunnen worden gevraagd in strafzaken:

> Het gebeurt te vaak dat de politie iemand pakt en dat ze die dan heenzenden met een dagvaarding. Terwijl er zoveel problemen spelen. […] Ik snap het, die jongen heeft geen strafblad, heeft keurig geleefd, maar dan ga je wel helemaal voorbij aan het hele traject van wat er nodig is bij deze jongen zodat hij niet weer de fout in gaat. (Focusgroep 1, Reclassering)

Volgens een andere reclasseringswerker komen de zaken vaak niet bij de reclassering terecht omdat de verdachten aan de ene kant te jong (minderjarig) zijn en aan de andere kant de zaken te zwaar, waarbij ze echt worden afgestraft. Dit wordt als een gemiste kans beschouwd. Door actief contact te zoeken met politie en OM willen zij deze samenwerking verbeteren:

> Het is wel jammer, want hoe meer zaken we krijgen, hoe meer we leren. Daarom zijn we nu bezig om bij politiebureaus langs te gaan en meer in contact te komen met officieren van 'hé, welke zaken komen er binnen?'. Dan kunnen wij ook zeggen 'dit zijn typische zaken voor ons'. Het OM weet ook niet wat wij met deze zaken wel zouden kunnen (Focusgroep 1, Reclassering).

Volgens een van de reclasseringswerkers zou het goed zijn verdachten niet direct weg te sturen met een dagvaarding maar voor te geleiden en te schorsen onder voorwaarden, namelijk de voorwaarde dat wordt meegewerkt aan een reclasseringsadvies of reclasseringstoezicht. Een OM-medewerker bevestigt het beeld dat de samenwerking tussen instanties, waaronder die van het OM met de RvdK, momenteel nog zeer versnipperd is.

Al met al komt uit de praktijk het beeld naar voren dat nog (te) weinig gebruik wordt gemaakt van de bestaande risicotaxatie-instrumenten in geval de reclassering of, in geval van minderjarigen, de RvdK niet wordt ingeschakeld in strafzaken waarbij mogelijk wel sprake is van problematiek op verschillende vlakken. Om hier meer zicht op te krijgen, zou meer van deze deskundigheid gebruik kunnen worden gemaakt. Bovendien is, zoals blijkt uit de voorgaande hoofdstukken, de diversiteit onder de daders groot, zodat een op maat gesneden aanpak op basis van een gerichte risicotaxatie zinvol lijkt. Tevens kan op die manier worden aangesloten bij de *What Works*-beginselen – de criminogene factoren, criminogene behoeften en responsiviteit – die van belang zijn voor het inzetten of ontwikkelen van effectieve interventies. In het nu volgende staan we hier nader bij stil aan de hand van onze onderzoeksbevindingen.

8.4. Cognitieve en sociale problemen en mogelijkheden

8.4.1. Versterken cognitieve en sociale vaardigheden

Een van de criminogene behoeften waarop volgens de *What Works* benadering dient te worden ingezet zijn antisociale persoonlijkheidspatronen. Hierbij kan gedacht worden aan impulsief handelen, spanning/avontuur zoeken, agressiviteit en rusteloosheid of snel geïrriteerd zijn. Bij traditionele daders wordt er doorgaans vanuit gegaan dat cognitieve gedrags- of sociale leertherapieën hiervoor effectief zijn, omdat daders over het algemeen responsief blijken te zijn voor deze methoden. Op basis hiervan kan gesteld worden dat cyberdaders net als traditionele daders baat zouden kunnen hebben bij interventies gericht op het versterken van sociale- en cognitieve vaardigheden zoals een sociale- en cognitieve vaardighedentraining, die bijvoorbeeld kan worden ingezet in het kader van een taakstraf of als bijzondere voorwaarde. Uit de expertinterviews komt vooral naar voren dat cyberdaders baat zouden kunnen hebben bij reguliere interventies die gericht zijn op het vergroten van sociale vaardigheden ingeval er sprake is van een gebrekkig sociaal netwerk of offline leven. Zo stelt een medewerker van de RvdK voor:

> Je zou bijvoorbeeld kunnen werken aan 'hoe maak ik contact'. Bij sommige jongeren is dat al eng. Als je geen contact durft te maken in het offline leven. Dat zou je als leerdoel kunnen stellen binnen de sociale vaardigheidstraining. Hoe spreek ik iemand aan waarvan ik kan denken 'goh, daar zou ik wel een maatje kunnen krijgen'. Wat ga je dan doen? Ga eens een leuk uitje verzinnen en hoe ga je dat dan brengen? (Expertinterview 6, Raad voor de Kinderbescherming).

De vraag hierbij is of reguliere interventies voldoende rekening houden met het online domein. Zoals uit hoofdstuk 3 en 6 naar voren kwam, kan een cyberdader, anders dan een traditionele dader, compleet van de buitenwereld afgezonderd zijn of een volledige online identiteit hebben, waardoor sprake kan zijn van sociaal isolement of een verstoord dag- en nachtritme. Als dit het geval is zouden interventies zich specifiek kunnen richten op het verbeteren van de balans tussen het online en offline bestaan. Een beleidsmedewerker van Jeugdzorg Nederland benoemt in dit kader dat een interventie is ontwikkeld waarmee jongeren 24 uur offline gaan. Een van de doelen van deze interventie is het reguleren van internetgebruik, door jongeren andere (offline) dingen te laten doen, zoals een potje voetbal op straat.

Daarnaast is de vraag of reguliere interventies gericht op het versterken van sociale en cognitieve vaardigheden wel voldoende rekening houden met de responsiviteit van cyberdaders. Zoals in hoofdstuk 3 duidelijk werd benoemen experts benoemen bijvoorbeeld dat mogelijk sprake is van autisme, dat cyberdaders meer introvert zijn en lastiger contact maken. Reclasseringswerkers laten tijdens de focusgroep weten dat zij behoefte hebben aan meer interventies op maat, waarbij specifiek rekening kan worden gehouden met mogelijkheden, leerstijlen en cognitieve en emotionele eigenschappen van cyberdaders. In geval van autisme zou bijvoorbeeld de cursus Cognitieve Vaardigheden (CoVa) ook individueel in plaats van in groepsverband kunnen worden gevolgd.

8.4.2 Sociale en psychische problematiek

Naast een gebrek aan cognitieve en sociale vaardigheden kan er, net als bij traditionele daders, sociale of psychische problematiek op de achtergrond of voorgrond spelen die van invloed is op het delictgedrag zoals psychologische, relationele of financiële problemen. Bij dergelijke problematiek zouden bestaande interventies kunnen volstaan. Volgens een reclasseringswerker kan er van alles

worden opgelegd in het kader van bijzondere voorwaarden: van psychische behandeling tot omgaan met verlies of emoties. Ook voor sociaal isolement en eenzaamheid, wat meerdere experts regelmatig terug zien komen bij cyberdaders, zijn interventies voorhanden, bijvoorbeeld doordat iemand vrijwilligerswerk moet gaan doen bij een wijkcentrum. Echter, zoals in de voorgaande paragraaf aan bod kwam, is er in de praktijk nog onvoldoende zicht op de problematiek die mogelijk speelt op verschillende leefgebieden en op persoonlijke factoren die een rol spelen, zoals identiteit, impulsiviteit en zelfcontrole. Hierbij is volgens experts nog onvoldoende duidelijk of het reguliere interventie-arsenaal dat hiervoor oplossingen kan bieden toereikend is.

In het bijzonder de advocaten, die met cyberdaders (of -verdachten) gedurende het hele strafproces contact hebben, laten zich positief uitlaten over de mogelijkheden die de reclassering op dit vlak te bieden heeft. Vooral voor jonge cyberdaders zou de reclassering *ad hoc* oplossingen op maat kunnen bieden die deze doelgroep nodig heeft:

> Als je gewoon naar een zaak kijkt, niet alleen naar wat iemand heeft gedaan en wat de schade is, maar ook van: hoe komt het nou dat iemand een misdrijf heeft gepleegd? Hoe komt dat? En dan bekijken waar dat probleem vandaan komt. […] Met de reclassering heb ik betere ervaring. Zeker bij mensen die bijvoorbeeld dakloos zijn en schuldenproblematiek hebben. Daar zitten echt goede mensen die ook ruimte krijgen om dat op te lossen. En soms is de oplossing ook gewoon heel simpel. (Expertinterview 5, Advocaat)

Deze expert meent dus dat er meer gekeken moet worden naar (reguliere) achterliggende problematiek, waar reeds oplossingen voor bestaan. Dit blijkt in de praktijk echter te weinig te gebeuren, omdat binnen bepaalde leefgebieden weliswaar problemen kunnen spelen, maar deze niet altijd als criminogene factoren uit de risicotaxatie naar voren kwamen. Volgens een reclasseringswerker kan het van belang zijn aan criminogene behoeften te werken, ook al worden problemen op het gebied van bijvoorbeeld opleiding of werk niet direct als delict-gerelateerde criminogene behoeften beschouwd. Dit zou volgens een andere expert ook gezien kunnen worden als het versterken van protectieve factoren.

Zoals blijkt uit hoofdstuk 3 zijn de achtergrondkenmerken van cyberdaders wat betreft intelligentie- en opleidingsniveau of gezinsproblematiek wellicht over het algemeen niet als problematisch te bestempelen, toch kan het zinvol zijn hierop in te zetten om pro-sociale bindingen en motivatie in het proces van *desistance* te bevorderen. Het creëren van 'succeservaringen', zoals deze reclasseringswerker dit noemt, bijvoorbeeld op de leefgebieden opleiding en werk, sluit aan op de *strength-based* benadering die centraal staat in de *desistance* theorie, waarbij werken aan identiteit en sociale bindingen het proces van stoppen met criminaliteit zou ondersteunen. Dit wordt door andere reclasseringswerkers in de focusgroep erkend, die aanvullen dat *intrinsieke motivatie* of teveel op het spel hebben staan (wat volgens de sociale bindingen-theorie *stake in corformity* wordt genoemd) ervoor zorgt dat iemand stopt met het plegen van criminaliteit.

Tot slot beschouwt een van de geïnterviewde advocaten de bijdrage die de reclassering kan leveren als positief omdat vooral de *eenzaamheid* die speelt bij meerderjarige verdachten hen vaak aan lijkt te zetten zich dieper in de virtuele wereld in te graven. Deze advocaat begrijpt van cliënten dat zij het fijn vinden om iemand naast zich te hebben staan, iemand om op terug te vallen en eens kritisch bevraagd te worden over bepaalde keuzes of contacten die ze hebben of juist niet hebben, terwijl ze zelf nooit een stap zouden zetten om hulp te zoeken. De meeste cliënten die intensief contact hebben gehad met een toezichthouder ervaren dat volgens deze advocaat als prettig. Dit zou

erop kunnen wijzen dat, misschien meer dan bij traditionele daders, het persoonlijke, sociale contact met een hulpverlener, waarmee hun sociaal isolement wordt doorbroken, een behoefte is waarop ingezet kan worden bij cyberdaders. Deze bevinding is lastig te staven op basis van onze daderinterviews, wat vooral ook te maken heeft met de samenstelling van de daderpopulatie. Eenzaamheid en sociaal geïsoleerd zijn is maar in beperkte mate gerapporteerd. Over het contact met de toezichthouder werd verschillend gedacht. Over het algemeen werd het vooral als een verplichting gezien.

8.5. Het ombuigen van pro-criminele attitudes

8.5.1. Bewustwording van strafbaarheid, schade en slachtoffer

Zoals uit hoofdstuk 6 naar voren kwam, is een deel van de (voornamelijk jonge) daders zich niet of nauwelijks bewust van de strafbaarheid van cybercriminaliteit. Verondersteld wordt, ook door de experts, dat hun delictgedrag deels voortkomt uit het feit dat de daders jong zijn en de gevolgen van hun gedrag nog niet helemaal kunnen overzien. Bewustwording ten aanzien van wat strafbaar is wordt dan ook genoemd als mogelijke (criminogene) behoefte waaraan kan worden gewerkt. Voorlichting op school zou hierbij mogelijk een goede optie zijn, zoals ook besproken in het hoofdstuk 7. Volgens de *What Works* benadering dient de interventie niet enkel gericht te zijn op afschrikking, maar dient specifiek gewerkt te worden aan het ombuigen van pro-criminele attitudes, waaronder het neutraliseren van crimineel gedrag of het hebben van een negatieve houding ten aanzien van de regels.

In dit kader wordt door enkele experts bijvoorbeeld de optie van zogenaamde *serious gaming* (Akhgar & Yates, 2011) genoemd, waarbij jongeren op een spelende manier goede en slechte manieren van hacken leren en ze tegelijkertijd aan het denken worden gezet hierover. Zo legt een expert uit hoe dergelijk spel in zijn werk gaat:

> Dan moeten ze een hacker pakken, en alles wat verboden is, mogen ze dan gebruiken in die game, en als het dan gelukt is kunnen ze de slechte hacker pakken. Maar aan het einde wordt wel gezegd van: 'ja, je hebt die slechte hacker gepakt maar je hebt vaak de wet overtreden, dus voor ethiek krijg je 0 punten. (Expertinterview 3, Journalist/schrijver).

Waar het bij sommige daders schort aan kennis over de strafbaarheid, geldt voor een relatief groter deel van de daders dat de perceptie van schade vrij gering is. Enerzijds is er weinig besef van wat precies de schade is die ze veroorzaakt hebben en anderzijds bestaat de tendens om de gepleegde feiten en schade te bagatelliseren. Hier kunnen net als bij traditionele criminaliteit verschillende oorzaken aan ten grondslag liggen, waaronder een gebrekkige gewetensontwikkeling of een mogelijke autismespectrumstoornis. Een reclasseringswerker noemt het voorbeeld van een cliënt die, waarschijnlijk vanwege autisme, zich niet kon inleven in hoe vervelend het was dat slachtoffers niet konden pinnen, omdat het in zijn ogen volstrekt onlogisch was dat mensen niet twee verschillende banken hebben. Hiertoe kunnen dan reguliere interventies gericht op moreel redeneren en gewetensontwikkeling worden toegepast.

Een medewerker van de RvdK noemt dat bijvoorbeeld via een soort 'keuzeboom' inzichtelijk kan worden gemaakt wie de personen zijn die ze geraakt hebben door het plegen van het delict – het slachtoffer, zichzelf en hun naaste omgeving – waarmee ze een stap verder kunnen komen in hun inzicht in wat ze hebben veroorzaakt. Ook in de Tools4U-interventie voor jongeren, die vaak in het kader van een leerstraf wordt opgelegd, wordt ingespeeld op de keuzes, de kosten-batenafweging die

daders online maken, waarbij de rol van anonimiteit ook duidelijk naar voren komt (wat immers de veronderstelde kosten verlaagd).

Dit sluit aan bij de *What Works* benadering, die binnen de criminogene behoefte 'pro-criminele attitudes' het ombuigen van rationalisaties of neutralisaties onderschrijft. De interventie zou zich dan tevens kunnen richten op het genereren van pro-sociale attitudes en het opbouwen van een pro-sociale identiteit (Bonta & Andrews, 2007).

Experts lijken in beginsel positief over het idee van herstelbemiddeling of *mediation*. Het werken aan herstel vindt op vrijwillige basis plaats, maar kan indien dit in de fase van het vooronderzoek plaatsvindt uiteindelijk invloed hebben op de op te leggen straf.[78] Sommige experts zijn van mening dat het ontmoeten van het slachtoffer een onderdeel van een goed passende (reguliere) interventie is.

> Dan krijgen ze gewoon te horen 'dit is wat je ons hebt aangedaan'. […] Om toch een spiegel voor te houden van dit is wat er aan de andere kant gebeurt. Voor jou is het misschien een dingetje herprogrammeren of aan- en uitzetten, maar voor hen is het hun hele omgeving waar allerlei mensen in zitten. (Expertinterview 2, Onderzoeker)

Ook een officier van justitie acht een confrontatie van de dader met het slachtoffer effectief, omdat daardoor inzicht kan ontstaan in de zin van: "O, er zitten echte mensen achter." Van de experts die positief zijn over een dergelijke interventie, zoals respondenten uit de advocatuur, van het OM, de reclassering of RvdK, heeft echter niemand hier zelf ervaring mee of voorbeelden van bij specifieke cyberdaders. Volgens een reclasseringswerker zou er nog veel meer nagedacht kunnen worden over hoe cyberdaders met slachtoffers in contact gebracht kunnen worden, waar volgens hem de Hack_Right interventie (zie paragraaf 8.7) een voorbeeld van is. Een andere medewerker van het OM wijst hierbij nog op het belang rekening te houden met de wensen van het slachtoffer, die vooral niet onder druk gezet zou moeten worden om hieraan mee te werken.[79]

Wat echter bij het inzetten op de criminogene behoefte 'pro-criminele attitudes' tevens belangrijk is, is dat rekening wordt gehouden met de online context die een rol speelt bij cybercriminaliteit (*responsiviteit*). Zoals in hoofdstuk 5 is uiteengezet, kan de online omgeving bepaalde denkprocessen, zoals het bagatelliseren van de schade, of *online disinhibition*, waarbij remmingen wegvallen door online anonimiteit, verder versterken. Online is schade vaak minder zichtbaar en het slachtoffer is erg 'abstract'. Interventies zouden hier meer rekening mee kunnen houden. De reclassering wijst op een specifieke methode, namelijk 'mentaliseren', wat inleven in een ander inhoudt. Een interventie die specifiek gebruikmaakt van mentaliseren zou volgens hen (momenteel) niet (meer) bestaan, maar zou wel goed aansluiten bij de responsiviteit van cyberdaders, waar het gaat om het kunnen inleven en inzicht verkrijgen in de gevolgen van hun *online* gedrag. Teruggrijpend naar de bevindingen uit hoofdstuk 5 over de percepties van cyberdaders ten aanzien van schade en slachtoffers, zouden aldus bestaande interventies die eraan bijdragen het slachtoffer minder abstract te maken nog onvoldoende worden ingezet. Ook zouden specifieke interventies, waar

[78] Volgens artikel 51h lid 1 Wetboek van Strafrecht bevordert het openbaar ministerie dat de politie in een zo vroeg mogelijk stadium het slachtoffer en de verdachte mededeling doet van de mogelijkheden tot herstelrechtvoorzieningen waaronder bemiddeling. Volgens lid 2 van dit artikel houdt de rechter, indien een bemiddeling tussen het slachtoffer en de verdachte tot een overeenkomst heeft geleid, bij het opleggen van een straf of maatregel daarmee rekening.

[79] Volgens artikel 51h Wetboek van Strafrecht dient het openbaar ministerie zich eerst ervan te vergewissen dat dader-slachtofferbemiddeling de instemming heeft van het slachtoffer alvorens deze bemiddeling wordt bevorderd.

mentalisering volgens de focusgroep met reclasseringswerkers een voorbeeld van is, kunnen worden ontwikkeld die rekening houden met de *online beleving* en daarmee met de *responsiviteit* van cyberdaders.

8.5.2. Online gedrag en ethisch hacken

De *What Works* benadering richt zich op het ombuigen van pro-criminele attitudes, zoals hierboven besproken, naar *pro-sociale attitudes* en het opbouwen van een *pro-sociale identite*it. Hierbij sluiten de *What Works* benadering en *desistance* op elkaar aan, omdat het *desistance*-perspectief juist het ontwikkelen van een nieuwe identiteit als belangrijke voorwaarde van het proces van stoppen met criminaliteit beschouwt. Bij cybercriminaliteit gaat het dan om het ontwikkelen van pro-sociale attitudes ten aanzien van online gedrag, in het bijzonder om het leren van ethisch hacken, of het aangaan van pro-sociale offline relaties waar deze door bijvoorbeeld sociaal isolement ontbreken. Hier kan op verschillende manieren op worden ingezet, zowel in de vorm van reactieve interventies door justitie als in de vorm van alternatieve, preventieve interventies door bijvoorbeeld private partijen.

Restricties of controle op computer- en internetgebruik

Specifieke interventiemaatregelen die door justitie ingezet kunnen worden zijn restricties gericht op het beïnvloeden van computer- ofwel internetgebruik. Deze restricties, gericht op pro-criminele attitudes, komen zowel uit de literatuur als de interviews naar voren als mogelijk effectief. Het verbieden of beperken van het gebruik van de computer en/of het internet zou ingezet kunnen worden tijdens het voorwaardelijk deel van de straf of als voorwaarde bij het schorsen van de voorlopige hechtenis, al dan niet onder toezicht van de reclassering (Smith et al., 2004). Dit kan bijdragen aan verandering van online gedrag, vooral wanneer daar met een hulpverlener over gesproken en op getraind kan worden (Smith et al., 2004).

Reclasseringswerkers laten in de focusgroep weten meer behoefte te hebben aan toezichtmogelijkheden op het online gedrag. Ze missen echter de kennis en tools om online mee te kijken. Ze zouden bijvoorbeeld weleens achter de computer van een cliënt willen gaan zitten en mogelijkheden hebben om zijn computergedrag te onderzoeken. Doordat bij cyberdaders het delictgedrag *online* plaatsvindt is volgens hen een kloof ontstaan tussen wat een huisbezoek vroeger en nu oplevert. De reclasseringswerkers zeggen op dit vlak nog zoekende te zijn en zelf ook beter bekend te willen worden met de online wereld en de online tools. In eerste instantie om daar überhaupt naar te kunnen vragen en in tweede instantie om erachter te komen of iemand in staat is online de juiste keuzes te maken. Zij zouden op basis daarvan bijvoorbeeld willen werken aan het vergroten van inzicht bij hun cliënten of hen een training willen aanbieden, maar dit staat volgens hen nog volledig in de kinderschoenen. Ook bij de politie wordt de behoefte geuit als schorsende voorwaarde op te leggen dat een verdachte moet meewerken aan het inzage geven aan de reclassering in zijn computer- of telefoongebruik. Het is wel de vraag of daar momenteel überhaupt professionals voor zijn die specifieke technische vaardigheden bezitten, anders lachen verdachten je volgens een agent “gewoon keihard uit.”

Ook andere experts pleiten voor een beter volgsysteem van het online gedrag van veroordeelden evenals voor het opleggen van beperkingen in het internetgebruik voor veroordeelden. Bijvoorbeeld door de toegang tot bepaalde sites, fora of (groeps)apps te beperken, terwijl ze nog wel gewoon van het internet gebruik kunnen maken zoals dat iedereen in beginsel ter beschikking staat. Hierbij lijkt zowel aan pro-criminele attitudes als aan het beperken van sociale steun voor criminele gedragingen te worden gewerkt, door contact met pro-criminele vrienden (via bepaalde sociale

media) te verbieden. Handhaafbaarheid lijkt hierbij het grootste obstakel te zijn. Zoals een rechter het uitdrukt: “Je kunt niet een soort computerenkelband hebben die ergens iets ingrijpt als je een bepaalde toets indrukt. Dat dan het systeem zegt: dat mag jij niet” (Expertinterview 11, Raadsheer).

Tot slot zien verschillende experts wel wat in een vorm van ‘offline detentie’ voor cyberdaders die een online identiteit hebben en een gebrek aan (pro-sociale) offline contacten en activiteiten. In tegenstelling tot fysieke detentie wordt iemands bewegingsvrijheid niet beperkt, maar mag de veroordeelde bijvoorbeeld simpelweg niet meer online komen. Het kan dan een soort *cooling down periode* zijn waarbij de dader zijn offline-leven weer wat op de rit kan krijgen en aangemoedigd wordt op zoek te gaan naar offline, pro-sociale vrijetijdsbesteding, zoals sport en hobby’s. Dit kan door bijzondere voorwaarden op te leggen, maar ook door bijvoorbeeld de maatregel van verbeurd verklaren van de inbeslaggenomen apparatuur. In beide gevallen is het effect dat er ruimte ontstaat voor alternatieve, pro-sociale vrijetijdsbesteding. Een politieagent geeft een voorbeeld van een jongen die (sociaal) geïsoleerd en volledig online leefde, waarbij het afnemen van zijn elektronica bij de aanhouding volgens deze agent een soort van ‘reset-knop’ vormde, waarna hij met wat aanmoediging ook een offline leven is gaan opbouwen en bijvoorbeeld een vriendin kreeg, waardoor ook zijn zelfvertrouwen toenam. Een advocaat verwacht eenzelfde soort effect van dergelijke interventies:

> Hup ga eens naar buiten, ga eens kamperen ofzo. Doet wonderen voor mensen. Zeker ook omdat je mensen soms uit hun criminele milieu moet trekken, omdat als je ze weer terugstuurt, ze er weer in vervallen. Ik zou mensen dan als maatregel opleggen: doorbreek de banden met internet. Ga op straat voetballen ofzo, ga een sport doen, weet ik veel, doe iets. Ik denk dat dat heel erg kan helpen bij mensen. (Expertinterview 5, Advocaat)

Diverse experts, zowel advocaten, reclasseringswerkers, politieagenten als een rechter, zijn dus voorstander van het restricties rondom computer- of internetgebruik. Er zijn echter geen voorbeelden dat hier in de praktijk al mee wordt gewerkt, mede vanwege moeilijke handhaafbaarheid. Het is immers niet eenvoudig de bewegingsvrijheid op het internet af te pakken, omdat computers in alle soorten en maten aan te schaffen zijn en men zich overal online toegang kan verschaffen. Sommige experts beschouwen dergelijke interventies ongeacht de leeftijd en dus niet alleen voor minderjarige cyberdaders van nut. Dergelijke restricties kunnen immers zowel zinvol zijn voor het beperken van de tijd die online wordt gespendeerd als gevolg van een sociaal isolement in de fysieke wereld, als de plekken die online worden bezocht (een spel, fora, chats, e.d.) waar contact plaatsvindt met pro-criminele online *peers*. Beide factoren kwamen in hoofdstuk 6 naar voren als van belang bij de initiatie en ontwikkeling van cybercriminaliteit.

Hack-in contest

Naast het beperken van contact en sociale steun van ‘criminele’ vrienden via computer- of internetrestricties, is er een interventie die zich specifiek richt op het ombuigen van dergelijke pro-criminele steun naar het verkrijgen van erkenning voor prestaties op een pro-sociale manier, via pro-sociale contacten, namelijk de *hack-in-contest* (of: hackathon). Deze interventie richt zicht vooral op de uitdaging en erkenning waar (jonge en jongvolwassen) hackers naar op zoek zijn en wordt in de literatuur ook wel *gamification* genoemd. Dit zijn doorgaans door private partijen gesponsorde hackwedstrijden waarbij hackers op verzoek systemen hacken. Voorbeelden hiervan zijn *Bug Bounty* programma’s en *Crime Diggers*. Private bedrijven zijn de uitvoerders van deze interventie (Oosterwijk & Fischer, 2017). Ook kan samengewerkt worden met publieke instanties. Een voorbeeld hiervan is de

hackwedstrijd *Hâck The Hague*, waarbij de gemeente Den Haag en het Haagse cybersecuritybedrijf Cybersprint samenwerkten. Een ander voorbeeld betreft *het Rehab For Hackers* weekend dat door de National Crime Agency (NCA) in het Verenigd Koninkrijk is opgezet (Ward, 2017). Hierbij wordt veel ingezet op voorlichting en preventieve adviezen (Keizer, 2019). Zo worden tijdens het hack-evenement ook de ouders of opvoeders van de jongeren uitgenodigd (Collins, 2018) en daarnaast is een lesplan voor leraren ontwikkeld (Stanton, 2019). Er zijn verschillende redenen om aan te nemen dat dit soort wedstrijden kunnen werken voor cyberdaders voor wie erkenning en uitdaging belangrijke drijfveren zijn.

Ten eerste speelt *hack-in-contest* in op de competitieve subcultuur van de hackerswereld. Wedstrijden maken een integraal onderdeel van de hackerscultuur en zouden daarom beter aansluiten bij de competitieve wereld van (potentiele) cyberdaders (Wible, 2003). Dit aspect wordt ook door enkele experts aangehaald. Het feit dat veel hackers een game-achtergrond hebben zou *hack-in-contest* aantrekkelijk kunnen maken en ook een goed alternatief kunnen maken voor illegaal hacken.

Ten tweede kunnen deze wedstrijden het gevoel van eigenwaarde versterken en ook een gevoel van (pro-sociale) erkenning geven. Erkenning en eigenwaarde gelden als cruciale elementen binnen het proces van *desistance* en komen ook uit de literatuur naar vormen als belangrijke elementen waarop cyberinterventies zich zouden moeten richten (Aiken et al., 2016). Een van de geïnterviewde cyberdaders vermeldt dat hij het fijn vindt dat je, als je vaak *bug bounties* binnenhaalt, echt een record opbouwt van prestaties (‘goede dingen’) (Daderinterview 9).

Ten derde, geldt als werkzaam element van hackwedstrijden, dat door verschillende experts naar voren wordt gebracht, dat deze hackers met (pro-sociale) anderen in contact brengen. Experts zijn positief over hackwedstrijden omdat het belangrijk zou zijn dat hackers elkaar niet alleen online maar ook fysiek ontmoeten. Hierbij gaat het wel om een specifieke doelgroep, namelijk jongeren die ‘op het randje’ zitten en waarop volgens sommige experts ‘alle clichés te plakken zijn’ die over hackers bekend zijn; zij hebben bijvoorbeeld moeite zich te handhaven op school en vooral geldt dat zij solistisch opereren. Een cybersecurityspecialist, die ervaring heeft met hackwedstrijden, zegt in dit kader dat veel hackers de ambitie tonen aan een *hack-in-contest* mee te doen, maar uiteindelijk niet op komen dagen, omdat zij over het algemeen toch wat verlegen zijn. Dit roept de vraag op of de meest sociaal-geïsoleerde cyberdaders, waarvoor pro-sociale bindingen wellicht het hardst nodig zijn, met deze interventie wel worden bereikt.

Ten vierde wordt door enkele experts gesteld dat de financiële vergoeding het ook aantrekkelijk kan maken om hier aan mee te doen, wat ook door een van de geïnterviewde daders die hier ervaring mee hebben, wordt beaamd. Hij geeft aan wel enkele duizenden euro’s te hebben verdiend en dat dit daarom volgens hem een mooi alternatief is voor illegaal hacken.

Tot slot wijzen Oosterwijk en Fischer (2017, p.32) nog op het feit dat *hack-in-contest* effectief kan zijn omdat het, naast positieve bekrachtiging, inzet op het verbeteren of herstellen van de relatie tussen hackers en professionals binnen het handhavings- en securitydomein. Hierdoor worden volgens de auteurs “de minder schadelijke vormen van hacken uitgefilterd en kan de handhaving zijn middelen inzetten op het meer destructieve hacken. Daarbij kunnen de deelnemers aan de *contests* bovendien een bijdrage leveren.”

De *hack-in-contest* lijkt dus niet voor alle type cyberdaders effectief. Enkele experts onderschrijven dit nog met hun mening dat jongeren simpelweg van rebelleren houden en dat een hackwestrijd degenen die kwaad willen of door de spanning ervan aangetrokken worden niet zal weghouden bij illegale activiteiten. Beide hoeven elkaar namelijk niet uit te sluiten. In de literatuur

wordt in dit kader nog gewezen op het feit dat het belangrijk is dat bij *hack-in-contest* voldoende aandacht is voor vormen van hacken die *wel* gecriminaliseerd zijn. Door dit wel te doen kun je sterkere signalen afgeven (Wible, 2003; Oosterwijk & Fischer, 2017), waarmee pro-criminele attitudes mogelijk beïnvloed worden.

Ethisch hacken

Ethisch leren hacken zou een specifiek onderdeel van een interventie gericht op het ombuigen van pro-criminele attitudes kunnen zijn en sluit ook naadloos aan op een *strength-based* benadering. Het versterken van morele overtuigingen, in plaats van afstraffen, kan volgens een Amerikaans onderzoek juist een effectieve methode zijn om recidive van cybercriminaliteit (in ruime) zin te voorkomen. Een vragenlijst onder 183 studenten liet zien dat schaamte en morele overtuigingen sterke voorspellers waren voor een neiging tot illegaal downloaden van software, zodat volgens de onderzoekers beter ingezet kan worden op educatieve interventies dan formele sancties (Siponen, Vance & Willison, 2012). Hoewel dit onderzoek over cybercriminaliteit in ruime zin gaat, zou hetzelfde werkzame mechanisme op het gebied van ethiek een rol kunnen spelen bij effectieve interventies gericht op cybercriminaliteit in enge zin. Vooral jonge hackers (tieners) zouden er baat bij hebben begeleid te worden in het aanleren van een meer volwassen hackersethiek, zodat ze beter bestand zijn tegen de druk die tijdens hun tienerjaren op dit vlak op hen afkomt (Kao, Huang & Wang, 2009).

Naar ethisch hacken (ofwel RD of CVD) is in Nederland nog geen empirisch onderzoek gedaan. In (Amerikaanse) literatuur worden een aantal voordelen genoemd van de Amerikaanse variant hiervan, namelijk *Duty to Report* of *look-and-see* hacken, waarbij niet strafrechtelijk wordt vervolgd indien geen schade wordt aangebracht aan systemen. Dit kan een bijdrage leveren aan het vergroten van internetveiligheid door het melden van kwetsbaarheden (Chatfield & Reddick, 2018). Daarnaast gelden als verwachte effecten: samenwerking en wederzijds vertrouwen tussen hackers en politie en justitie, vergroten van zelfregulatie en (juridische en ethische) normen onder hackers en, tot slot, mogelijkheden tot ontwikkeling van creativiteit en technische vaardigheden (Wible, 2003). Op basis hiervan kan worden verwacht dat ethisch hacken bijdraagt aan het ombuigen van pro-criminele attitudes, pro-sociale bindingen versterkt (ook met professionals) en tot slot prestaties vergroot en uitdaging biedt op een legale wijze.

Om dit effect te sorteren is het volgens verschillende experts erg belangrijk dat er een beloning tegenover het vinden van een kwetsbaarheid staat, want anders werkt het uiterst demotiverend en kan de balans omslaan naar niet-ethisch hacken. Deze beloning hoeft niet per se uit een financiële tegenprestatie te bestaan, ook erkenning van of kennisdeling door ervaren hackers is juist belangrijk. Een expert, oprichter van een cybersecuritybedrijf, vertelt dat hij op de eigen website van zijn bedrijf tientallen malen per dag potentiële hackers voorbij ziet komen. Volgens hem is het allerbelangrijkste met deze jongens in gesprek te gaan, bijvoorbeeld via een chatfunctie op hun website of via LinkedIn: “Jezelf ook kwetsbaar opstellen van: mocht je iets vinden laat het weten we hebben een *bug bounty* programma. Ik zie dat je die net gelezen hebt: meld als er dingen zijn” (Expertinterview 14, Computersecurityexpert).

Engagement is volgens deze expert erg belangrijk, omdat deze jongens uiteindelijk vooral op zoek zijn naar kennis, soms ook naar geld. Volgens hem wordt op het online platform HackerOne bijvoorbeeld aan beide behoeften tegemoet komen. Dit internationale platform kan door verschillende (grote) bedrijven ter wereld worden gebruikt voor hun *vulnerability disclosure* en *bug bounty* programma’s, zo valt op de website te lezen. Volgens de cybersecurityexpert geeft dit jongeren

enerzijds de gelegenheid wat te leren en anderzijds om wat geld te verdienen, wat zou voorkomen dat ze de criminaliteit ingaan.

Rolmodellen

Volgens de *desistance* benadering zijn bij het opbouwen van een nieuwe identiteit rolmodellen van groot belang. Zo zouden rolmodellen uit de hackerswereld een voorbeeldfunctie kunnen vervullen waar het gaat aan het ombuigen van pro-criminele attitudes richting een ethische wijze van hacken. Naar het effect van rolmodellen voor cyberdaders is weinig onderzoek gedaan, echter is in het Verenigd-Koninkrijk in een rapport op basis van (88) gesprekken met aangehouden of potentiële verdachten van cybercriminaliteit (in ruime zin) geconcludeerd dat rolmodellen en mentoren waardevol zijn om jonge cyberdaders weg te houden bij cybercriminaliteit (National Crime Agency, 2017). Ook in Nederland zou de voorbeeldfunctie die de hackersgemeenschap heeft volgens verschillende experts niet moeten worden onderschat. Zo stelt een expert dat er sprake is van een 'zelfreinigend vermogen' van de groep zelf, waarbij hackers elkaar corrigeren. Deze expert gelooft ook in het belang van oudere, *white hat* hackers (dertigers en veertigers) die jonge hackers onder de arm nemen en zich opstellen als een soort coach:

> Ik denk dat voor de context wel belangrijk is dat er een groot vangnet is rondom de hackers. En dat als zij op die tweespan staan, dat er in ieder geval mensen omheen zijn die ze naar de goede kant trekken. (Expertinterview 2, Onderzoeker)

Ook door politie-experts wordt het belang van begeleiding en ondersteuning door een soort van 'technische coach' onderstreept, bij voorkeur iemand uit de hackerswereld waar zij tegenop kunnen kijken. Met 'reguliere' begeleiders zou er een te grote kloof zijn qua belevingswereld, waardoor zij elkaar niet aanvoelen. Daarbij is het van belang dat voldoende tijd geïnvesteerd wordt in de relatie en de coach over een langere tijd met iemand kan meelopen: "En niet denken, met twee gesprekken ben ik er van af, gewoon wat langer doortrekken. Ik denk dat het de tijdsinvestering terugverdient" (Expertinterview 25, Politie).

Volgens de *desistance* benadering is stoppen met criminaliteit een proces dat zich met vallen en opstaan voltrekt. Een pro-sociale identiteit en pro-sociale attitudes ontwikkelen zich meestal niet van de een op de andere dag. Vandaar dat, zoals blijkt uit bovenstaande paragraaf, het belang van rolmodellen of coaches die langere tijd bij dit proces betrokken kunnen zijn, vooral ervaren ethisch hackers of IT-experts waar jongeren tegenop kunnen kijken, door experts als waardevol wordt bestempeld. Zoals in hoofdstuk 4 naar voren kwam is het zichzelf willen *uitdagen* een belangrijke drijfveer voor een relatief groot deel van de cyberdaders. Dit kan enerzijds gerelateerd zijn aan de interesse in IT, een zekere leergierigheid en behoefte aan zelfontwikkeling en *self-challenge* (wat als niet-criminogene behoeften kunnen worden beschouwd). Hiervoor kan verwacht worden dat *hack-in-contest* en ethisch leren hacken succesvolle interventies kunnen zijn. Anderzijds kan de behoefte aan uitdaging ook gerelateerd zijn aan bewijsdrang en de behoefte aan erkenning van pro-criminele (online of offline) leeftijdgenoten of vrienden. Het zoeken naar sociale steun van 'criminele' vrienden kan dan als criminogene behoefte worden beschouwd. In dergelijk geval zouden interventies passend zijn die bewerkstellingen dat de drang om te presteren en erkenning en aanzien te krijgen op een alternatieve, legale manier en via pro-sociale contacten bereikt kan worden, bijvoorbeeld via

rolmodellen of coaches. Een andere manier om sociale steun voor criminaliteit te verminder zou zijn via reactieve interventies in de vorm van restricties of controle op computer- en internetgebruik.

8.6. Vergroten IT-vaardigheden en carrièreperspectieven

Naast het ethisch leren hacken, waaronder via hackwedstrijden, is het volgens de *What Works* benadering van belang dat interventies zich richten op problemen die zich kunnen voordoen ten aanzien van het succesvol zijn op school of op het werk. Eerder kwam aan bod dat cyberdaders niet altijd voldoende uitgedaagd worden op school of ontevreden zijn over het vakkenaanbod wanneer er onvoldoende aandacht is voor lessen op het gebied van IT. Daarnaast kan er door andere oorzaken, zoals autisme of een gebrek aan sociale vaardigheden, sprake zijn van uitval op school of het niet kunnen verkrijgen van werk. Aan deze criminogene behoefte op het vlak van werk/school dient niet alleen volgens de *What Works* benadering, maar ook volgens de *desistance* benadering aandacht te worden besteed. *Desistance* gaat in het bijzonder uit van het ontwikkelen van identiteit en het versterken van persoonlijke vaardigheden, zodat als gevolg hiervan nieuwe rollen in de samenleving aangenomen kunnen worden, zoals die van student of werknemer.

IT-vaardigheden versterken

Verschillende experts zijn, net als het leren om ethisch te hacken, verwachtingsvol over het versterken van de technische vaardigheden van jonge (potentiële) hacker. Daarmee wordt juist de 'kracht' of het talent waarover zij beschikken versterkt en omgebogen door hen te wijzen op de mogelijkheden hier op een verantwoorde, constructieve manier mee om te gaan, bijvoorbeeld bij een IT-bedrijf. Een politieagent verwacht dat vooral jonge cyberdaders er vatbaar voor zijn omgedraaid te worden richting een kant waar ze hun technische vaardigheden op een betere manier kunnen inzetten. Experts zijn er voorstander van dat het bieden van alternatieve mogelijkheden voor het inzetten van hun technische talent, in plaats van klassieke straffen, als primaire reactie zou gelden voor cybercriminaliteit gepleegd door jonge cyberdaders met goede technische vaardigheden en zonder delictgeschiedenis die uit nieuwsgierigheid of baldadigheid een delict pleegden. Een rechter beschouwt het bieden van alternatieven voor het inzetten de technische vaardigheden die iemand bezit als een van de weinige heilzame interventies, omdat afschrikking hooguit in enkele gevallen zou werken. Iemand kan de eenmaal geleerde vaardigheden niet afleren, dus wat je volgens hem hoogstens kunt doen is:

> Iemand laten overstappen van fout naar goed. […] Wat je ziet bij de politie. Dat ze jongeren […] duidelijk maakt van 'goh, kom bij ons werken'. Want dan ga je meewerken aan een veiligere samenwerking en je gaat ons helpen om opsporingsmiddelen effectiever te laten zijn en slechte mensen te vangen. [….] Daar zie je iets dat per saldo veel effectiever is. (Expertinterview 11, Raadsheer).

Ook enkele geïnterviewde daders benadrukken het belang dat hackers een tweede kans krijgen om hun talent op een goede wijze te benutten. In het algemeen delen experts aldus de mening dat positieve aandacht voor iemands capaciteiten, het stimuleren en waarderen, en erop wijzen hoe een jonge hacker op een positieve manier ingezet kan worden cruciaal is voor het proces van stoppen met criminaliteit. Dit wordt onder andere gerelateerd aan de ervaring dat het jonge hackers niet uitmaakt dat grote bedrijven (imago)schade leiden door hun acties of burgers het vertrouwen in overheidsinstellingen verliezen, maar dat juist hún eigen imago zwaar weegt. Het gaat er vooral om

dat zíj iets hebben gevonden, zodat niet zozeer inzicht in de schade zal helpen hen aan de goede kant te krijgen als wel het geven van waardering: "*Dankjewel, je helpt ons nu om onze veiligheid die is super belangrijk, en jij hebt nu onze veiligheid nu naar een hoge niveau weten te tillen. En super, daar zijn we jou heel dankbaar voor*." (Expertinterview 4, Onderzoeker).

Volgens een ex-hacker dienen alle uren die een jonge cyberdader graag in de techniek wil steken benut te worden. Pas als een jongere niet gemotiveerd is mee te werken of steeds in herhaling valt, zou naar punitieve interventies moeten worden gegrepen, zo is de algemene indruk van de experts:

> Kijk wat je in eerste instantie wilt doen is natuurlijk jongeren belonen en stimuleren om hun energie en creativiteit op een goede manier aan te wenden. Dus daar zullen toch de meeste alternatieve benaderingen ongeveer op neerkomen. Hoe kun je die kennis en vaardigheden die je als samenleving eigenlijk hard nodig hebt zo kanaliseren dat je er ook wat aan hebt? […] Hoe kun je nou dat soort mensen ook een plek geven waar je er wat aan hebt? (Expertinterview 17, Onderzoeker).

Carrièreperspectief bieden

Vooral voor de doelgroep van hackers die *jong* zijn op het moment dat ze met justitie in aanraking komen wordt het bieden van carrièrekansen door experts als cruciaal beschouwd. Deze doelgroep heeft er baat bij op een jonge leeftijd bereikt te worden en in de praktijk te zien, bijvoorbeeld door een leerwerkplek bij een ICT-bedrijf, dat iemand met zijn vaardigheden ook goede dingen kan gaan doen. Volgens een advocaat zijn er diverse werkzame mechanismen aanwezig in het bieden van carrièrekansen aan hackers. Zij kunnen hun creativiteit kwijt, kunnen met eigen ogen zien wat cybercriminaliteit kan aanrichten en krijgen erkenning of een beloning voor hun vaardigheden. Dit zou vooral van belang zijn voor cyberdaders met goede technische vaardigheden, die echt interesse hebben in de techniek. Een politieagent zegt: "Ik denk dat sommige securitybedrijven wel staan te springen om jongens die niet kunnen weerstaan om te hacken, maar dan voor hun" (Expertinterview 25, Politie). Juist vanwege het verwachte effect van zowel creativiteit ontwikkelen en erkenning krijgen als bewust worden van schade van cybercriminaliteit vinden sommige experts het bij uitstek een idee om jonge hackers in te zetten voor of aan te nemen bij politie of justitie. Met name in een kleinschalig team, zoals een cyberteam van de politie, zouden deze jongeren erkenning krijgen voor als ze iets goed hebben gedaan of iets hebben gevonden; dit zouden zij niet krijgen bij een groot bedrijf waar zij een radartje in de molen zijn, aldus een advocaat.

Hierbij speelt nog wel de vraag over welke negatieve impact het hebben van een strafblad heeft op de baankansen van cyberdaders. Zoals eerder bleek, hangt het af van het type bedrijf of organisatie of daarvoor wel of geen screening moet plaatsvinden. Hetzelfde geldt voor het niet hebben van een diploma, waarbij het ook per bedrijf zou verschillen of ze een hacker zonder diploma wel of niet willen aannemen.

In het algemeen geldt, hoe eerder jongeren bereikt worden door hen carrièreperspectieven voor te spiegelen die zij, met hun vaardigheden, in het verschiet hebben liggen, hoe eerder zij gemotiveerd kunnen worden die weg in te slaan, in plaats van het verkeerde pad op te gaan. Dit draagt niet alleen bij aan het ombuigen van pro-criminele attitudes maar ook aan het bieden van alternatieve, pro-sociale (vrije)tijdsbesteding, wat de gelegenheid en motivatie tot het betrokken raken bij criminele activiteiten beperkt vanwege het creëren van een zogeheten *stake in conformity*. Een cybersecurityexpert verklaart dit als volgt:

> Ik denk dat je als overheid een rol kunt nemen, dat je de jongens helpt om een bedrijfje te starten. Op het moment dat je het niet kanaliseert, kunnen ze hele gekke dingen doen. Als iemand maar gewoon werk heeft en inkomen heeft, dan zal iemand minder geneigd zijn het slechte pad op gaan. Ook de jongens willen wel een keer een vriendinnetje, een huis en een kindje. Die komen ook in een normaal stramien terecht. Structuur helpt voor heel veel mensen. […] Geef die jongens wat te doen in een gestructureerde omgeving, waar ze erkend worden. (Expertinterview 21, cybersecurityexpert)

Een rol voor de samenleving

Diverse experts benadrukken, zoals ook uit bovenstaande quote blijkt, dat de samenleving hierbij een belangrijke rol te vervullen heeft, juist omdat jonge personen met goede IT-vaardigheden 'zo hard nodig zijn', nu en in de toekomst mogelijk nog meer. Zij moeten begeleid worden naar een constructieve, *white hat* rol in samenleving. Verschillende expert zien veel mogelijkheden voor allerlei maatschappelijke partners, zowel overheid als bedrijven, om hierin een rol te spelen: van politie, gemeenten, ICT-bedrijven, het Midden en Klein Bedrijf, scholen en de Kamer van Koophandel tot ziekenhuizen. Zij kunnen jongeren via *bug bounty* programma's hun IT-vaardigheden laten inzetten om de betreffende organisaties te helpen bij het vergroten van hun cybersecurity. In het bijzonder zouden gemeenten in samenwerking met een van de genoemde bedrijven plannen kunnen maken om voor jongeren die 'uit de bocht gevlogen zijn' een alternatief traject, dat wil zeggen buiten het strafrecht om, aan te bieden. Gemeenten kunnen namelijk *maatwerk* bieden en een rol hebben in het corrigerend optreden door middel van een soort van 'waarschuwende straf'; wat niet alleen een vraagstuk van justitie zou behoren te zijn.

> Maatwerk is denk ik het sleutelwoord. Laten zien dat ze hun talenten op de goede manier kunnen gebruiken. Er is niks mis mee om te erkennen dat mensen wat kunnen, zet ze maar in hun kracht, prima, alleen begeleidt ze wel een klein beetje. […] Dat hij nu ook ziet: 'Okee, ik kan er gewoon een normale baan in krijgen en kan nog lekker verdienen ook (Expertinterview 25, politie).

Het merendeel van de experts beschouwt dergelijke maatschappelijke projecten als zinvol. Bijvoorbeeld omdat jonge cyberdaders dan bezig worden gehouden en zodoende hun tijd niet kunnen invullen met eigen (criminele) 'projectjes', wat aansluit bij de criminogene behoefte van een pro-sociale vrijetijdsbesteding. Ook zien experts bijvoorbeeld mogelijkheden voor jongeren die beweren dat zij handig zijn in een schoolsysteem hacken, om andere scholen te gaan helpen hun beveiliging beter op orde te krijgen. Of dat bijvoorbeeld een ziekenhuis vooraf afspraken maakt met jonge hackers om hun cybersecurity te laten testen, waarbij deze jongens ook eerlijk geld krijgen voor wat zij doen. Zij kunnen op die manier een waardevolle bijdrage leveren. Verschillende experts zien ook mogelijkheden voor de politie, waar jongeren als vrijwilliger zouden kunnen werken en tegelijkertijd ethisch leren hacken. Een expert noemt in dit kader het voorbeeld van *Teenage Crime Fighters*, een programma waarbij jongeren de politie helpen met bepaalde vraagstukken; wat zowel voor de jongeren als de politie iets kan opleveren. Volgens een politieagent zou de politie hierop moeten inzetten:

> Het kat-en-muisspel vinden ze vaak gaaf, de technologie anders inzetten dan dat deze bedoeld is. Het maakt niet uit aan welke kant je zit, als je maar in het spel zit. Het zijn de omstandigheden die bepalen dat of je dat bij een bedrijf gaat doen of dat je het in de criminele hoek gaat zoeken. (Expertinterview 27, Politie)

Het aannemen van een nieuwe, constructieve rol in de samenleving is volgens de *desistance* benadering erg belangrijk om uiteindelijk het proces van stoppen met criminaliteit succesvol te kunnen doorlopen. Daarmee is mogelijk dat (cyber)daders *desist into something* (McNeill et al., 2011).

Een geïnterviewde cyberdader benadrukt eveneens het belang dat hackers een tweede kans krijgen om hun talent op een goede wijze te benutten en ziet in aansluiting op de experts ook een rol weggelegd voor scholen. In de praktijk komt het echter voor dat jongeren die het schoolsysteem hacken van school worden gestuurd:

> Maar een jonge jongen die iets met de beste intentie aan school meldt, ondanks dat hij even iets verder is gegaan, dan hoor je toch als school die jongen te helpen. Straf hem dan vanuit school of zoiets. Als school vind ik het onverantwoordelijk om zijn kansen op een toekomst moeilijker te maken door hem met justitie in aanraking te laten komen. Ik vind dat je als school verantwoordelijk moet zijn voor de toekomst van je studenten, dat is toch het doel van school, dat je mensen helpt aan een toekomst. […] Ik geloof er echt in dat het beter opgelost moet kunnen worden. (Daderinterview 9)

Experts bevestigen het beeld dat het bieden van interventies waarbij jongeren hun vaardigheden kunnen inzetten en vergroten waardevol zijn vooral zowel de jongeren als de maatschappij. Een expert noemt het voorbeeld van een jongen die is ingezet om les te geven over een IT-gerelateerd onderwerp waar hij bijzonder veel van af wist, terwijl deze jongen van zijn vorige school was afgestuurd omdat hij het schoolsysteem had gehackt. Deze expert noemt het voorbeeld van een andere school die daar juist heel anders mee omging en de betreffende jongen via een *responsible disclosure* contract de mogelijkheid bood de kwetsbaarheden in het schoolsysteem aan te tonen; wat deze jongen meteen zou hebben aangegrepen als zijnde een visitekaartje naar een fantastische baan, aldus deze expert.

Cyberwerkplaatsen

Een voorbeeld van een initiatief waarbij zowel het vergroten van technische vaardigheden, bieden van carrièreperspectief en het versterken van sociale vaardigheden als belangrijke werkzame factoren samenkomen is de cyberwerkplaats*,* een plek waar IT-vaardige jongeren terecht kunnen om bijvoorbeeld workshops te volgen of aan IT-projectjes te werken. In Nederland bestaan twee cyberwerkplaatsen, namelijk Cyberwerkplaats Rotterdam en Hacklab Friesland. Een cyberwerkplaats wordt gerund door vrijwilligers en gesponsord door maatschappelijke partners en bedrijven. Jongeren kunnen daar op vrijwillige basis heen om op een ethische manier te leren hacken en les te krijgen van experts, om daarmee hun vaardigheden te vergroten, met als doel uiteindelijk een stage of werkplek te vinden. Zo is ‘Hack je gek en verdien een werkplek’ een van de motto’s van een cyberwerkplaats. Experts zijn hier enthousiast over. Een cyberwerkplaats is niet bedoeld als officiële justitiële interventie.

> Daar proberen ze juist die groep die een beetje op het randje loopt, ik noem het maar even potentiële drop outs, binnen te krijgen […] er lopen gewoon mentoren rond op de vloer. En

> de mensen die daar zitten en de boel begeleiden hebben ook gewoon een goed netwerk in het bedrijfsleven. De bedoeling is eigenlijk om die groep zo ver te krijgen dat ze hun capaciteiten in positieve zin inzetten waardoor ze – ja, want voor werkgevers is het natuurlijk en hele interessante groep – na bemiddeling tot een baan komen. Zij zorgen ook voor die match tussen bedrijven en die ethische hackers. (Expertinterview 4, Onderzoeker).

Een van de experts noemt het een soort 'sociale digitale werkplaats.' Op een cyberwerkplaats kan maatwerk worden geboden en worden ingezet op allerlei (niet-)criminogene behoeften van jongeren. Een reclasseringswerker noemt het voorbeeld van een jongen die hij begeleidde die van school afging en wilde gaan werken, maar daar niet in slaagde. Deze jongen is toen naar een cyberwerkplaats verwezen, waardoor zijn dag-en-nachtritme weer beter werd, zijn softdrugsgebruik voor een deel is afgenomen, hij over het algemeen rustiger is geworden en beter in zijn vel zit én met een ICT-cursus bezig is. Initiatieven als de cyberwerkplaats kunnen jongeren stimuleren te kiezen voor een carrière waarbij ze hun capaciteiten in positieve zin kunnen gebruiken. Vooral aan kansarme jongeren, die bijvoorbeeld niet meekomen of gestopt zijn met school, biedt een cyberwerkplaats bij uitstek kansen om weer op het juiste pad te komen volgens een expert: "Door ze te leren hacken en van de straat af te halen en een leen-laptop te geven en te zeggen: hier kijk maar hoe ver je daarmee komt" (Expertinterview 14, Cybersecurityexpert).

Daarom acht hij dergelijke initiatieven enorm waardevol, omdat er beginnende hackers door worden afgeleverd die vervolgens bijvoorbeeld bij hem in de securitywereld echt iets kunnen bijdragen en op die manier ook aan de maatschappij.

8.7. De Hack_Right interventie

Een specifiek voor (jonge) cyberdaders ontwikkelde interventie is de Hack_Right interventie. Hierbij wordt aan criminogene behoeften gewerkt, waaronder bewustwording van de schade en het waar mogelijk herstellen daarvan en wordt vooral bijgedragen aan het proces van *desistance* door jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving. De voorloper van Hack_Right betreft de pilot Yoda die in 2017 is opgezet door Halt met het idee om minderjarige cyberdaders als straf mee te laten lopen bij een ICT bedrijf. Hack_Right is hieruit voortgevloeid (Expertinterview 12, Halt medewerker). Hack_Right is tot stand gekomen vanuit een breed samenwerkingsverband tussen strafrechtelijke instanties en particulieren: van politie, OM, Halt, RvdK, Reclassering Nederland en het ministerie van Justitie en Veiligheid tot bedrijven, wetenschappers en ethisch hackers. Volgens de coördinerend beleidsadviseur van het Landelijk Parket wordt hiermee beoogd een oplossing te bieden aan de geconstateerde moeilijkheden bij het bepalen van een passende interventie voor jeugdige daders (12 tot 23 jaar) van hightech cybercriminaliteit. Het gaat namelijk om daders die iets ernstigs op hun kerfstok hebben, maar nog jong zijn en afwijken van traditionele daders (De Bruijne, 2018). Naast leeftijd en technische vaardigheden geldt als voorwaarde dat het moet gaan om een *first offender* die gemotiveerd is en dat het delict niet te ernstig is. Dit laatste aspect levert nog wel wat moeilijkheden op, doordat een hacker volgens de betrokken strategisch adviseur van THTC met een kleine handeling al veel schade kan aanrichten (De Bruijne, 2018). Hack_Right richt zich op recidivevermindering en het behouden van digitaal talent door middel van verschillende modules (herstel, training, alternatief en coaching). De interventie wordt momenteel onder andere opgelegd als voorwaarde bij een voorwaardelijk sepot of als leer- of werkstraf bij Halt, de reclassering of de RvdK. Daarnaast kan Hack_Right worden opgelegd als

bijzondere voorwaarde bij een voorwaardelijke straf of als aanvulling op een reguliere straf.[80] De pilot telt aan het einde van 2019 ongeveer 20 deelnemers, aldus een betrokken expert van THTC.[81]

De geïnterviewde experts zijn positief over de ontwikkeling dat bepaalde daders na het plegen van hun delict, als onderdeel van een justitiële interventie, een leerwerkplek krijgen bij een IT-bedrijf.[82] Tegelijkertijd is sprake van een soort boetedoening, omdat zij iets terugdoen voor de samenleving, liefst daar waar de schade is veroorzaakt, zodat een jongere het slachtoffer vervolgens ook ontmoet, aldus een expert die met Hack_Right-jongeren werkt. Erkennen van schade en slachtofferschap worden als belangrijke werkzame elementen beschouwd, die volgens de *What Works* benadering kunnen bijdragen aan het ombuigen van pro-criminele attitudes. Volgens voornoemde expert werkt dat juist heel goed voor daders die niet sociaal of inlevend zijn. Daarnaast kunnen talentvolle (jonge) daders door middel van een leerwerkplek bij een IT-bedrijf goed tot hun recht komen, wat bijdraagt aan het ontwikkelen van hun identiteit.

> Hack_Right leert waar de grens ligt, daarbinnen wordt jongeren geleerd dat ze hele leuke dingen kunnen doen en dat als ze die vaardigheden leren, ze een gouden toekomst hebben. Zo trek je iemand permanent naar de goede kant toe, wat veel beter is dan iemand op straat vuil te laten prikken (Expertinterview 15, Juridisch medewerker OM).

De meeste experts vinden de Hack_Right interventie passend voor de doelgroep van jonge daders die geen zwaar vergrijp hebben gepleegd en niet eerder met justitie in aanraking zijn geweest, al willen ze ook heel graag weten of deze interventie daadwerkelijk effectief blijkt te zijn. Sommige experts stellen dat deze interventie breder toepasbaar zou moeten worden en bijvoorbeeld niet alleen maar voor *first offenders* moet gelden. Daarnaast zou een dergelijke interventie meerderjarige cyberdaders goed helpen op het rechte pad te komen, beter dan een 'traditionele' straf. Diverse experts zeggen expliciet geen effect te verwachten van het opleggen van een reguliere werkstraf,[83] zoals schoffelen of papierprikken. Met de Hack_Right interventie, die als leer- of werkstraf ingezet kan worden, lijkt beter te kunnen worden aangesloten bij het *responsiviteitsbeginsel*. Er kan bij de uitvoering van de straf namelijk rekening worden houden met de mogelijkheden, vaardigheden en kracht (*strength*) van cyberdaders (*algemene responsiviteit*), die als anders beschouwd worden dan die van daders van traditionele criminaliteit: "Als een jonge hacker voorlichting moet gaan geven bij oudere mensen in het bejaardentehuis van hoe ze veilig moeten Facebooken of met e-mail om moeten gaan, dan vind ik dat persoonlijk veel zinniger" (Expertinterview 8, Reclasseringsmedewerker).

Daarbij is het echter de vraag of voldoende rekening wordt gehouden met de *specifieke responsiviteit*, waarbij onder andere de verschillende leerstijlen en motivaties voor het delictgedrag

---

[80] Er wordt aan gewerkt hier een erkende gedragsinterventie van te maken, zodat dit deel uitmaakt van het officiële justitiële interventiepakket.

[81] https://www.politie.nl/nieuws/2019/oktober/30/11-pilot-twintigtal-bedrijven-helpt-justitie-jonge-hackers-op-het-rechte-pad-te-krijgen.html

[82] Recentelijk hebben twintig bedrijven een intentieverklaring getekend om mee te werken aan de pilot en de jongeren te trainen en te coachen. Dit betreffen niet alleen IT-bedrijven, maar bijvoorbeeld ook organisaties uit de bankensector (https://www.politie.nl/nieuws/2019/oktober/30/11-pilot-twintigtal-bedrijven-helpt-justitie-jonge-hackers-op-het-rechte-pad-te-krijgen.html)

[83] Werkstraffen zijn formeel niet ingericht vanuit de RNR methodiek, het belangrijkste doel is dat cliënten op deze manier iets terugdoen voor de samenleving die zij schade hebben aangedaan (zie: https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/werkstraffen). Werkstraffen zouden echter wel bijdragen aan recidivebeperking doordat cliënten werkritme opdoen en werknemersvaardigheden kunnen leren tijdens de straf (waarmee mogelijk criminogene factoren worden opgeheven). Dit kan een eerste stap zijn naar een reguliere baan. Voor cyberdaders zouden de vaardigheden uit de reguliere werkstraffen minder goed aansluiten bij mogelijke toekomstige banen.

een rol spelen, die volgens de *What Works* benadering sterk tussen daders kunnen verschillen. Een kritisch geluid dat experts ook laten horen is dat hieraan het risico kleeft dat daders er 'te gemakkelijk' vanaf komen. Een expert die Hack_Right daders begeleidt, twijfelt er weleens aan of er daadwerkelijk sprake is van een laag risico bij de daders die deze interventie opgelegd krijgen. De verschillen tussen Hack_Right daders kunnen volgens deze expert bovendien enorm zijn, bijvoorbeeld iemand die een stommigheid heeft begaan en direct spijt heeft van wat hij heeft gedaan, of iemand die echt een hacker is en technisch een stuk verder was en zich mogelijk niets aantrekt van wat een ander daarvan vindt; terwijl beide daders dezelfde straf opgelegd hebben gekregen. Jongeren die echt een criminele neiging vertonen, lijken er met deze interventie heel makkelijk vanaf te komen, aldus experts. Volgens het risico-beginsel van de *What Works* benadering zou de intensiviteit van de interventie zich moeten verhouden tot het risico op en de ernst van herhaald delictgedrag. Dit roept volgens een expert de vraag op hoe binnen Hack_Right moet worden gevarieerd met de intensiviteit of zwaarte van de interventie. De expert noemt het voorbeeld van een dader die in de vorm van een leer- of werkstraf aan de slag 'mag' bij een IT-bedrijf, terwijl deze dader al een baan in de IT heeft en het dus eigenlijk gewoon werk voor hem is; daar zou volgens de expert bijgevolg geen punitief element in zitten. Dit wordt bevestigd door een politie-expert, die ervan uitgaat dat jongeren een leerwerkplek bij een IT-bedrijf zeer interessant vinden, waardoor dit eerder kan worden ervaren als een beloning van crimineel gedrag dan als straf.

Andere experts uiten niet zozeer hun twijfels over *specifieke afschrikking* maar over het beperkte effect ten aanzien van *generale afschrikking* dat een dergelijke interventie mogelijk zal sorteren. Zo zouden binnen de hackersgemeenschap de meningen verdeeld zijn over Hack_Right en zouden sommigen zich afvragen of het wel handig is om iemand die een ethische en juridische grens is overgegaan, een duwtje in de rug te geven. Bovendien zouden dezelfde jongeren die misschien net niet de grens zijn overgegaan net zo hard dat duwtje in de rug kunnen gebruiken. Het kan volgens experts naar de maatschappij in het algemeen een averechts effect hebben, omdat dat het te 'soft' overkomt.

In enkele strafmodaliteiten waarin Hack_Right wordt uitgevoerd, krijgen de daders geen strafblad, maar in de meeste modaliteiten wel. Volgens een beleidsmedewerker van het OM is een belangrijke vraag voor het bepalen binnen welke strafmodaliteit Hack_Right wordt toegepast: "Krijgt iemand hier een strafblad voor of doen we dit anders af?" Het niet krijgen van een stafblad kan de toekomstkansen op de arbeidsmarkt van de deelnemers ten goede komen. Zoals in hoofdstuk 6 is beschreven stellen experts dat er negatieve gevolgen kleven aan het hebben van een strafblad en wordt dit ook beschreven door enkele daders die zelf een strafblad hebben. Deze gedachtegang sluit aan bij een belangrijk principe uit de *desistance* benadering, namelijk het voorkomen of ombuigen van het negatieve label van 'crimineel' dat iemand door justitiecontact krijgt opgeplakt, wat het proces van re-integratie in de samenleving, in het bijzonder op de arbeidsmarkt kan belemmeren. Bij Hack_Right is het voorkomen van een strafblad geen doel op zich, wat ook al blijkt uit het feit dat daders in de meeste modaliteiten wel een strafblad krijgen. De nadruk ligt vooral op het bieden van een alternatief voor illegaal hacken, waar een leerwerkplek bij een IT-bedrijf een belangrijk onderdeel van vormt. De interventie lijkt goed aan te sluiten bij de *desistance* benadering in de zin dat beoogd wordt jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving. Echter, het strafblad kan daarbij nog wel een obstakel zijn.

8.8. Conclusie

In deze afsluitende paragraaf wordt kort stilgestaan bij welke interventies volgens de literatuur en de interviews worden verwacht het meest zinvol te zijn. Uit het literatuuroverzicht blijkt dat er weinig interventies gericht op recidivebeperking voor specifiek cyberdaders voorhanden zijn, met uitzondering van de Hack_Right interventie. Deze interventie sluit aan op de *desistance* benadering door jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving, onder andere door middel van een leerwerkplek bij een IT-bedrijf, coaching door een ervaren hacker (rolmodel) en ethisch leren hacken. Experts zijn erg verwachtingsvol over wat dit voor de doelgroep (jong, *first offender*, geen ernstig delict, schuld bekend en gemotiveerd) kan betekenen. Tegelijkertijd plaatsen sommige experts vraagtekens bij het afschrikwekkende effect; mogelijk genereert een dergelijke interventie onvoldoende generale en wellicht ook onvoldoende specifieke afschrikking.

Hoewel experts over het algemeen enthousiast zijn over de specifieke interventie Hack_Right, kunnen bij cyberdaders ook op allerlei leefgebieden problemen spelen die via 'traditionele' interventies kunnen worden aangepakt. Hierbij valt te denken aan het verbeteren van de relatie met ouders, het aanleren van sociale vaardigheden, het omgaan met verlies, het werken aan schulden of verslaving en het krijgen van werk of het volgen van een opleiding. Om aan te sluiten bij de responsiviteit van cyberdaders zou aan dergelijke aspecten, zoals sociale vaardigheden, een sociaal netwerk of pro-sociale vrijetijdsbesteding, kunnen worden gewerkt door interventies waarmee zij geen of beperkte mogelijkheden hebben voor het voortzetten van hun *online* (pro-criminele) activiteiten en waarmee aan een betere balans tussen hun online en offline bestaan gebouwd kan worden. Dit kan bijvoorbeeld door middel van bijzondere voorwaarden gericht op restricties op computer- of internetgebruik of, zoals voor jongeren ontwikkeld is, een speciale interventie gericht op 24-uur offline zijn. Tegelijkertijd zou gewerkt kunnen worden aan pro-sociale online vrijetijdsbesteding (waaronder ethisch hacken), rekening houdende met het feit dat deze doelgroep juist graag online zijn of haar tijd doorbrengt.

Daarnaast geldt dat eenzaamheid, sociaal isolement, gebrek aan sociale vaardigheden en autisme in de praktijk naar voren komen als specifieke kenmerken van (een deel van de) cyberdaders, waar interventies ofwel rekening mee kunnen houden (responsiviteit) ofwel kunnen proberen dit om te buigen. Er is bij experts momenteel echter nog onvoldoende zicht op welke leefgebieden zich problemen voordoen die gelden als criminogene factoren of waar protectieve factoren versterkt kunnen worden met behulp van bestaande interventies. Een van de redenen hiervoor lijkt te zijn dat deskundigenrapportages, gebaseerd op erkende risicotaxatie-instrumenten van bijvoorbeeld de reclassering, de Raad voor de Kinderbescherming of forensisch psychologen en psychiaters, in strafzaken weinig worden opgevraagd. De kennis lijkt derhalve te blijven steken op het niveau van (de vaak beperkte) persoonlijke ervaringen van experts. Bovendien is, zoals blijkt uit de voorgaande hoofdstukken, de diversiteit onder cyberdaders groot, zodat een op maat gesneden aanpak op basis van een gevalideerde risicotaxatie voor deze type daders zinvol lijkt. Zo wordt door experts aanleiding gezien interventies op het gebied van moreel redeneren en gewetensontwikkeling in te zetten, bijvoorbeeld in de vorm van *serious gaming* (bij minderjarige cyberdaders) of op het gebied van mentaliseren (het inleveren in de ander) te ontwikkelen (voor meerderjarige cyberdaders).

Naast reguliere interventies blijkt, op basis van de literatuur en de interviews, veel te worden verwacht van *strength-based* interventies voor cyberdaders, waaronder het versterken van technische vaardigheden, het aanleren van hackersethiek en het concreet bieden van carrièrekansen. Op die manier krijgen daders de mogelijkheid '*to desist into something*'. Reactieve interventies, gericht op het beïnvloeden van de rationele keuze, zouden teveel afbreuk kunnen doen aan het sociaal kapitaal

(werk of opleiding) waarover daders van cybercriminaliteit, meer dan daders van 'traditionele' criminaliteit, lijken te beschikken.

Een initiatief dat door veel experts als voorbeeld van een alternatieve, *strength-based* interventie wordt aangehaald zijn cyberwerkplaatsen, die zich vooral inzetten voor kansarme jongeren, die bijvoorbeeld van school zijn gestuurd of in een sociaal isolement zitten. Hen worden concrete IT-vaardigheden aangeleerd waardoor zij zowel leren hun vaardigheden op een ethische manier in te zetten als concreet aan hun toekomstmogelijkheden werken. Een andere manier om vaardigheden te vergroten en te leren deze op een goede manier in te zetten zijn hackwedstrijden (*hack-in-contest*). Juist bij het bieden van dergelijke alternatieve trajecten voor jongeren die (eenmalig) over de schreef zijn gegaan zou een expliciete rol zijn weggelegd voor (een samenwerking tussen) lokale overheden en bedrijven, omdat zij maatwerk kunnen bieden. Door middel van het werken aan *strengths* (door het vergroten van IT-vaardigheden en begeleiden naar een werkplek) krijgen niet alleen jongeren perspectief op het 'rechte pad'; ook de samenleving heeft hier baat bij doordat het jonge IT-talent dat hard nodig zou zijn terechtkomt op een plek waar zij er wat aan heeft en mogelijk toekomstig daderschap wordt voorkomen.

Hoofdstuk 9 Conclusie

9.1. Opzet van het onderzoek

Hacken, DDoS-aanvallen, ransomware en andere vormen van cybercriminaliteit in enge zin lijken steeds vaker te worden gepleegd door zowel jeugdigen als volwassenen. Bij deze delicten is er doorgaans sprake van veel schade. Of we hierbij te maken hebben met een wat teruggetrokken minderjarige op een zolderkamertje (het stereotypebeeld), een professionele cybercrimineel of een (traditionele) oplichter is niet altijd duidelijk. Wat er exact toe heeft geleid dat daders, soms al op hele jonge leeftijd, in de cybercriminaliteit verzeild raken, is vaak ook nog een vraag. Is het geld, de kick of ligt het toch complexer? Meer kennis over wie deze daders zijn en waarom zij deze delicten plegen, is van groot belang om tot een gedegen en effectieve aanpak te komen. Belangrijke vragen hierbij zijn: hebben we te maken met andersoortige daders dan traditionele daders, in hoeverre en op welke wijze verschillen cyberdaders onderling van elkaar en wat zijn de implicaties hiervan voor de aanpak van deze dadergroep? Deze vragen zijn samengevat in de volgende centrale probleemstelling:

"In hoeverre bestaan er verschillen qua profiel(en) van cyberdaders en daders van 'traditionele' criminaliteit, en in hoeverre en op welke wijze dienen (eventuele) verschillen gevolgen te hebben voor de aard van interventies voor cyberdaders?"

Het onderzoek richt zicht daarbij specifiek op daders van cybercriminaliteit in enge zin, waarbij ICT zowel het middel als het doelwit van criminaliteit is. Dit gaat om delicten als hacken, het uitvoeren van DDoS-aanvallen, botnets en ransomware. Om de onderzoeksvragen te beantwoorden zijn twee systematische zoekopdrachten in de literatuur uitgevoerd en zijn interviews en focusgroepen gehouden met experts en interviews met daders van cybercriminaliteit in enge zin. De eerste zoekopdracht leverde 99 bronnen op over kenmerken van daders van cybercriminaliteit in enge zin, al dan niet in vergelijking met traditionele daders. De tweede zoekopdracht leverde 25 bronnen op over interventies gericht op cyberdaders in enge zin. In totaal hebben 52 experts in het onderzoek geparticipeerd waaronder vrijwel alle samenwerkingspartners uit de veiligheidsketen (waaronder politie, openbaar ministerie, reclassering Halt, GGZ en jeugdhulp) en daarnaast onderzoekers op het gebied van cybercriminaliteit en experts uit het bedrijfsleven. Tevens zijn 14 daders geïnterviewd, waarvan bij het merendeel hacken het primaire delict vormde. Hoewel dit allemaal meerderjarige daders betrof, zijn bij alle respondenten de ontwikkelingen in hun criminele carrière besproken. Bij een groot deel van de respondenten begon deze al tijdens de adolescentie en bij een aantal werd deze ook al in de adolescentie afgebroken.

9.2. Beperkingen van het onderzoek

Het onderzoek kent een aantal beperkingen. Ten eerste kent de gevonden literatuur beperkingen. Zo is er relatief veel literatuur gevonden over hackers (zij het wel veel verouderde literatuur), maar weinig over daders die betrokken zijn bij andere vormen van cybercriminaliteit in enge zin (DDoS, ransomware). Tevens zijn er weinig (effect)studies gevonden waarin de toepassing van traditionele of cyber-gerelateerde interventies op cyberdaders is onderzocht en is er dus nog weinig systematische kennis van mogelijke zinvolle interventies voor cyberdaders voorhanden. Ten tweede zijn bij de expertinterviews diverse respondenten betrokken die zelf nog maar met enkele cyberdaders ervaring hadden (zie hoofdstuk 2). Daarbij gaat het grotendeels om daders die in beeld zijn gekomen bij politie en justitie (en daardoor bij andere samenwerkingspartners in de veiligheidsketen). De antwoorden

van deze experts zijn dus bepaald door een klein aantal zaken en verder wellicht medebepaald door verhalen van collega's, beelden uit de media of het maatschappelijke debat. Voor de uitkomsten van het empirisch onderzoek betekent dit dat de informatie van de experts in grotere mate gebaseerd is op indrukken, verwachtingen of anekdotisch bewijs, dan op daadwerkelijke (systematische) kennis van de dadergroep en de mogelijkheden en effecten van besproken interventies. Ten derde vormen de geïnterviewde daders een specifieke groep (volwassen, meerderheid veroordeeld en met hacken als primair delict), waardoor minder focus ligt op andere dadertypen in dit onderzoek. Bovendien betreft het uitsluitend Nederlandse daders. Ten slotte zijn de uitkomsten afhankelijk van zelfrapportage door de daders. Over de validiteit van rapportages van deze specifieke groep is geen onderzoek bekend, maar het is mogelijk dat daders niet al hun delictgedrag rapporteren, waardoor het criminele verleden als minder ernstig kan zijn afgeschilderd dan het in de realiteit was, of recente delicten worden verzwegen. Daarnaast kan het ook zijn dat de daders de delicten of hun delictcarrière juist 'succesvoller' afschilderden dan ze werkelijk waren. Dit zou ingegeven kunnen zijn door het eergevoel en de behoefte aan status die bij sommige (groepen) cyberdaders bestaan.

9.3. Kenmerken en profielen van daders van cybercriminaliteit in enge zin

Met de informatie uit het eerste deel van het onderzoek kan antwoord gegeven worden op de eerste onderzoeksvraag: wat zijn de kenmerken van cyberdaders en in hoeverre zijn er verschillende profielen van daders te onderscheiden? Daartoe is onderzocht wat de achtergrondkenmerken, drijfveren en beleving, criminele carrières en percepties ten aanzien van strafbaarheid, pakkans en schade zijn. De kenmerken zijn bovendien vergeleken met kenmerken van traditionele daders waardoor verschillen met deze daders konden worden beschreven (onderzoeksvraag 3). We onderscheiden (offline en online) criminogene en protectieve factoren voor het ontstaan en de ontwikkeling van het delictgedrag van cyberdaders. Bij de analyses van de dadergroep is gebruik gemaakt van verschillende algemene criminologische benaderingen zoals de differentiële-associatietheorie, neutralisatietechnieken, zelfcontrole en de rationele keuzetheorie en van concepten die specifiek ontwikkeld zijn om online en technische aspecten van daderschap te duiden zoals het *online disinhibition effect*, *digital drift* en *mastery.*

Profielen

De resultaten laten zien dat een eenvoudige clustering op grond van het wel of niet aanwezig zijn van bepaalde kenmerken geen realistisch beeld oplevert. Bij de daders zijn verschillende kenmerken aanwezig zoals vaardigheden (waaronder technische kennis) en specifieke motivaties (zoals uitdaging zoeken of status verwerven) die in verschillende combinaties en mate voorkomen. Dit leidt vervolgens tot (een bepaalde ontwikkeling in) het delictgedrag (criminele carrière). De impact van verschillende daderkenmerken op (de ontwikkeling in) het delictgedrag moet daarom zowel individueel als in hun onderlinge samenhang bekeken worden. Het startpunt van de beschrijving van daderkenmerken zijn de drijfveren voor het delictgedrag (hoofdstuk 4). De drijfveren bepalen voor een belangrijk deel wat cyberdaders als opbrengst van het delict beschouwen en daarmee een belangrijk deel van de kosten-baten ratio waarop interventies kunnen ingrijpen. Naast drijfveren zijn er in het onderzoek persoonlijke en contextkenmerken beschreven die het risico op het plegen van cyberdelicten verhogen (criminogene factoren) of juist verlagen (protectieve factoren).

Drijfveren

Een belangrijke conclusie uit het onderzoek is dat de drijfveren voor het plegen van cybercriminaliteit zeer divers zijn. Daarbij blijken drijfveren vaak naast elkaar voor te komen en zich te ontwikkelen door de tijd. Zo kan een dader die start met hacken uit nieuwsgierigheid en de behoefte aan status onder vrienden, tot de ontdekking komen dat er ook gemakkelijk geld mee te verdienen is en vervolgens financiële drijfveren ontwikkelen.

Drijfveren die volgens de literatuur en de interviews vaak een rol spelen bij cybercriminaliteit vooral door jeugdigen zijn nieuwsgierigheid, leergierigheid en de behoefte aan mentale uitdaging (als doel op zich en niet als middel). Deze drijfveren komen nauwelijks voor bij daders van traditionele criminaliteit. Met name nieuwsgierigheid kenmerkt een deel van de (jonge) daders, die gedreven zijn te kijken *of* en *hoe* bepaalde technische of online aspecten werken. Bij hen is sprake van het plegen van cybercriminaliteit voor de lol, en is de beschikbaarheid van kant-en-klare tools een faciliterende factor. Daders die vanuit de behoefte aan mentale uitdaging delicten plegen, zijn veelal intelligent en gedisciplineerd en ontwikkelen complexe technische vaardigheden. Dit zijn kenmerken die doorgaans juist niet als criminogene factoren voor criminaliteit worden gezien. Interventies die gericht zijn op het verhogen van de inspanningen die nodig zijn om een delict te plegen (door middel van bijvoorbeeld een situationele interventie) zullen naar verwachting bij deze daders niet erg effectief zijn. Door de toegang tot doelwitten moeilijker te maken, neemt de uitdaging toe en dat is precies waar de dader op uit is. Daarmee ontstaat niet de gewenste verandering in de kosten-batenafweging.

Andere belangrijke drijfveren zijn het verlangen naar erkenning en *peer respect*. Hoewel dit ook belangrijke drijfveren zijn bij traditionele criminaliteit, ligt bij cyberdaders een veel sterkere nadruk op het 'kunnen' en zijn. Om aan deze drijfveer te voldoen zijn (technische) vaardigheden en discipline nodig.

Belangrijke drijfveren voor cyberdaders die meer overeenkomen met die van traditionele daders zijn financiële redenen, wraak, macht en ideologische motieven. Deze motieven blijken veel minder voor te komen onder jeugdigen. Bovendien zijn de volwassen daders van deze delicten vaak ook plegers van traditionele delicten. Als jeugdigen delicten plegen met financiële redenen lijkt dit net als bij traditionele criminaliteit vaker in georganiseerd verband te gebeuren waarbij ook rekrutering van jeugdige, technisch vaardige hackers door de criminele organisaties plaats kan vinden.

Zoals hierboven beschreven, zijn de drijfveren belangrijk om in te kunnen schatten hoe de kosten-batenanalyse van daders tot stand komt. Daarnaast zijn in het onderzoek verschillende persoonlijke- en contextkenmerken naar voren gekomen als criminogene (risico-verhogende) of protectieve (risico-verlagende) kenmerken. Deze kenmerken worden hieronder beschreven.

Persoonlijke kenmerken

Er komen uit het onderzoek twee categorieën persoonlijke kenmerken naar voren die als belangrijke criminogene factor voor het plegen van cybercriminaliteit kunnen worden gezien. Beide categorieën worden niet of nauwelijks teruggevonden bij traditionele criminaliteit. De eerste categorie is hierboven al benoemd en betreft persoonlijkheids- of psychologische kenmerken die bijdragen aan de noodzakelijke talenten voor het tot stand komen van de delicten (nieuwsgierigheid, leergierigheid, zelfcontrole, perfectionisme, behoefte aan erkenning en bewijsdrang ten aanzien van technische vaardigheden). Daders met deze kenmerken starten veelal jong met experimenteren. Dit kan ook wel de fase van 'affectie voor computers' worden genoemd. Het hangt af van tal van andere factoren, zoals het vermogen tot moreel redeneren, het persoonlijke moreel kompas, de bindingen in de offline

wereld (gezin, school en werk), en de contacten in de online wereld (*peers*, rolmodellen) hoe de carrière zich ontwikkelt (of bijvoorbeeld financiële of ideologische drijfveren een rol gaan spelen).

De tweede categorie betreft persoonlijkheids- of psychologische kenmerken die offline sociale interactie bemoeilijken (zoals introversie, kenmerken van een autismespectrumstoornis en sociale onhandigheid). Deze kenmerken komen bij cyberdaders van alle leeftijden en in de verschillende fasen van de loopbaan voor, terwijl zij bij daders van traditionele criminaliteit juist minder dan gemiddeld voorkomen. Het betreft over het algemeen moeilijk veranderbare kenmerken. Interventies moeten zich daarom vooral richten op het ontwikkelen van protectieve factoren (offline of online) die de ontwikkeling van een criminele carrière bij daders met deze persoonlijkheidskenmerken voorkomen. Er zijn tot slot weinig aanwijzingen gevonden voor de aanwezigheid van de (criminogene) factoren gebrekkige zelfcontrole en beperkte verstandelijke vermogens die bij een deel van de traditionele criminaliteit een belangrijke rol spelen.

Contextkenmerken

Sociale context

Gebrek aan ouderlijk toezicht (bij jeugdigen) of toezicht vanuit intieme relaties (bij volwassenen) wordt zowel in de literatuur als door de experts als een belangrijke criminogene factor aangeduid. Omdat ouderlijk toezicht op het online gedrag echter veel complexer is dan op offline gedrag (door onder andere het gebrek aan grenzen in tijd en plaats en de kennisachterstand van ouders) is er een veel grotere en minder duidelijk af te bakenen groep ouders die onvoldoende in staat is adequaat toezicht te houden. Gezinsproblematiek zoals een scheiding of verslavingsproblematiek bij de ouders lijkt wel bij te dragen aan het risico dat er onvoldoende toezicht is, maar dit lijkt veel minder aan de orde te zijn dan bij offline criminaliteit. Daartegenover staan studies die aangeven dat sociaaleconomische en intellectuele hulpbronnen van ouders (die doorgaans als protectief worden beschouwd) ook juist bij kunnen dragen aan het delictgedrag van een jongere omdat de ontwikkeling van technische vaardigheden op de computer sterk gestimuleerd wordt door de ouders. Op basis van deze uitkomsten kan verwacht worden dat de bestaande diagnose-instrumenten waarmee criminogene factoren in het gezin worden geïdentificeerd niet volstaan bij cyberdaders. Zo zou een gebrek aan bewustzijn bij ouders over de gevaren van het internet voor jongeren en de wijze waarop zij problematisch internetgebruik door hun kinderen kunnen herkennen ook als een criminogene factor kunnen worden aangeduid. Deze factor is niet in de huidige instrumenten opgenomen.

De oudere literatuur wijst tevens op gezinsproblematiek als factor die ertoe leidt dat jeugdigen veel online zijn (als vlucht uit de gespannen of eenzame situatie) en daarmee veel gelegenheid hebben online delictgedrag te ontwikkelen. Bovendien zou een gebrek aan ouderlijke betrokkenheid samenhangen met een beperkte gewetensontwikkeling. Experts herkennen deze subgroep cyberdaders waarbij gezinsproblematiek een rol lijkt te spelen, maar er is meer empirisch onderzoek nodig voordat hierover conclusies kunnen worden getrokken. Gezinsproblematiek speelt overigens op dezelfde wijze een rol bij daders van traditionele criminaliteit. Ook daar ontvluchten jeugdigen de situatie thuis maar dan veelal richting de straat en hun offline *peers*. In de aanpak hiervan zouden dus mogelijk vergelijkbare interventies ingezet kunnen worden als bij traditionele criminaliteit.

Naast het gezin bepalen vooral de *peers* de sociale context waarin jeugdigen verkeren. Het hebben van (veel) online (delinquente) vrienden wordt gezien als een belangrijke criminogene factor voor delictgedrag. Hoewel ook bij traditionele criminaliteit de *peers* een belangrijke rol spelen, worden in de online wereld de processen nog versterkt omdat er 24/7 interactie gaande is, die bovendien (op

online platformen) op grotere schaal plaatsvindt. Bovendien ligt er een sterke nadruk op laten zien wat je 'kunt' qua technische vaardigheden hetgeen als een directe aanmoediging geldt voor het plegen van delicten. Mechanismen die een rol spelen zijn het creëren van gelegenheid door actieve deelname op (game) fora, blootstelling aan criminele definities, normvervaging, normalisering van het delictgedrag en de behoefte aan het verkrijgen van status van de *peers*.

Over de rol van scholen als protectieve of criminogene factor bij cybercriminaliteit in enge zin wordt in de literatuur en de expertinterviews nauwelijks gesproken. Wel wordt de school als plek genoemd waar preventieve interventies kunnen worden ingezet (zie paragraaf 7.4.2).

Ten aanzien van oudere daders is er nog erg weinig bekend over de sociale context als criminogene of protectieve factor. Omdat de risico's ofwel de kosten van het online delictgedrag als laag worden ingeschat (pakkans en straffen zijn laag, daders wanen zich anoniem online) en het beter te combineren lijkt met een normale baan (zeker als die al in de ICT is), zijn klassieke inzichten over de rol van bindingen waarschijnlijk minder bruikbaar.

Online context en percepties van schade

Het feit dat cyberdelicten online plaatsvinden heeft twee belangrijke implicaties. Deze zijn uiteraard voor alle potentiële daders aanwezig maar zullen afhankelijk van de persoonlijke kenmerken en sociale omgeving meer of minder bijdragen aan het tot stand komen van de delicten. Beide implicaties zijn gerelateerd aan het *online disinhibition effect*, als gevolg waarvan door de online anonimiteit van daders en slachtoffers een andere evaluatie van het gedrag plaatsvindt door de dader dan wanneer de interactie offline zou zijn.

De eerste implicatie van de online context is dat daders de ernst van het delict en de aangerichte schade bagatelliseren. Hoewel ontkenning van het slachtoffer of de aangerichte schade ook bij daders van traditionele criminaliteit voorkomt, wordt dit online versterkt door de afstand tot slachtoffer, de hyperrealiteit waarin het gedrag tot stand komt (het voelt als een spel), de normalisering die ontstaat door gamen (waar het routine en normaal is om elkaar te DDoSsen of te hacken in het spel). Door het gemak waarmee bepaalde delicten (in hoge frequentie) gepleegd kunnen worden, is het besef van de aangerichte schade bij de dader nog minder aanwezig. Deze effecten zullen bij jonge startende daders die zich in de fase van 'nieuwsgierige exploratie' bevinden het grootst zijn, omdat zij nog meegesleept worden door de kick, een beperkt ontwikkeld inlevingsvermogen hebben en weinig geconfronteerd zijn met de aangerichte schade. Bij een deel van de daders neemt het effect van de online context volgens experts en de literatuur af met het ouder worden, doordat ze een beter inlevingsvermogen ontwikkelen en mogelijk (doordat ze een keer gepakt zijn) meer geconfronteerd zijn met de aangerichte schade. Als gevolg daarvan zal ook vaak het delictgedrag afnemen. Uit de daderinterviews komt naar voren dat naar verloop van tijd de spanning of kick die gepaard gaat met het plegen van het delict weg kan gaan, waardoor ze dan stoppen. Bij oudere daders die hun carrière voortzetten, lijkt het bagatelliseren van de schade een minder grote rol te spelen. Zij erkennen de schade maar de drijfveren die zij hebben voor het gedrag (financieel, wraak, ideologisch, etc.) zijn voor hen belangrijk genoeg om de carrière voort te zetten.

De tweede implicatie van de online context is dat daders vanwege de online anonimiteit sneller tot een actie overgaan waar ze in de offline wereld teveel remmingen voor zouden voelen vanwege het oordeel van anderen of andere gevreesde consequenties. Dit mechanisme is gevonden voor jeugdige daders maar speelt mogelijk ook een rol bij volwassen daders. Het geldt niet alleen voor cybercriminaliteit in enge zin, maar ook voor ruime zin.

Het is nog niet goed duidelijk in hoeverre het *online disinhibition effect* enerzijds maakt dat personen van wie het niet wordt verwacht - op basis van criminogene factoren als impulsiviteit, beperkte empathie en gebrekkig moreel redeneren - toch delicten plegen. Anderzijds kan dit effect eraan bijdragen dat meer en ernstigere delicten worden gepleegd door personen die toch al hoog scoren op deze criminogene factoren.

Strafrechtelijke context

Zowel de perceptie van strafbaarheid van de illegale activiteiten die cyberdaders ondernemen als de perceptie van een zeer lage pakkans maken dat cyberdaders hun daden als weinig risicovol inschatten voor wat betreft de kosten door eventuele juridische sancties. De gebrekkige perceptie van strafbaarheid bij een deel van de vooral jonge daders komt onder andere voort uit de afwezigheid van toezicht in de online wereld, de onzichtbaarheid van de aangerichte schade en voor een deel van de daders de aanwezigheid van drijfveren die in aanleg niet kwaadaardig zijn (nieuwsgierigheid, mentale uitdaging, erkenning van talenten). Binnen deze laatste categorie vallen ook de delicten waarbij beveiligingsproblemen worden aangetoond, maar onduidelijkheid bestaat over de juridische grenzen en de kaders van *responsible disclosure*. Daarmee is de beperkte perceptie van strafbaarheid een belangrijkere criminogene factor bij cyberdaders dan bij traditionele daders.

Met het voortgaan van de carrière neemt het besef van de strafbaarheid bij daders toe, maar wordt dit volgens experts deels weer teniet gedaan door de zeer beperkte zichtbaarheid van politie en justitie als het gaat om online criminaliteit. Er is nog weinig aanwezigheid van politie op online fora en markten en er zijn weinig voorbeeldcasussen met serieuze straffen, waarvan een signaalfunctie kan uitgaan. De perceptie van strafbaarheid van het gedrag hangt dus samen met (de perceptie van) een serieuze pakkans en straf. Omdat cyberdaders de pakkans als zeer laag inschatten, leidt dit tot een gevoel van onaantastbaarheid, zowel bij jeugdigen als volwassenen. Hoewel ook bij vele vormen van traditionele criminaliteit de pakkans laag is, ligt deze bij cyberdelicten doorgaans nog vele malen lager. Ook is de kans dat er voldoende bewijs wordt gevonden waardoor een verdachte ook daadwerkelijk veroordeeld wordt relatief laag.

De literatuur en experts maken duidelijk dat het niet de daadwerkelijke strafdreiging en pakkans zijn maar vooral de *gepercipieerde* strafdreiging en pakkans die bepalend zijn voor de rationele afwegingen van (potentiële) cyberdaders. Daders die steeds wegkomen met hun delicten en weinig voorbeelden om zich heen zien van gepakte daders gaan de pakkans mogelijk als steeds lager inschatten. Bij daders die al verder in hun carrière zijn (bijvoorbeeld in de fase van 'criminele exploitatie'), werkt de lage pakkans dus mogelijk nog meer criminogeen dan bij startende daders die deze ervaringen nog niet hebben.

Ook voor deze aspecten is het weer van belang meer zicht te krijgen op de manier waarop ze samenhangen met persoonlijke en contextkenmerken van potentiële daders. Voor een deel van de daders (met weinig criminogene factoren) zal voorlichting over de strafbaarheid wellicht voldoende zijn om het delictgedrag te stoppen. Voor andere daders maakt voorlichting wellicht alleen dat ze hun gedrag beter gaan afschermen.

Uit het voorgaande komt het beeld naar voren dat er een grote variatie bestaat in typen cyberdaders, zowel wat betreft drijfveren als criminogene- en protectieve factoren voor het plegen van criminaliteit. Bovendien is stilgestaan bij hoe de online en strafrechtelijke context (op uiteenlopende wijzen) bijdragen aan criminele carrières. Daarbij zijn de kenmerken waar mogelijk vergeleken met traditionele daders. Daarmee is een antwoord gegeven op de eerste en derde

onderzoeksvraag van dit onderzoek. In de volgende paragraaf richten we ons op de conclusies over de aansluiting van beschikbare of te ontwikkelen interventies bij deze kenmerken van cyberdaders.

9.4. Passende interventies

Het tweede deel van dit onderzoek richtte zich op de vraag welke interventies bestaan die aansluiten bij de aard van de daders van cybercriminaliteit zoals beschreven in het eerste deel van het onderzoek. Daarbij gaat het zowel om interventies die specifiek gericht zijn op daders van cybercriminaliteit (onderzoekvraag 2) als op interventies die ontwikkeld zijn voor traditionele daders en mogelijk ingezet kunnen worden voor daders van cybercriminaliteit (onderzoeksvraag 4).

Een belangrijke eerste conclusie is dat er weinig interventies bestaan die specifiek gericht zijn op daders van cybercriminaliteit. Ook zijn er nauwelijks evaluatieonderzoeken gevonden waarin de (potentiële) effectiviteit van interventies voor cyberdaders wordt onderzocht. Om na te gaan wat mogelijk passende interventies voor deze doelgroep zijn, gaan we daarom af op de verwachtingen over de effectiviteit zoals vermeld in de literatuur en interviews. In deze analyse over potentieel effectieve interventies maken we een tweedeling in het type interventies.

In de eerste plaats bespreken we interventies gericht op afschrikking en situationele criminaliteitspreventie die direct ingrijpen op de perceptie van de kosten-baten verhouding bij het plegen van cybercriminaliteit (rationele keuzebenadering). In de tweede plaats bespreken we interventies die ingrijpen op de bestaande criminogene en protectieve factoren voor het plegen van cybercriminaliteit bij het individu en de verschillende contexten waarin het individu verkeert (*What Works* en de *desistance* benadering). De benaderingen kunnen niet helemaal los van elkaar gezien worden. Zo zullen er interventies zijn die zodanig ingrijpen op criminogene of protectieve factoren dat daarmee de kosten-baten afweging voor cybercriminaliteit wordt beïnvloed (denk aan interventies gericht op versterking van het ouderlijk toezicht).

9.4.1. Gelegenheidsbeperking, bewustwording en strafrechtelijke gevolgen

Volgens de rationele keuze-benadering baseren potentiële daders hun beslissingen over het plegen van delicten op een kosten-batenafweging. Interventies zouden daardoor effectief zijn als ze ofwel de kosten voor het plegen van een delict verhogen ofwel de baten verlagen. De kosten van het plegen van een delict worden gevormd door de inspanningen die nodig zijn om het delict te plegen en de negatieve gevolgen die het delict voor de potentiële dader heeft. De baten zijn de opbrengsten van het delict en deze kunnen variëren van financieel gewin, tot sociale, mentale of fysieke opbrengsten (zoals status, uitdaging en kick).

Situationele preventiestrategieën (zoals *warning banners* en de verstoring van digitale markten) kunnen een rol spelen bij het verhogen van het risico en de noodzakelijke inspanningen. Klassieke afschrikkingstheorieën beschrijven daarnaast dat de gepercipieerde kosten van criminaliteit omhoog gaan met een grotere (gepercipieerde) pakkans en hogere strafdreiging bij de delicten. Als gevolg van de grote diversiteit aan drijfveren voor het plegen van cybercriminaliteit, zijn ook de gewenste opbrengsten bij cybercriminaliteit meer divers dan bij de meeste vormen van traditionele criminaliteit. Vaker dan bij traditionele criminaliteit gaat het om drijfveren anders dan financieel gewin, jaloezie, wraak, of het verwerven van status. De alternatieve gewenste opbrengsten (zoals intellectuele uitdaging of erkenning van talenten) die subgroepen cyberdaders nastreven, lijken doorgaans minder goed beïnvloedbaar met traditionele interventies die zich baseren op situationele preventie of afschrikking.

Tabel 9.1 geeft een overzicht van de interventies gebaseerd op situationele preventie en afschrikking die in dit onderzoek zijn gevonden. Daarbij is steeds weergegeven voor welke groep daders bekend is of verwacht wordt dat de interventies potentieel effectief zijn en voor welke groep daders ze niet effectief lijken te zijn of zelfs tot een hoger risico op delicten lijken te leiden. Voor dadergroepen die niet worden benoemd is in de literatuur of door de experts geen informatie gegeven op basis waarvan de mogelijke effectiviteit kan worden ingeschat.

Van alle beschreven interventies is het verstoren van digitale markten (een voorbeeld van situationele preventie) de interventie die het meest direct ingrijpt op de inspanningen die geleverd moeten worden om delicten te plegen en daarmee op de kosten van het delict. Subgroepen die gevoelig zijn voor deze kosten zijn daders met financiële drijfveren in alle fasen van hun loopbaan en daders (ongeacht hun drijfveren) die hun delicten plegen met behulp van gekochte tools. Voor deze subgroepen zou de verstoring van digitale markten dus effectief kunnen zijn.

Andere interventies die zich richten op verhoging van de gepercipieerde kosten zijn interventies gericht op bewustwording van de risico's die het delict voor de dader meebrengt (zoals de kans op straf) of van de aangerichte schade (bewustzijn over deze schade kan het geweten van een dader belasten en daarmee als last worden beleefd). Of dergelijke interventies effectief zijn, hangt af van de mate waarin de daders open staan voor de informatie die in de interventies wordt overgedragen (responsiviteit). Zo zullen de interventies gericht op bewustwording van schade voor slachtoffers minder impact hebben op het gedrag van de meestal (zeer) jonge daders of daders met specifieke persoonlijkheidskenmerken waardoor inleven in de ander minder goed verloopt. Jeugdigen voor wie deze interventie mogelijk effectief is, zijn degene met een goed ontwikkeld empathisch vermogen en goede gewetensontwikkeling. Ook interventies gericht op informatie over strafbaarheid zullen vooral effectief zijn voor startende daders die niet de intentie hebben strafbaar of schadelijk gedrag te vertonen. Voor interventies gericht op bewustwording (voorlichting, *warning banners*) zal in het algemeen gelden dat ze niet effectief zijn voor meer ervaren daders en daders die er drijfveren op na houden waarbij de strafbaarheid een onderdeel is van de opbrengsten (bijvoorbeeld meer spanning of status).

Belangrijk is dat bij deze interventies door experts ook steeds gewezen wordt op mogelijk averechtse effecten. Dit kan te maken hebben met de responsiviteit van cyberdaders, waarbij door dergelijke bewustwordingsacties juist motivaties als nieuwsgierigheid, behoefte aan spanning (*sneaky thrill*) of verlangen naar status kunnen worden getriggerd.

In het onderste gedeelte van tabel 9.1 zijn de strafrechtelijke reacties opgenomen. Ook deze interventies zijn vooral gericht op het verhogen van de (gepercipieerde) kosten. Omdat zowel de pakkans als de strafdreiging bij cyberdelicten zeer laag is, gaat er momenteel volgens experts en de literatuur weinig generaal preventieve werking van deze reacties uit. Ook het specifieke preventieve effect is beperkt omdat het lang duurt voordat een veroordeling volgt en de straffen doorgaans laag zijn. Snel straffen is volgens alle experts vooral van belang bij jonge daders. Terwijl voor hen juist negatieve effecten uitgaan van hoge straffen zonder resocialiserende aspecten (hoge boetes of lange vrijheidsstraffen).

Zoals uit tabel 9.1 blijkt, wordt een verhoging van de pakkans en strafdreiging voor specifieke dadergroepen potentieel effectief geacht. Dit betreft vooral jonge daders zonder financiële motieven waarbij een waarschuwing door de handhavende instanties (*knock and talk*) en (dreiging van) arrestatie los van veroordeling een schrikeffect teweeg zou brengen en een besef dat het gedrag strafbaar en schadelijk is. Dit functioneert vervolgens als een aangrijpingspunt voor gedragsverandering (*hook for change*-principe). Voor jeugdigen met veel technische vaardigheden of

met drijfveren zoals het verwerven van status wordt verwacht dat (alleen) het verhogen van de gepercipieerde pakkans en strafdreiging geen effect zal hebben. Meer in het algemeen zullen rationele dadergroepen zich door meer zichtbaarheid van (de capaciteiten van) de handhavende instanties vooral beter gaan beveiligen om niet gepakt te worden. De zichtbaarheid van daadwerkelijk succesvolle cyberacties door de politie, waaruit eventueel hoge straffen voortkomen, zou wel bijdragen aan afname van het delictgedrag bij voornamelijk financieel gemotiveerde (georganiseerde) daders. Door die zichtbaarheid verdwijnt het gevoel van onaantastbaarheid en ontstaat een aangepaste kosten-baten uitkomst wat hen mogelijk doet afzien van cyberdelicten.

Tabel 9.1 Overzicht potentiele effectiviteit interventies gericht op gelegenheidsbeperking en strafrechtelijke reacties

Type interventie	**Potentieel effectief voor**	**Geen of negatief effect verwacht voor**	**Bron**
Gelegenheid beperkend			
Verstoring/sluiting markten (o.a. door aanpakken facilitators)	- Financieel gemotiveerde daders (alle fasen) - (Startende) daders die kant-en klare tools gebruiken en/of kennis hebben van markten		Literatuur
Warning banners *Knock and talk*	- (Zeer) jonge potentiële en startende daders (hackers), met beperkte kennis van strafbaarheid en juridische gevolgen (want interventie is gericht op bewustwording strafbaarheid)	- Ervaren daders (fase van rijping of later) - Statusgerichte jeugdige daders - Daders (hackers) met spanning, kick en macht als drijfveer - Financieel gemotiveerde daders (o.a. phishers)	Literatuur/ experts
Online *policing* (toezicht, bewustwording, advies)	- (Zeer) jonge potentiële en startende daders, met beperkte kennis van strafbaarheid en juridische gevolgen	- Daders in de ontdekkingsfase: affectie voor computers - Statusgerichte jeugdige daders - Daders met spanning, kick, macht als drijfveer - Ervaren daders (fase van rijping of later)	Literatuur
Voorlichting op scholen (over schade voor slachtoffers en risico's eigen toekomst)	- (Zeer) jonge potentiële en startende daders met beperkte kennis van strafbaarheid en juridische gevolgen), mits goede empathische vermogens en gewetensontwikkeling (zwakke aanwijzingen)	- Statusgerichte jeugdige daders - Daders met spanning, kick en macht als drijfveer	literatuur/experts
Strafrechtelijke reacties			
(Perceptie over) pakkans verhogen: - Feitelijke/dreiging arrestatie - Zichtbaarheid cyberacties/ capaciteit/bevoegdheden	- Jonge niet financieel gemotiveerde *first offenders* (zwakke aanwijzingen) - Financieel gemotiveerde (georganiseerde) daders	- Technisch vaardige daders (die zich goed weten af te schermen) - Daders die uit zijn op status van *peers*	Experts literatuur/ experts/ daders
Sneller straffen / schorsende voorwaarden	- Jonge startende daders		Literatuur/experts/daders
Strafdreiging verhogen	- Rationele dadertypes (zwakke aanwijzingen)	- Jonge *first offenders* - Hackers met behoefte aan spanning, kick of macht als drijfveer	Literatuur/experts
Feitelijk geëiste/opgelegde straffen verhogen	- Rationele dadertypes (generale preventie)	- Jonge daders zonder kwade bedoelingen	Literatuur/experts

Vrijheidsstraf	- Rationele dadertypes (indien kosten te hoog worden tov baten)	- Jonge *first offenders* - Financieel gemotiveerde daders (o.a. phishers) (nieuwe connecties tijdens detentie, betere afscherming, etc)	Literatuur/experts
Financiële straf - Verbeurdverklaringen - Geldboete - Schadevergoeding	- Daders met zelf ontwikkelde tools - (jeugdige en volwassen) daders die bewust of onbewust aanzienlijke schade hebben aangericht	- Jonge daders (bij hoge boetes of schadevergoedingen)	Experts

9.4.2. Interventies op basis van *What Works* en de *desistance* benadering

De *What Works* benadering heeft voor traditionele criminaliteit laten zien dat met vrijheidsbeperkende interventies alleen geen recidive-vermindering of zelfs een toename in recidive wordt bereikt. Belangrijke redenen daarvoor zijn dat vrijheidsbeperkende straffen vaak een versterkend effect hebben op de criminogene factoren die aan het delictgedrag ten grondslag liggen. In het huidige onderzoek wordt deze gedachte door experts onderschreven door te wijzen op de schade die vrijheids- en financiële straffen hebben voor het sociale kapitaal en andere bindingen van cyberdaders. Deze schade zou mogelijk zelfs groter zijn dan bij traditionele daders omdat cyberdaders voorafgaand aan het delict (zoals ook uit deel 1 van dit onderzoek blijkt) meer hulpbronnen bezitten zoals een goede band met de ouders, prosociale vrienden, een opleiding en een baan.

Over (effectiviteit van) de inzet van interventies gericht op de criminogene behoeften van cyberdaders is in de literatuur en bij experts nog weinig bekend. Een belangrijke constatering hierbij is dat er nog nauwelijks sprake is van een goede risicotaxatie bij deze groep daders. In de eerste plaats bleek dat er nog maar beperkt zicht is op hoe de criminogene factoren bij cyberdaders precies gemeten moeten worden (voorbeelden waren de kwaliteit van de ouderlijke supervisie en de wijze waarop persoonlijke en psychologische kenmerken van daders gerelateerd kunnen worden aan delictgedrag in de online context). Daardoor lijken bestaande diagnose-instrumenten nog onvoldoende gevalideerd ten aanzien van de criminogene en protectieve factoren waarop interventies specifiek bij cyberdaders ingezet moeten worden. Daarnaast geven verschillende experts aan dat er van (tijdige) risicotaxatie met de noodzakelijke verdiepende analyse door deskundigen bij deze dadergroep nog onvoldoende sprake is. Hiervoor is een juiste 'routering' in het afdoeningsproces noodzakelijk. Meer inzet uit de risicodiagnose zou de kennis over de criminogene en protectieve kenmerken van deze dadergroep kunnen verdiepen.

Ondanks dit gebrek aan adequate diagnoses van de (criminogene) behoeften van cyberdaders, zijn er in de interviews diverse concrete interventies benoemd die gebaseerd zijn op *What Works* en *desistance* principes. Deze worden in het vervolg van deze tekst beschreven. Daarbij wordt, net als in de vorige paragraaf, aangegeven bij welke subgroepen daders effectiviteit wordt verwacht. Voor deze interventies is anders dan bij de tabel in de vorige paragraaf niet aangegeven voor welke subgroepen ze negatieve effecten hebben of niet effectief zijn, omdat daarover in de interviews geen informatie naar voren is gekomen.

Risk-based-interventies

Als het om interventies gaat waarbij wordt ingezet op criminogene behoeften van daders dan blijkt voornamelijk verwezen te worden naar bestaande interventies voor traditionele daders (bovenste gedeelte tabel 9.2). Experts verwijzen naar interventies gericht op diverse leefgebieden zoals de relatie met ouders, het aanleren van sociale vaardigheden, het aanpakken van een pro-criminele houding en het werken aan schulden of verslaving. Deze interventies zouden effectief kunnen zijn voor het aanpakken van de betreffende criminogene factor bij daders van verschillende leeftijden en in verschillende fasen van de criminele loopbaan mits motivatie voor verandering aanwezig is of kan worden gecreëerd. De verwachting is echter dat daders in het algemeen onvoldoende responsief zullen zijn voor deze interventies zoals die nu worden toegepast omdat deze – met uitzondering van de online variant van de leerstraf tools4U - geen rekening houden met de online context waarin de delicten plaatsvinden. Online is schade bijvoorbeeld vaak minder zichtbaar en het slachtoffer is erg 'abstract'. Om daar meer rekening mee te houden, wordt door experts verwacht dat een methode als *mentaliseren*, wat inleven in een ander inhoudt, zinvol kan zijn. Ook verwachten experts positieve

effecten van contact met het slachtoffer. Er zijn echter nog weinig ervaringen met een dergelijke interventie en bovendien lijkt het in cyberzaken, meer dan bij traditionele zaken, vaker om een veelheid aan slachtoffers te gaan (denk aan ransomware en online oplichting of fraude), wat ook uit de daderinterviews naar voren komt. Deze en andere methoden die eraan bijdragen het slachtoffer minder abstract te maken zouden moeten worden geïntegreerd in bestaande interventies om voldoende aan te sluiten bij de *responsiviteit* van cyberdaders.

De enige specifiek op cyberdaders gerichte interventies die genoemd zijn, zijn het opleggen van restricties rondom computer en internetgebruik en de inzet van *serious gaming*. Restricties rondom computer en internet gebruik kunnen onder meer zorgen voor het afsluiten van contact met online criminele *peers* (een belangrijke criminogene factor). Een dergelijke afsluiting is echter complex te bewerkstelligen en zal altijd tijdelijk zijn. Deze interventie moet dus gezien worden als een interventie die een momentum schept voor andere interventies die op de meer lange termijn *desistance* in gang kunnen zetten (door bijvoorbeeld het ombuigen van de pro-criminele houding en het aanreiken van alternatieven).

De inzet van *serious gaming* is potentieel effectief voor jonge niet kwaadwillende daders die op deze manier spelenderwijs bewust worden gemaakt van goede en slechte aspecten van het hacken. Dit is daarmee een relatief lichte interventie die bij kan dragen aan kennis over ethiek en bewustwording bij jonge hackers. Hoewel geen negatieve effecten kunnen worden verwacht van deze interventie, blijft het nog de vraag of de effecten die gegenereerd worden in een spelsetting ook in 'real life' effect hebben. Daar staat weer tegenover dat *serious gaming* plaatsvindt in een context van begeleiding en er naar alle waarschijnlijkheid over ethische grenzen wordt gesproken. Bij dit laatste resteert de vraag in hoeverre men vatbaar (responsief) is voor deze informatie en of hun morele kompas daadwerkelijk wordt bijgestuurd. Meer onderzoek is nodig om antwoord te kunnen geven op deze vragen.

Het is tot slot opvallend dat door de experts niet of nauwelijks gesproken is over interventies gericht op ouders. Dit is mogelijk het gevolg van de focus die in het onderzoek is gelegd op de daders. Toch is bij traditionele interventies voor jeugdigen al enige tijd veel aandacht voor de meer systeemgerichte interventies waarbij de dader en de interactie van de dader met het systeem rondom de dader (veelal het gezin) in de interventie centraal staan. Hiervan lijkt bij cyberdaders nog weinig gebruik gemaakt te worden. Een meer systeemgerichte aanpak kan van belang zijn om de gesignaleerde beperkingen in het ouderlijk toezicht op het online gedrag weg te nemen en protectieve factoren te versterken.

Strength-based interventies

Behalve voor interventies gericht op het verminderen van criminogene behoeften, is in de literatuur en onder experts ook aandacht voor *strength-based* interventies. Dergelijke interventies sluiten nauw aan bij theorieën over *desistance*, waarbij niet alleen het stoppen met criminaliteit, maar ook het ontwikkelen van een nieuwe identiteit en nieuwe pro-sociale relaties centraal staan. Belangrijk uitgangspunt hierbij is dat daders de mogelijkheid krijgen '*to desist into something*'. Toegepast op cyberdaders beschrijven experts interventies die inspelen op de technische vaardigheden en talenten die (potentiële) cyberdaders bezitten en die proberen het (criminele) gebruik van die talenten om te buigen door hen te leren wat ethisch hacken inhoudt en hen perspectieven te bieden van wat zij met deze vaardigheden zouden kunnen bereiken op de arbeidsmarkt.

Meer dan bij daders van traditionele criminaliteit zijn bij een aanzienlijk deel van de daders van cybercriminaliteit in engere zin talenten aanwezig die veel waarde hebben voor de samenleving

mits ze op een pro-sociale manier worden ingezet. Door experts in dit kader veelgenoemde preventieve interventies zijn cyberwerkplaatsen en hackwedstrijden. Deze interventies zijn gericht op het vergroten van IT-vaardigheden en het leren van ethisch hacken. Door dergelijke interventies krijgen jongeren tevens erkenning, leren zij andere hackers kennen en wordt gebouwd aan (zowel technische als sociale) vaardigheden en toekomstperspectief. Een andere vorm van een *strength-based* interventie(onderdeel) is begeleiding door rolmodellen. Zowel experts als de literatuur benoemen dit als een belangrijk element bij het opbouwen van een nieuwe identiteit en relaties. Dergelijke interventies moeten volgens de experts in samenwerking tussen overheidsinstantie en private partijen tot stand komen waarmee een sterk signaal uitgaat naar de hackers dat de samenleving open staat voor hun talenten en kansen biedt voor de inzet van die talenten op een legale manier.

Een specifiek op cyberdaders gerichte interventie waarbij gewerkt wordt aan het versterken van talent en het ethisch leren hacken door middel van een leerstraf bij een IT-bedrijf en waarbij ervaren hackers als coaches worden ingezet is de Hack_Right interventie. Hierbij wordt aan verschillende criminogene behoeften gewerkt, waaronder bewustwording van de schade en het waar mogelijk herstellen daarvan, en tegelijkertijd bijgedragen aan het proces van *desistance* door jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving. Experts verwachten dat dit voor de specifieke doelgroep waarvoor de interventies is bedoeld (jonge *first offenders* die geen zwaar delict hebben gepleegd, die technisch vaardig en gemotiveerd zijn en die het delict hebben bekend) veel kan betekenen. Tegelijkertijd zijn kritische geluiden te horen, zoals dat deze doelgroep zo een beloning krijgt als straf (namelijk een sterker CV), terwijl dit voor andere doelgroepen niet geldt en dit tevens afbreuk zou doen aan het generaal preventieve effect van straf.

Naast de kansen die *strength-based* interventies aan de daders bieden, zouden ze ook tot een afname van toekomstig daderschap leiden en daarmee tot een positieve uitkomst voor de samenleving. Ook bij de inzet van deze interventies is het uiteraard van belang dat de juiste doelgroepen worden geselecteerd, waarbij de drijfveren voor het delictgedrag een belangrijk criterium lijken te vormen. Bovendien is het van belang dat de verschillende onderdelen in combinatie terugkomen in de interventie. Alleen werken aan het vergroten van de IT-vaardigheden en het bieden van een netwerk of carrièrekansen zonder dat gewerkt wordt aan het moreel besef en het ombuigen van een eventuele pro-criminele houding kan immers tot meer cybercriminaliteit leiden.

Tabel 9.2 *Risk-based* en *strength-based* interventies op basis van *What Works* en *desistance* benadering

Type interventie	**Potentieel effectief voor (in alle gevallen is het bewijs zwak)**	**Bron**
Risk-based interventie (onderdelen)		
Traditionele interventies gericht op aanpak van pro-criminele attitudes (moreel redeneren, ombuigen rationalisaties of neutralisaties)	- Daders met beperkt inlevingsvermogen - Daders met beperkt besef van de gevolgen van het gedrag - Daders met beperkte ontwikkeling van het moreel redeneren	Literatuur/experts/daders
Traditionele interventies gericht op verbetering sociale vaardigheden, relaties (met ouders of prosociale vrienden), aanpak van schulden of verslaving	- Daders die sociaal geïsoleerd leven of alleen online (criminele) vrienden hebben - Daders die weinig steun van ouders of sociaal netwerk ervaren	Literatuur/experts
Traditionele interventies gericht op de aanpak van schulden of verslaving	- Daders met schulden of verslaving gerelateerd aan het plegen van cyberdelicten	Experts
Herstelbemiddeling met slachtoffer (vrijwillig voor dader en slachtoffer)	- Daders met beperkt inlevingsvermogen - Daders met beperkte ontwikkeling van het moreel redeneren	Experts
Restricties rondom computer en internetgebruik (afsluiting van criminele peers)	- Daders met online criminele peers als criminogene factor - Daders van alle leeftijden	Literatuur/experts
Serious gaming (leren van goede en slechte aspecten van hacken, moreel redeneren/ethiek)	- Jonge niet kwaadwillende daders - Daders met beperkt besef van de gevolgen van het gedrag - Daders met beperkte ontwikkeling van het moreel redeneren	Experts
Strength-based interventie (onderdelen)		
Vergroten IT-vaardigheden en carrièremogelijkheden, pro-sociaal netwerk opbouwen, positief bijdragen aan maatschappij en aanleren ethisch hacken - *Responsible disclosure* - Rolmodellen	- Technisch vaardige daders - Daders met of zonder financiële motieven - Specifiek: daders met drijfveren mentale uitdaging, nieuwsgierigheid, status	Experts/literatuur/daders

- Cyberwerkplaatsen - Hackwedstrijden (*Bug bounty's*/*hack in contest*) Initiatieven als signaal van open houding vanuit samenleving voor talenten		
Hack_Right	- Technisch vaardige *first offenders* met een laag recidiverisico	Experts/daders

9.5. Slotconclusie en aanbevelingen

In dit onderzoek is een analyse gemaakt van de (unieke) kenmerken van cyberdaders en de mate waarin beschikbare interventies aansluiten bij deze kenmerken. Deze analyse leidt tot een aantal aanbevelingen over de wijze waarop interventies voor cyberdaders vormgegeven moeten worden. We bespreken hier een drietal aanbevelingen.

In de eerste plaats is het van belang dat er *meer* en meer *toegesnede*n verdiepingsdiagnostiek plaatsvindt ten behoeve van beslissingen over (strafrechtelijke) interventies voor cyberdaders. Nu de diversiteit onder cyberdaders groot blijkt, is een op maat gesneden aanpak van belang en daartoe moeten de criminogene en protectieve kenmerken en de wijze waarop deze het delictgedrag in de online omgeving beïnvloeden in kaart worden gebracht. De huidige instrumenten lijken nog onvoldoende in staat om deze specifieke cyberdader gerelateerde kenmerken te meten. Naast criminogene behoeften is daarbij ook specifiek aandacht nodig voor responsiviteit voor interventies (leerstijlen en motivaties) van cyberdaders die in een online omgeving hun delicten plegen. Voor cyberdaders lijkt het aangewezen dat specifieke aanvulling op bestaande diagnose-instrumenten beschikbaar komt.

In de tweede plaats lijken interventies waarin bewustwording, mentaliseren (inleven in de ander), moreel redeneren (in combinatie met ethisch hacken) en het aanbieden van kansen gecombineerd worden veel potentie te hebben om effectief te zijn voor met name jonge technisch vaardige daders. Echter, deze interventies blijken ook ongewenste effecten op te kunnen leveren, omdat ze daders onbedoeld op ideeën kunnen brengen of de status van cyberdaders bij hun *peers* kunnen verhogen. Het is dus belangrijk om van deze interventies zowel de bedoelde als de onbedoelde effecten goed te onderzoeken en duidelijke doelgroepen te beschrijven voor wie de interventies potentieel effectief zijn effectief zijn.

In de derde plaats bleek dat voor zowel jongere als oudere daders in verschillende fasen van de criminele loopbaan, maar met andere drijfveren dan nieuwsgierigheid en het zoeken van mentale uitdaging, traditionele interventies potentieel geschikt zijn. Dit betreft de interventies die zich richten op specifieke criminogene factoren (zoals verslaving, gebrek aan sociale vaardigheden of ondersteunende relaties). Deze interventies houden echter nog geen rekening met de responsiviteit van cyberdaders in de online context waardoor de effectiviteit voor deze doelgroep waarschijnlijk tegenvalt. Onze laatste aanbeveling is dan ook om na te gaan welke aanpassingen er in deze bestaande interventies nodig zijn om aan te sluiten bij de responsiviteit van cyberdaders.

Literatuurlijst

Aiken, M., Davidson, J., & Amann, D. (2016). *Youth pathways into cybercrime*. Europol: European Cybercrime Centre/UCD Geary institute for public policy /Middlesex University.

Akers, R.L. (1998). *Social learning and social structure: a general theory of crime and deviance*. Boston: Northeastern University Press.

Andrews, D. A., Zinger, I., Hoge, R. D., Bonta, J., Gendreau, P., & Cullen, F. T. (1990). Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis. *Criminology, 28(3)*, 369-404.

Andrews, D. A., & Dowden, C. (2005). Managing correctional treatment for reduced recidivism: A meta analytic review of program integrity. *Legal and Criminological Psychology, 10*(2), 173-187.

Andrews, D. A., Bonta, J., & Wormith, J. S. (2006). The recent past and near future of risk and/or need assessment. *Crime & Delinquency, 52*(1), 7-27.

Árpád, I. (2013). A greater involvement of education in fight against cybercrime. *Procedia – Social and Behavioral Sciences, 83*, 371-377.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1-2), 643-565.

Bae, S.M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review, 78*, 74-80.

Bentham, J. (1789). An introduction to the principles of morals and legislation. Londen: T. Payne and Son.

Bijlenga, N., & Kleemans, E.R. (2017). Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *European Journal on Criminal Policy and Research, 24*(3), 253-268.

Bonta, J., & Andrews, D.A. (2007). *Risk-Need-Responsitivity Model for Offender Assessment and Rehabilitation.* Ottawa: Carleton University/Public Safety Canada.

Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T. J. Holt & B. H. Schell (Reds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 38-67). Hershey: IGI Global

Brar, H.S., & Kumar, G. (2018). Cybercrimes: a proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, 1-11.

Brewer, R., Cale, J., Goldsmith, A & Holt, T. (2018). Young people, the internet and emerging pathways into criminality: a study of Australian adolescents. *International Journal of Cyber Criminology, 12*(1), 115-132.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Bruijne, M. de (2018). Hack_Right. Een interventie voor jonge, naïeve cybercriminelen. *Opportuun, 24*(2).

Bruinsma, G., Bernasco, W., & Elffers, H. (2010). Ruimtelijke verplaatsing van criminaliteit: theorie,

methodologie en empirie. In E. R. Muller, J. P. van der Leun, L. M. Moerings, & P. J. V. van Calster (Reds.), *Criminaliteit en criminaliteitsbestrijding in Nederland.* Alphen aan den Rijn: Kluwer.

Cassidy, W.E.M., Faucher, C., & Jackson, M. (2013). Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International, 34*(6), 575-612.

Cayubit, R.F.O., Rebolledo, K.M., Kintanar, R.G.A., Pastores, A.G., Santiago, A.J.A., & Valles, P.B.V. (2017). A cyber phenomenon: A Q-analysis on the motivation of computer hackers. *Psychological Studies, 62*(4), 386-394.

Chatfield, A.T., & Reddick, C.G. (2018). Crowdsourced cybersecurity innovation: The case of the Pentagon's vulnerability reward program. *Information Polity, 23*(2), 177-194.

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers. The science of criminal profiling as applied to the world of hacking.* Boca Raton: Auerbach Publications.

Cho, S-Y. (2016). *A crime 2.0: Cybercrime, e-talent, and institutions.* (Working Paper). Geraadpleegd van https://www.econstor.eu/handle/10419/129288

Choo, K.R. (2011). The cyber threat landscape: challenges and future research directions. *Computer & Security,* 30, 719-731.

Clarke, R.V.G., & Felson, M. (1993). *Routine activity and rational choice*. New Brunswick: Transaction Publishers.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Collins, K. (2018). Inside the bootcamp reforming teenage hackers. *CNET.* Geraadpleegd via https://www.cnet.com/news/inside-the-boot-camp-reforming-teenage-hackers/

Cornish, D.B., & Clarke, R.V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York: Transaction Publishers.

Dahan, M. (2013). *Hacking for the homeland: Patriotic hackers versus hacktivists.* Artikel gepresenteerd op The 8th International Conference on Information Warfare and Security, Denver, USA.

Dalal, A.S., & Sharma, R. (2007). Peeping into a hackers mind: Can criminological theories explain hacking? *The IUP Journal of Cyber Law,* 1-20.

Decorte, T., & Zaitch, D. (2016). *Kwalitatieve methoden en technieken in de criminologie*. Den Haag: Acco.

DeMarco, J. V. (2001). It's not just fun and war games juveniles and computer crime. *United States Attorneys' Bulletin, 49*(3), 48-55.

Donner, C.M., Jennings, W.G., & Banfield, J. (2015). The general nature of online and off-line offending among college students. *Social Science Computer Review, 33*(5), 663-679.

Dremliuga, R. (2014). Subculture of hackers in Russia. *Asian Social Science, (10)*8, 158-162.

Dupont, B. (2014). Skills and trust: A tour inside the hard drives of computer hackers. In C. Morselli (Red.), *Crime and Networks* (pp. 195-216). New York: Routledge.

Eisenberg, N., Sadovsky, A., Spinrad, T.L., Fabes, R.A.& Losoya, S.H. (2005). The relations of problem behavior status to children's negative emotionality, effortful control, and impulsivity: concurrent relations and prediction of change. *Dev Psychol, 41*, 193–211.

Floyd, K., Harrington, S.J., & Hivale, P. (2007). *The autotelic propensity of types of hackers*. Artikel

gepresenteerd op InfoSecCD '07 Proceedings of the 4th annual conference on Information security curriculum development, Kennesaw, USA.

Furnell, S. (2009). Hackers, viruses and malicious software. In Y. Jewkes & M. Yar (Reds.), H*andbook of Internet Crime* (pp. 173-193). London: Routledge.

Gibbs, J. (1975). *Crime, Punishment and Deterrence*. New York: Elsevier.

Giodarno, P.C., Cernkovich, S.A., & Rudolph, J.L. (2002). Gender, crime, and desistance: Toward a theory of cognitive transformation. *American Journal of Science, 107*(4), 990-1064.

Goldman, Z.K., & McCoy, D. (2016). Deterring financially motivated cybercrime. *Journal of National Security Law & Policy, 8,* 595-619.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology, 19*(1), 112-130.

Goode, S., & Cruise, S. (2006). What motivates software crackers? *Journal of Business Ethics, 65*(2), 173-201.

Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime.* California: Stanford University Press.

Hald, S.L.N., & Pedersen, J.M. (2012). *An updated taxonomy for characterizing hackers according to their threat properties.* Artikel gepresenteerd op 14th International Conference on Advanced Communication Technology, PyeongChang, Korea.

Hampson, K.S. (2018) Desistance approaches in youth justice – The next passing fad or a sea-change for the positive? *Youth Justice, Vol. 18*(1), 18–33.

Henson, B. Zwartz, K., & Reyns, B.W. (2017). #Respect: Applying Anderson's code of the street to the online context. *Deviant Behavior, 38*(7), 768-780.

Heeramun, R., Magnusson, C., Gumpert, C., Granath, S., Lundberg, M. Dalman,C., Rai, D. (2017). Autism and Convictions for Violent Crimes: Population-Based Cohort Study in Sweden. *Journal of the American Academy of Child & Adolescent Psychiatry* 2017; 56(6): 491–497.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley: University of California Press.

Hoek van Dijke, N. (2016). *Onderzoeksrapportage. Jongeren over cybercrime en gedigitaliseerde criminaliteit*. Den Haag: Ministerie van Justitie en Veiligheid.

Holt, T.J. (2005). *Hacks, cracks, and crime: an examination of the subculture and social organization of computer hackers* (Proefschrift). Geraadpleegd van https://irl.umsl.edu/dissertation/616/

Holt, T.J., & Kilger, M. (2008). *Techcrafters and makecrafters: a comparison of two populations of hackers.* Artikel gepresenteerd op 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing, Amsterdam, Nederland.

Holt, T.J., Bossler, A.M., & May, D.C. (2012). Low self-control, deviant peer associations and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378-395.

Holt, T.J., Burruss, G.W., & Bossler, A.M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime & Justice, 33*(2), 31-61.

Holt, T.J., Freilich, J.D., & Chermak, S.M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice, 33*(3), 212-233.

Holt, T.J., Kilger, M., Chiang, L., & Yang, C-S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behaviour, 38*(3), 356-373.

Howell, C.J., Cochran, J.K., Powers, R.A., Maimon, D., & Jones, H.M. (2017). System trespasser behavior

after exposure to warning messages at a Chinese computer network: an examination. *International Journal of Cyber Criminology, 11*(1), 63-77.

Hulst, R.C. van der & Neve, R.J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie.* Den Haag: Boom Juridische Uitgevers/WODC.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 61*(1), 1-20.

Hutchings, A. (2016). Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T.J. Holt (Red.), *Crime online: correlates, causes, and context* (pp. 117-140). Durham: Carolina Academic Press.

Hutchings, A., & Holt, T.J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*(1), 11-30.

Jelsma, Y. (2017). *Still Hacking Anyway: Een onderzoek naar de hackercultuur en differentiatie binnen de Nederlandse hackergemeenschap* (Masterscriptie).

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Kaal, H.L. (2016). *Notitie: Prevalentie licht verstandelijke beperking in het justitiedomein.* Leiden: Hogeschool Leiden.

Kao, D-Y., Huang, F.F-Y & Wang, S-J. (2009). Persistence and desistance: examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law & Security Review, 25*(5), 464-476.

Katz, J. (1988). *Seductions of Crime: Moral and sensual attractions in doing evil*. New York: Basic Books.

Keizer, S. (2019). *Wat te doen met de jonge cyberdaders? Een kwalitatief vergelijkingsonderzoek tussen Nederland en het Verenigd Koninkrijk naar de interventies voor jonge daders van cybercrime in enge zin* (Masterscriptie).

Kerstens, J., & Stol, W. (2012). *Jeugd en cybersafety. Online slachtoffer- en daderschap onder Nederlandse jongeren.* Den Haag: Boom Lemma Uitgevers.

Khey, D.N., Jennings, W.G., Lanza-Kaduce, L., & Frazier, C.E. (2009). An exploration into the factors associated with specialization among college student computer criminals. *Criminal Justice Studies, 22*(4), 4210-434.

King, C., & Murphy, G.H. (2014). A systematic review of people with autism spectrum disorder and the criminal justice system. *Journal of Autism and Developmental Disorders, 44*(11): 2717-2133.

Kirwan, G., & Power, A. (2013). *Cybercrime: the psychology of online offenders*. Cambridge: Cambridge University Press.

Kleck, G., Sever, B., Li, S., & Gertz, M. (2005). The missing link in general deterrence research. *Criminology*, *43*(3), 623-660.

Koppen, M.V. van, Poot, C.J., de, Kleemans, E.R., & Nieuwbeerta, P. (2010). Criminal trajectories in organized crime. *The British Journal of Criminology, 50*(1), 102-123.

Kroese, G.J., & Staring, R.H.J.M. (1993). *Prestige, professie en wanhoop. Een onderzoek onder gedetineerde overvallers.* Arnhem: Gouda Quint.

Krohn, M.D., Thornberry, T.P., Gibson, C.L., & Baldwin, J.M. (2010). The development and impact of self-report measures of crime and delinquency. *Journal of Quantitative Criminology, 26*(4), 509-525.

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R. Roks, R.A., Kouwenberg, R.J., Nabi, S.S., Fiorito, T., &

Ruitenburg, T. van (2018). *Georganiseerde criminaliteit en ICT. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde misdaad.* Den Haag/Amsterdam: WODC/NSCR.

Laan, A.M. van der & Goudriaan, H. (2016). *Monitor jeugdcriminaliteit. Ontwikkelingen in de jeugdcriminaliteit 1997 tot 2005.* Den Haag: WODC.

Laan, A.M. van der, Beerthuizen, M.G.C.J., & Weijters, G. (2016). Jeugdige daders van online-criminaliteit. *Cahier Politiestudies, 4*(41), 145-168.

Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism, 1*(1), 2-11.

Leukfeldt, E.R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime, 17*(4), 231-249.

Leukfeldt, E.R., & Weulen Kranenbarg, M. (2017). De menselijke factor in cybercrime. *Tijdschrift voor Criminologie, 59*(3), 282-290.

Leukfeldt, E.R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Leukfeldt, E.R., Domenie, M.M.L., & Stol, W. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Uitgevers.

Leukfeldt, E.R., Kleemans, E.R., & Stol, W. (2017a). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21-37.

Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017b). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks*. The British Journal of Criminology, 57*(3), 704-722.

Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017c). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39-53.

Leukfeldt, R., Veenstra, S., Domenie, M., & Stol, W. (2012). *De strafrechtketen in een gedigitaliseerde samenleving: Een onderzoek naar de strafrechtelijke afhandeling van cybercrime*. Leeuwarden: Lectoraat Cybersafety.

Levin, R., Richardson, J., Warner, G., & Kerley, K. (2012). *Explaining cybercrime through the lens of differential association theory, Hadidi44-2.php Paypal Case Study*. Artikel gepresenteerd op 2012 eCrime Researchers Summit, Las Croabas, Verenigde Staten.

Li, X. (2008). The criminal phenomenon on the internet: hallmarks of criminals and victims revisited through typical cases prosecutes. *University of Ottawa Law & Technology Journal*, *5*(1-2), 125-140.

Lickiewicz, J. (2013). The perpetrators of computer crimes as a heterogeneous group. *Problems of Forensic Sciences, 93*, 391-403.

Lipsey, M. W., & Cullen, F. T. (2007). The effectiveness of correctional rehabilitation: A review of systematic reviews. *Annual Review of Law and Social Science, 3*, 297-320.

Lowenkamp, C.T., Latessa, E.J., Holsinger, A.M. (2006). The Risk Principle in Action: What Have We Learned From 13,676 Offenders and Correctional Programs? *Crime & Delinquency, 52*(1), 77-93

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology, 52*(1), 33-59.

Marcum, C.D., Higgins, G.E. & Tewksbury, R. (2012). Incarceration or community placement: examining

the sentences of cybercriminals. *Criminal Justice Studies, 25*(1), 33-40.
Marcum, C.D., Higgins, G.E., Ricketts, M.L., & Wolfe, S.E. (2014). Hacking in high school: Cybercrime perpetration by juveniles*. Deviant Behavior, 35*(7), 581-591.
Maruna, S., & Farrall, S. (2004). Desistance from crime: A theoretical reformulation. *Kolner Zeitschrift fur Soziologie und Sozialpsychologie* 43, 171–194.
Maruna, S., & Toch, H. (2005) The impact of imprisonment on the desistance process. In J. Travis & C. Visher (Reds.), *Prisoner Reentry and Crime in America* (pp. 139-178). New York: Cambridge University Press.
Matthijsse, S.R. (2017). *De hacker: computergenie of crimineel. Een kwalitatief onderzoek naar de framing van hackers in het Nederlandse nieuws* (Masterscriptie).
McMurran, M., & Ward, T. (2010). Treatment readiness, treatment engagement and behaviour change. *Criminal Behaviour and Mental Health, 20*(2), 75-85.
McNeill, F. (2012). Four forms of 'offender' rehabilitation: Towards an interdisciplinary perspective. *Legal and Criminological Psychology, 17*(1), 18-36.
McNeill, F. (2016). Desistance and criminal justice in Scotland. In H. Croall, G. Mooney en R. Munro (Reds.) *Crime, Justice and Society in Scotland* (pp. 200-216). London: Routledge.
McNeill, F., Anderson, K., Colvin, S., Overy, K., Sparks, R., & Tett, L. (2011). Kunstprojecten en 'what works'; een stimulans voor desistance? *Justitiële verkenningen, 37*(5), 80–101.
McNeill, F., Farrall, S., Lightowler, C., & Maruna, S. (2012). Reexamining evidence-based practice in community corrections: Beyond 'a confined view' of what works. *Justice Research and Policy 14*(1), 35–60.
Merkom, J. van (2017). *De digitale criminele school? Een kwalitatief onderzoek naar differentiële associatie op een hackers forum* (Masterscriptie).
Miller, B., & Morris, R.G. (2014). Virtual Peer Effects in Social Learning Theory. *Crime & Delinquency, 62*(12), 1543-1569.
Moerland, H. (1991). *Winkeldiefstal, een te riskante zaak?*. Arnhem: Gouda Quint.
Moffitt, T.E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review, 100*(4), 674-701.
Morris, R.G. (2010). Computer hacking and the techniques of neutralization: an empirical assessment. In USA Information Resources Management Association (Red*.), Cyber Crime: Concepts, methodologies, tools and applications* (pp-457-473). Pennsylvania: IGI Global.
Morris, R.G., & Blackburn, A.G. (2009). Cracking the code: an empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice, 31*(1), 1-34.
National Crime Agency (2017). *Pathways into cyber crime*. Geraadpleegd op 15 oktober 2018 van https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file/
NCSC (2013). *Leidraad om te komen tot een praktijk van Responsible Disclosure*. Den Haag: NCSC.
NCSC (2018). *Coordinated vulnerability disclosure: De leiddraad*. Den Haag: NCSC.
Nodeland, B., & Morris, R. (2018). A test of social learning theory and self-control on cyber offending. *Deviant Behavior*, 1-16.
Nycyk, M. (2016). The new computer hacker's quest and context with the experienced hackers: a

qualitative study applying Pierre Bourdieu's field theory. *International Journal of Cyber Criminology, 10*(2), 92-109.

Odinot, G., Verhoeven, M.A., Pool, R.L.D., & Poot, D.J. de (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Den Haag: WODC.

Oerlemans, J.J. (2017b). De wet computercriminaliteit III: meer handhaving op internet. *Strafblad, 4*(15), 350-359.

Ogilvie, J.M., Stewart, A.L., Chan, R.C.K., & Shum, D. (2011). Neuropsychological measures of executive function and antisocial behavior: A meta-analysis. *Criminology*, *49*(4), 1063–1107.

Oldegarm, P., & Holterman, L. (Reds.) (2019). *Cybersecurity woordenboek. Van cybersecurity naar Nederlands.* Naarden: Cyberveilig Nederland.

Oosterwijk, K., & Fischer, T.F.C. (2017). *Interventies jeugdige daders cybercrime*. Den Haag: WODC

Paternoster, R. McGloin, J.M., Nguyen, H., & Thomas, K.J. (2012). The causal impact of exposure to deviant peers: An experimental investigation. *Journal of Research in Crime and Delinquency, 50*(4), 476-503.

Petticrew, M., & Roberts, H. (2006). *Systematic Reviews in the Social Sciences. A Practical Guide*. Oxford: Blackwell Publishing

Politie (2019, 14 februari). Jongeren één klik verwijderd van cybercrime. Geraadpleegd op 2 april 2019 van https://www.politie.nl/nieuws/2019/februari/13/00-9456-jongeren-een-klik-verwijderd-van-cybercrime.html/

Popma, A., & Doreleijers, T. (2019). *GAST!* Eindrapport: H.E.T. Onderzoek Academische Werkplaats bij De Nieuwe Kans.

Preuß, J., Furnell, S.M., & Papadaki, M. (2007). Considering the potential of criminal profiling to combat hacking. *Journal of Computer Virology, 3*(2), 135-141.

Rege, A. (2012). *Cybercrimes against the electricity infrastructure: exploring hackers and industry perceptions* (Proefschrift). Geraadpleegd van http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.870.6948&rep=rep1&type=pdf

Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies, 22*(3), 261-271.

Richet, J. (2013). From young hackers to crackers. *International Journal of Technology and Human Interaction, 9*(3), 53-62.

Rieb, A., Gurschler, T., & Lechner, U. (2017). A gamified approach to explore techniques of neutralization of threat actors in cybercrime. In E. Schweighofer, H. Leitold, A. Mitrakas, & K. Rannenberg (Reds.), *Privacy Technologies and Policy* (pp. 87-103), Wenen: Springer International Publishing.

Rogers, M.K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study* (Proefschrift). Geraadpleegd van https://mspace.lib.umanitoba.ca/xmlui/handle/1993/19563

Rogers, M.K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigations, 3*(2), 97-102.

Rogers, M.K. (2010). The psyche of cybercriminals: a psycho-social perspective. In S. Ghosh & E. Turrini (Reds.), *Cybercrimes: A Multidisciplinary analysis* (pp. 217-235). Heidelberg: Springer.

Rogers, M.K., Smoak, N.D., & Liu, J. (2006). Self-reported deviant computer behavior: A Big-5, moral

choice, and manipulative exploitive behavior analysis. *Deviant Behavior, 27*(3), 245-268.
Rokven, J.J., Weijters, G., & Laan, A.M. van der (2017). *Jeugddelinquentie in de virtuele wereld. Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?* Den Haag: WODC.
Rokven, J. J., Boer, G. de, Tolsma, J., & Ruiter, S. (2017). How friends' involvement in crime affects the risk of offending and victimization. *European Journal of Criminology, 14*(6), 1-23
Ruiter, S., & Bernaards, F. (2013). Verschillen crackers van andere criminelen? Een vergelijking op basis van Nederlandse verdachtenregistraties. *Tijdschrift voor Criminologie, 55*(4), 342-359.
Ryan, R.M., & Deci, E.L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55*(1), 68-78.
Sampson, R.J., & Laub, J.H. (2005). A life-course view of the development of crime. *ANNALS of the American Acadamy of Political and Social Science, 602*, 12-45.
Schell, B.H., & Holt, T.J. (2010). A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer hacker insiders and outsiders. In T.J. Holt & B.H. Schell (Reds.), *Corporate hacking and technology driven crime: Social dynamics and implications* (pp. 190-213*)*. Hershey, PA: IGI Global.
Schell, B. H., & Melnychuk, J. (2010). Female and male hacker conference attendees: Their autism-spectrum quotient (AQ) scores and self-reported adulthood experiences. In T. J. Holt & B. H. Schell (Reds.), *Corporate hacking and technology driven crime: Social dynamics and implications* (pp. 144 - 169). Hershey, PA: IGI Global.
Schuiringa, H., Nieuwenhuijzen, M. van, Orobio de Castro, B., & Matthys, W. (2017). Executive functions and processing speed in children with mild to borderline intellectual disabilities and externalizing behavior problems. *Child Neuropsychology*, *23*(4), 442–462.
Seebruck, R. (2015). A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45.
Seigfried-Spellar, K.C., & Treadway, K.N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior, 35*(10), 782-803.
Seigfried-Spellar, K.C., O'Quinn, C.L., & Treadway, K.N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology, 34*(5), 533-542.
Siponen, M., Vance, A. & Willison, R. (2012). New insights into the problem of software piracy: the effects of neutralization, shame and moral beliefs. *Information & Management, 49*(7-8), 334-341.
Smith, G.S. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1), 104-125.
Smith, R., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial.* Port Melbourne: Cambridge University Press.
Smit, P.R., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, Bongers, F., Kabki, A., Zaitch, D. (2018). *Tasten in het duister*. *Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten - Deel 1: Hoofdrapport.* Den Haag: WODC/Dialogic.
Staa, A. van & Evers (2015). Thick analysis. Strategie om de kwaliteit van kwalitatieve analyse te verbeteren, *Kwalon, 15*(1), 5-12.

Stambaugh, H., Beuapre, D.S., Icove, D.H., Baker, R., Cassady, W., & William W.P. (2001). *Electronic crime needs assesment for state and local law enforcement.* Washington: National Institute of Justice.

Stanton, J. (2019). *NCA Cyber Choices lesson Plan*. Geraadpleegd via https://www.cybersecuritychallenge.org.uk/education/schools/parents

Steinmetz, K.F. (2015a). Craft(y)ness. An ethnographic study of hacking. *The British Journal of Criminology, 55*(1), 125-145.

Steinmetz, K.F. (2015b). Becoming a hacker: demographic characteristics and developmental factors. *Journal of Qualitative Criminal Justice and Criminology, 3*(1), 31-60.

Steinmetz, K.F. (2017). Ruminations on warning banners, deterrence and system intrusion research. *Criminology & Public Policy, 16*(3), 727-737.

Steinmetz, K.F., Schaefer, B.P., & Green, E.L.W. (2017). Anything but boring: A cultural criminological exploration of boredom. *Theoretical Criminology, 21*(3), 342-360.

Suler, H. (2004). The online disinhibition effect. *Cyberpsychology & Behavior, (7)*3, 321-236.

Sutherland, E.H. (1947). *Principles of criminology*. Oxford: J.B. Lippincott.

Sykes, G.M., & Matza, D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Tanczer, L.M. (2017). The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists. In M. Conway, L. Jarvis, O. Lehane, S. Macdonald & L. Nouri (Reds.), *Terrorists' Use of the Internet* (pp. 77-92). Amsterdam: IOS Press.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers. Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy, 16*(3), 689-726.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

Turkle, S. (1984). The second self: computers and the human spirit. New York: Simon & Schuster.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology, 10*(2), 127-146.

Vermaas, P. (2018). Actiedag DDoS-aanvallen. *Opportuun, 02*.

Wagen, W. van der (2018). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime offenders and victims through the lens of Actor-Network Theory* (Proefschrift). Geraadpleegd van https://www.rug.nl/research/portal/publications/from-cybercrime-to-cyborg-crime(f3a5c5e0-ff0f-4dad-ac6c-2bc91d96a1b4).html

Wagen, W. van der, Althoff, M., & Swaaningen, R. van (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur & Criminaliteit, (6)*1, 27-41.

Ward, M. (2017). Rehab camp aims to put young cyber-crooks on right track. *BBC*. Geraadpleegd via https://www.bbc.com/news/technology-40629887

Warr, M. (2002). *Companions in Crime. The social aspects of criminal conduct.* New York: Cambridge University Press.

Wegberg, R. van, & Verburgh, T. (2018). *Evolution of the Darknet*. Workshop gegeven op The Web Science Conference (WebSci), Amsterdam, Nederland.

Weerman, F.M. (2011). Delinquent peers in context: a longitudinal network analysis of selection and influence effects. *Criminology, 49*(1), 253-286.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: an empirical comparison* (Proefschrift). Geraadpleegd van http://dare.ubvu.vu.nl/handle/1871/55530?show=full

Weulen Kranenbarg, M., Ruiter, S., Van Gelder J., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life Course Criminology 4*(3)*,* 343–364.

Wible, B. (2003). A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. *The Yale Law Journal, 112*(6), 1577-1623.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency, 52*(6), 829-955.

Woo, H-J. (2003). *The hacker mentality: exploring the relationship between psychological variables and hacking activities* (Proefschrift). Geraadpleegd van https://pdfs.semanticscholar.org/3302/e173939ae434ad30f91d4c60d69f5e4a05e3.pdf

Woo, H.J., Kim, Y., & Dominick, J. (2004). Hackers: militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology, 6*(1), 63-82.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64-74.

Yar, M. (2005). Computer hacking: just another case of juvenile delinquency? *The Howard Journal, 44*(4), 387-399.

Akhgar, B., & Yates, S. (2011). *Intelligence management. Knowledge driven frameworks for combating terrorism and organized crime*. Londen: Springer-Verlag.

Zand, E.G. van 't (2017). *Invisible bars: The impact of having a criminal record on young adults' position in the labour market* (Proefschrift). Geraadpleegd van https://dspace.library.uu.nl/handle/1874/357001

Zebel, S., Vries, P. de, Giebels, E., Kuttschreuter, M., & Stol, W. (2013). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*. Den Haag: WODC.

Bijlage 1A Zoektermenreeksen systematische review

Tabel 1 Ontwikkeling algemene cyber zoektermreeks systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie a.d.h.v. de zoekreeks in het onderzoeksvoorstel	(“cybercriminal*” OR “cyber offender*” OR “cyber deviant*” OR “cyber delinquent*” OR “cybercriminal actor*” OR “hacker*” OR “cracker*” OR “malware writer*” OR “virus writer*” OR “online offender*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 11,984
2	Termen toegevoegd	(“cybercriminal*” OR “cyber offender*” OR “cyber deviant*” OR “cyber delinquent*” OR “cybercriminal actor*” OR “hacker*” OR “cracker*” OR “malware writer*” OR “virus writer*” OR “online offender*” OR “online perpetrator*” OR “internet criminal*” OR “internet offender*” OR “virtual criminal*” OR “ict criminal*” OR “computer criminal*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 12,129
3	In relevante literatuur naar mogelijk relevante zoektermen gezocht en deze toegevoegd	(“cybercriminal*” OR “cyber offender*” OR “cyber deviant*” OR “cyber delinquent*” OR “cybercriminal actor*” OR “hacker*” OR “cracker*” OR “malware writer*” OR “virus writer*” OR “online offender*” OR “online perpetrator*” OR “internet criminal*” OR “internet offender*” OR “virtual criminal*” OR “ict criminal*” OR “computer criminal*” OR “black hat*” OR “black hat hacker*” OR “hacktivist*” OR “carder*” OR “bot herder*” OR “skimmer*” OR “spammer*” OR “fraudster*” OR “scriptkidd*” OR “cybervandal*” OR “ddos*” OR “defacement*” OR “cyberpunk*” OR “computer felon*” OR “high tech crime*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 21,260
4	Getest of het verplaatsen van de asterisk nog andere relevante resultaten oplevert	(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack*” OR “crack*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “black hat*” OR “black hat hack*” OR “hacktivis*” OR “carder*” OR “bot herd*” OR “skimm*” OR “spam*” OR “fraudster*” OR “scriptkidd*” OR “cyber vandal*” OR “ddos*” OR “defac*” OR “cyberpunk*” OR “computer felon*” OR “high tech crim*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 493,934
5	Niet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen. Zo is “hack*” vervangen voor “hack”, “hacker*” en “hacking*” om niet relevante literatuur (zoals bijvoorbeeld auteurnamen	(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*”	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 44,772

	zoals Hackman en Hackett) eruit te filteren en toch de relevante resultaten te behouden. Hiernaast is “skimm*” vervangen voor “skimming*” om niet-relevante resultaten over o.a. skimmed milk eruit te filteren en de relevante resultaten te behouden.	OR “bot* herd*” OR “skimming*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “script kidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high-tech crim*”)	
6	Met zoekreeks #5 is verder gewerkt.		

Tabel 2 Ontwikkeling zoektermreeks persoonskenmerken systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“personal character*” OR “character*” OR “individual character*” OR “offender character*” OR “demograph*” OR “categor*” OR “taxonom*” OR “profiling*” OR “offender profil*” OR” typolog*” OR “classif*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 9,451
2	Termen toegevoegd	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“personal character*” OR “character*” OR “individual character*” OR “offender character*” OR “demograph*” OR “categor*” OR “taxonom*” OR “profil*” OR “offender profil*” OR “crim* profil*” OR ”typolog*” OR “classif*” OR “personalit*” OR “age*” OR “gender*” OR “ethnicit*” OR “education*” OR “ethnograph*” OR “differen*” OR “psycholog*” OR “forensic*” OR “circumplex*” OR “type*” OR ”mental*” OR “personae*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 22,951
3	Niet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen. De term “character*” in het algemeen levert veel niet-relevante resultaten op. Dus is gekozen om de term te specificeren o.b.v. termen uit de relevante literatuur, waarbij is gecheckt of de relevante literatuur nog steeds naar bovenkomt. Hetzelde geldt voor “category*”, “taxonom*” en “profil*”.	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“case character*” OR “personal* trait*” OR “crim* character*” OR “cyber* character*” OR “psych* character*” OR “predisposition*” OR “crim* categor*” OR “categor* cyber*” OR “category* of cyber*” OR “cyber* taxonom*” OR “hack* taxonom*” OR “offend* profil*” OR “crim* profil*” OR ”typolog*” OR “ethnography*”) AND NOT (“porn*” OR “sex*” OR “bully*” OR “piracy*” OR “victim*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 147
4	Met zoekreeks #3 is verder gewerkt.		

Tabel 3 Ontwikkeling zoektermreeks problematiek & criminogene- en protectieve factoren systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“risk*” OR “risk factor*” OR “protective factor*” OR “promotive factor*” OR “determinant*” OR “self control*” OR “self-control*” OR “online disinhibition*” Or “anonym*”OR “impulsive*” OR “guardian*” OR “peer*” OR “famil*” OR ”communit*” OR “school*” OR “biolog*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 8,092
2	Termen toegevoegd	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“risk*” OR “risk factor*” OR “protective factor*” OR “promotive factor*” OR “determinant*” OR “self control*” OR “self-control*” OR “online disinhibition*” Or “anonym*”OR “impulsive*” OR “guardian*” OR “peer*” OR “famil*” OR ”communit*” OR “school*” OR “biolog*” OR “neigbour*” OR “neighbor*” OR “routine activit*” OR “opportunit*” OR “subculture*” OR “impulsiv*” OR “rational choice*” OR “social learn*” OR “predict*” OR “problem*” OR “general theory*” OR “autism*” OR “autistic*” OR “antisocial*” OR “ behavior*” OR “behaviour*” OR “cause*” OR “time spent*” OR “attachment*” OR “disorganiz*” OR “psycho*” OR “tie*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 21,340
3	Niet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen.	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY (“risk assesment*” OR “risk factor*” OR “protective factor*” OR “promotive factor*” OR “self-control*” OR “online disinhibition*” OR “guardian*” OR “routine activit*” OR “subculture*” OR “impulsiv*” OR “rational choice*” OR “social learn*” OR “differential association*” OR “predictor*” OR “general theory*” OR “autism*” OR “antisocial*” OR “psych*” OR “addict*” OR “disengage*”) AND NOT (“victim*” OR “victimization*” OR “piracy*” OR “porn*” OR “sex*” OR “protection*” OR “ian hacking*” OR “bully*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 472
4N	iet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen. De term “psych*” is gespecificeerd om niet-relevante literatuur eruit te filteren.	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY (“risk factor*” OR “protective factor*” OR “self-control*” OR “online disinhibition*” OR “guardian*” OR “routine activit*” OR “subculture*” OR “rational choice*” OR “social learn*” OR “differential association*” OR “autism*” OR “antisocial*” OR “psych* profil*” OR “psychopathology*” OR “social psych*” OR “crim* psych*” OR “psychological theor*” OR “addict*” OR “criminogenic*”) AND NOT (“victim*” OR “victimization*” OR “piracy*” OR “porn*” OR “sex*” OR “protection*” OR “ian hacking*” OR “bully*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 167
5	Met zoekreeks #4 is verder gewerkt.		

Tabel 4 Ontwikkeling zoektermreeks criminele carriere systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY("life-course persistent*" OR "adolescence-limited*" OR "crim* career*" OR "onset*" OR "initiat*" OR "persist*" OR "deter*" OR "life event*" OR "turning point*" OR "maturation*" OR "offending frequenc*" OR "duration*" OR "traject*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 5,214
2	Niet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen.	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY("life-course*" OR "adolescence-limited*" OR "criminal career*" OR "age of onset*" OR "desistance*" OR "life event*" OR "turning point*" OR "offen* frequenc*" OR "barrier to entr*" OR "crim* type*" OR "offen* type*") AND NOT ("porn*" OR "sex*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 38
3	Met zoekreeks #2 is verder gewerkt.		

Tabel 5 Ontwikkeling zoektermreeks modus operandi systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY ("modus operand*" OR "method*" OR "technique*" OR "target*" OR "attack*" OR "strateg*" OR "avoid*" OR "crime script*" OR "offender convergen*" OR "IT knowledge*" OR "ICT knowledge*" OR "technolog* knowledge*" OR "IT skill*" OR "ICT skill*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 30,484
2	Termen toegevoegd	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY ("modus operandi*" OR "crime script*" OR "offender convergen*" OR "IT knowledge*" OR "ICT knowledge*" OR "technolog* knowledge*" OR "IT skill*" OR "ICT skill*" OR "computer knowledge*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 104
3	Aanvullingen uit relevante literatuur	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY ("modus operandi*" OR "crime script*" OR "offender convergen*" OR "ICT knowledge*" OR "technolog* skill*" OR "IT skill*" OR "crim* path*" OR "skill* set*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 114
4	Met zoekreeks #3 is verder gewerkt.		

Tabel 6 Ontwikkeling zoektermreeks drijfveren & neutralisaties systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY ("motiv*" OR "motif*" OR "revenge*" OR "curious*" OR "fun*" OR "financial gain*" OR "money*" OR "ideolog*" OR "hack* ethic*" OR "peer*" OR "neutraliz*" OR "neutralis*" OR "technique* of neutraliz*" OR "technique* of neutralis*" OR "denial*")	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 10,535

2	Termen aangepast	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY (“motivation*” OR “motive*” OR “revenge*” OR “curious*” OR “curios*” OR “fun” OR “financial gain*” OR “prank*” OR “ideolog*” OR “hack* ethic*” OR “technique* of neutraliz*” OR “technique* of neutralis*”) AND NOT (“victimization*” OR “porn*” OR “sex*” OR ”bully*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 792
3	Niet-relevante resultaten eruit gefilterd door de zoekreeks aan te passen. Zo is “financial gain*” eruit gefilterd omdat dit geen relevante resultaten opleverde. De termen “motivation*” en “motive*” zijn gespecificeerd om de niet-relevante literatuur eruit te filteren.	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY (“motiv* factor*” OR “crim* motiv*” OR “attack* motiv*” OR “motiv* to hack*” OR “underlying* motiv*” OR “hack* motiv*” OR “motiv* perspective*” OR “motiv* of hack*” OR “revenge*” OR “pleasure*” OR “curious*” OR “curios*” OR “prank*” OR “ideolog*” OR “hack* ethic*” OR “technique* of neutraliz*” OR “technique* of neutralis*”) AND NOT (“victimization*” OR “porn*” OR “sex*” OR ”bully*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 288
4	Met zoekreeks #3 is verder gewerkt.		

Tabel 7 Ontwikkeling zoektermreeks drijfveren & neutralisaties systematische review

	Wat	Zoektermen	Resultaten
1	Eerste inventarisatie	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“differen*” OR “traditional offen*” OR “traditional crim*” OR ”offline*” OR “contrast*” OR “similar*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 11,346
2	Termen aangepast	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY(“traditional offen*” OR “traditional crim*” OR “traditional typ* of crim*” OR ”offline crim*” OR “old wine*” OR “new wine*”)	Resultaten Scopus o.b.v. zoeken naar titel, abstract & keywords: 75
3	Met zoekreeks #2 is verder gewerkt.		

Tabel 8 Uiteindelijke zoektermenreeksen systematische review

	Wat	Zoektermen	Resultaten
1	Algemene cyber searchstring + persoonskenmerken searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot* herd*” OR “skimming*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “script kidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high-	Resultaten internationale databases o.b.v. zoeken naar titel, abstract & keywords: 351

		tech crim*”) AND TITLE-ABS-KEY(“case character*” OR “personal* trait*” OR “crim* character*” OR “cyber* character*” OR “psych* character*” OR “predisposition*” OR “crim* categor*” OR “categor* cyber*” OR “category* of cyber*” OR “cyber* taxonom*” OR “hack* taxonom*” OR “offend* profil*” OR “crim* profil*” OR ”typolog*” OR “ethnography*”) AND NOT (“porn*” OR “sex*” OR “bully*” OR “piracy*” OR “victim*”)	
2	Algemene cyber searchstring + Problematiek & criminogene- en protectieve factoren searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot herd*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high tech crim*”) AND TITLE-ABS-KEY (“risk factor*” OR “protective factor*” OR “self-control*” OR “online disinhibition*” OR “guardian*” OR “routine activit*” OR “subculture*” OR “rational choice*” OR “social learn*” OR “differential association*” OR “autism*” OR “antisocial*” OR “psych* profil*” OR “psychopathology*” OR “social psych*” OR “crim* psych*” OR “psychological theor*” OR “addict*” OR “criminogenic*”) AND NOT (“victim*” OR “victimization*” OR “piracy*” OR “porn*” OR “sex*” OR “protection*” OR “ian hacking*” OR “bully*”)	Resultaten internationale databases o.b.v. zoeken naar titel, abstract & keywords: 636
3	Algemene cyber searchstring + criminele carriere searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot* herd*” OR “skimming*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “script kidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high-tech crim*”) AND TITLE-ABS-KEY(“life-course*” OR “adolescence-limited*” OR “criminal career*” OR “age of onset*” OR “desistance*” OR “life event*” OR “turning point*” OR “offen* frequenc*” OR “barrier to entr*” OR “crim* type*” OR “offen* type*”) AND NOT (“porn*” OR “sex*”)	Resultaten internationale databases o.b.v. zoeken naar titel, abstract & keywords: 87
4	Algemene cyber searchstring + modus operandi searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR	Resultaten internationale databases o.b.v. zoeken

		“cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot* herd*” OR “skimming*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “script kidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high-tech crim*”) AND TITLE-ABS-KEY (“modus operandi*” OR “crime script*” OR “offender convergen*” OR “ICT knowledge*” OR “technolog* skill*” OR “IT skill*” OR “crim* path*” OR “skill* set*”)	naar titel, abstract & keywords: 213
5	Algemene cyber searchstring + drijfveren & neutralisaties searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot herd*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high tech crim*”) AND TITLE-ABS-KEY (“motiv* factor*” OR “crim* motiv*” OR “attack* motiv*” OR “motiv* to hack*” OR “underlying* motiv*” OR “hack* motiv*” OR “motiv* perspective*” OR “motiv* of hack*” OR “revenge*” OR “pleasure*” OR “curious*” OR “curios*” OR “prank*” OR “ideolog*” OR “hack* ethic*” OR “technique* of neutraliz*” OR “technique* of neutralis*”) AND NOT (“victimization*” OR “porn*” OR “sex*” OR ”bully*”)	Resultaten internationale databases o.b.v. zoeken naar titel, abstract & keywords: 702
6	Algemene cyber searchstring + verschillen met traditionele daders searchstring	TITLE-ABS-KEY(“cybercrim*” OR “cyber crim*” OR “cyber offen*” OR “cyber devian*” OR “cyber delinquen*” OR “cybercrim* actor*” OR “hack” OR “hacker*” OR “hacking*” OR “malware writ*” OR “virus writ*” OR “online offen*” OR “online perpetrat*” OR “internet crim*” OR “internet offen*” OR “virtual crim*” OR “ict crim*” OR “computer crim*” OR “hacktivis*” OR “bot* herd*” OR “skimming*” OR “online fraud*” OR “internet fraud*” OR “scriptkidd*” OR “script kidd*” OR “cyber vandal*” OR “web* defacement*” OR “cyberpunk*” OR “computer felon*” OR “high-tech crim*”) AND TITLE-ABS-KEY(“traditional offen*” OR “traditional crim*” OR “traditional typ* of crim*” OR ”offline crim*” OR “old wine*” OR “new wine*”)	Resultaten internationale databases o.b.v. zoeken naar titel, abstract & keywords: 151
			Totaal: 2140

Tabel 9 Zoektermreeks interventies systematische review

	Wat	Zoektermen
1	Gebruikte zoekreeks	**(Algemene cyber zoektermreeks)** AND TITLE-ABS-KEY (“interven” OR “sanction*” OR “deter*” OR “reduction” OR “discourage*” OR “resocial*” OR “punish*”OR “recidiv*” OR “prevent*”)

Bijlage 1B In- en exclusiecriteria systematische review

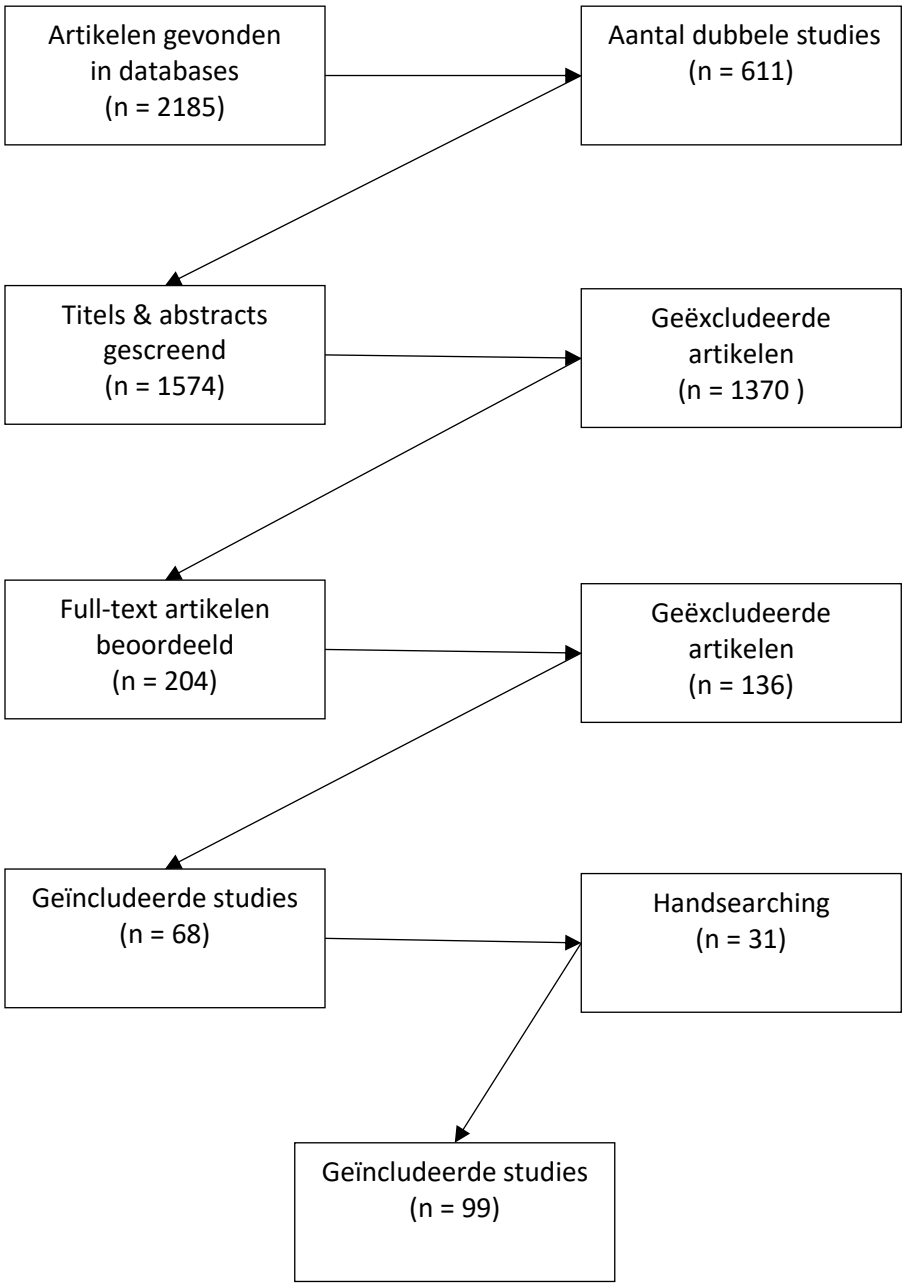
Het selectieproces van de systematische review heeft plaatsgevonden aan de hand van vastgestelde in- en exclusiecriteria. De eerste basis voor deze criteria is gelegd aan de hand van verscheidene bronnen met informatie over het uitvoeren van een systematische review (o.a. Petticrew & Roberts, 2006; PRISMA checklist) evenals wetenschappelijke studies die gebruik hebben gemaakt van een systematische review, waarbij de onderzoeksvragen en het doel van het onderzoek in het achterhoofd zijn gehouden. Deze in- en exclusiecriteria zijn vervolgens verder afgestemd met het onderzoeksteam en verder aangepast in samenspraak met de begeleidingscommissie.

Tabel 1 In– en exclusiecriteria systematische review

Wat	Inclusie	Exclusie	Aantal uitgesloten bronnen
Beschikbaarheid	Beschikbaar in online databases of bibliotheken	Niet beschikbaar in online databases of bibliotheken of tegen betaling	24
Soort bron	Wetenschappelijke bronnen (inclusief master scripties)	Nieuwsartikelen, blogs, recensies en overige bronnen die niet gebaseerd zijn op wetenschappelijke data	2
Soort studie	Kwantitatief en kwalitatief		
Publicatiejaar	Vanaf publicatiejaar 2000[84]	Publicatiejaar ouder dan 2000	5
Taal	Nederlands en Engels	Overige talen	2
Besproken soorten cybercriminaliteit (zie paragraaf 1.3)	Cybercriminaliteit in enge zin en randgevallen	Cybercriminaliteit in ruime zin	8
Relevantie voor onderzoeksvragen	Onderzoeken gericht op de thema's uit de onderzoeksvragen	Bijvoorbeeld onderzoeken over slachtofferschap, studies die slechts categorieën cybercriminaliteit noemen of te gedetailleerd en technisch ingaan op de modus operandi	86
Kwaliteit onderzoek		Onderzoeken met een erg gebrekkige validiteit of betrouwbaarheid of waarin uitspraken gedaan worden die niet onderbouwd worden met bronnen of data	2
Artikel duplicaten	Unieke bronnen	Artikelen die dubbel in de selectie zitten omdat ze bijvoorbeeld letterlijk zijn vertaald in een andere taal of zowel gepubliceerd zijn als een los artikel in een wetenschappelijk tijdschrift en als een promotieonderzoek	2
Dataset duplicaten	Unieke bronnen	Artikelen die dezelfde dataset gebruiken en tevens op dezelfde aspecten ingaan	5
		Totaal	136

[84] Deze keuze is gemaakt omdat cybercriminaliteit een snel ontwikkelend veld is en onderzoeken van voor het jaar 2000 waarschijnlijk niet representatief meer zijn voor de situatie anno 2019.

Bijlage 1C Flowchart systematische review



Bijlage 2 Interviewprotocol expertinterviews

Introductie

Wij willen u allereerst hartelijk danken voor uw bereidheid medewerking te verlenen aan ons onderzoek naar het profiel van cyberdaders en passende interventies. De opdracht tot het doen van dit onderzoek hebben wij ontvangen van het WODC. Aanleiding voor dit onderzoek vormde onder andere de Kamerbrief van Minister Grapperhaus over de integrale aanpak van cybercriminaliteit van afgelopen 20 april, waarin hij stelde dat voor beleidsvorming op de langere termijn meer kennis nodig is van daders en de aanpak daarvan. Onze onderzoeksvraag luidt als volgt:

"In hoeverre bestaan er verschillen qua profiel(en) van cybercriminelen en daders van 'traditionele' criminaliteit, en in hoeverre en op welke wijze dienen (eventuele) verschillen gevolgen te hebben voor de aard vaninterventies voor cybercriminelen?"

Om diepgaand inzicht in deze doelgroep te krijgen, horen wij graag van u, als expert, uw ervaringen, indrukken, ideeën en aanbevelingen. Wij richten ons nadrukkelijk op cybercriminaliteit in enge zin, waarbij de computer zowel het middel als het doel van het delict is (te denken valt aan hacken, DDoS-aanvallen en malware). We richten ons op daders van alle leeftijden. Het interview heeft twee overkoepelende thema's die wij met u willen bespreken: aan de ene kant de kenmerken (of: profielen) van cyberdaders, aan de andere kant passende straffen en interventies. Het interview zal +/- een uur in beslag nemen. Alle informatie die u deelt, wordt vertrouwelijk en anoniem behandeld en verwerkt. In de verslaglegging zullen we er zo ver als mogelijk voor zorgdragen dat niet herleidbaar zal zijn dat het uw antwoorden betreft.

1) Achtergrond expert

Alvorens we van start gaan, horen we graag wat meer over uw functie en de manier waarop u met cybercriminaliteit en de plegers daarvan in aanraking komt. Hoe lang bent u werkzaam op het gebied van cybercriminaliteit, wat houdt uw huidige functie in, en wat waren eventueel uw eerdere functies op dit gebied? Op welke wijze hebt u als experts kennis verzameld over cyberdaders en straffen/interventies?

2) Daderprofiel

Wij willen graag horen wat uw beeld van 'de' cybercrimineel is, en zullen hierbij vragen naar specifieke achtergrondkenmerken, verschillende onderdelen van de criminele carrière en tot slot naar hun morele percepties en attitudes.

Zou u allereerst iets kunnen vertellen over uw algemene indruk/beeld van dit type dader?

[vervolgens per suboonderdeel langslopen, eerst open, dan concreet, voldoende ruimte laten voor de visie van de expert zelf]

Achtergrondskenmerken

- Leeftijd
- Sekse
- Etnische achtergrond
- Opleiding
- Werk

- Inkomen, schulden
- Huidige thuissituatie (partner/kind)
- Gezin waarin opgegroeid
- Hobby's/vrije tijdsbesteding (hoeveel uur online)
- Sociale contacten (online & offline, evt. verschillen daartussen)
- Persoonlijkheidstype (intro/extravert, sociale vaardigheden, intelligentie, enz)
- Op welke bronnen is uw beeld omtrent deze achtergrondkenmerken gebaseerd (daders gesproken, dossiers, collega's, media, anders?)
- In hoeverre zijn er volgens u qua achtergrondkenmerken verschillende 'profielen' of 'typologieën' van cyberdaders te onderscheiden?
- In hoeverre bent u bekend met de achtergrondkenmerken van daders van traditionele criminaliteit?
- In hoeverre zijn er qua achtergrondkenmerken overeenkomsten/verschillen tussen cyberdaders en plegers van traditionele criminaliteit?
- Met welke (subgroep) traditionele daders komen cyberdaders qua achtergrondkenmerken mogelijk het meest overeen?

Criminele carrière

- Hoe voor het eerst met cybercriminaliteit in aanraking gekomen?
- Benodigde ICT-vaardigheden, hoe opgedaan?
- Welke type delicten? (specialist/generalist, on-/offline)
- Hoeveel delicten worden gemiddeld gepleegd? (eenmalig/veelpleger)
- Werkwijze, MO? (alleen/groep, locatie van plegen, doelwitselectie, benodigde tools, anonimiseringstools)
- Motivatie/drijfveren (uitdaging, status, nieuwsgierigheid, boosheid, politie ideologie, geld)
- Vinden hierbij veranderingen over tijd plaats?
- Rol van bepaalde (levens)gebeurtenissen en/of omstandigheden (financieel, situationeel, sociaal, persoonlijk) (bijv. thuissituatie, toezicht ouders/partner, krijgen kind, invloed vrienden, psychische problemen, verslavingen, schulden, etc.)
- Wat helpt bij het stoppen met criminaliteit?
- Op welke bronnen is uw beeld omtrent de criminele carrière gebaseerd (daders gesproken, dossiers, collega's, media, anders?)
- In hoeverre zijn er volgens u qua criminele carrières verschillende 'profielen' of 'typologieën' van cyberdaders te onderscheiden?
- In hoeverre bent u bekend met de criminele carrière van daders van traditionele criminaliteit?
- In hoeverre zijn er qua criminele carrière overeenkomsten/verschillen tussen cyberdaders en plegers van traditionele criminaliteit?
- Met welke (subgroep) traditionele daders komen cyberdaders qua criminele carrière mogelijk het meest overeen?

Morele percepties & attitudes

- Verschillen online/offline gedrag & rol anonimiteit? (online disinhibitie)
- Online moraal, grenzen? (wat mag wel/niet online)
- Neutralisaties ('iedereen doet het', 'het was voor de lol', ontkenning verantwoordelijkheid)
- Schuld/schaamte
- Bewustzijn slachtoffer? (wie is slachtoffer, confrontatie met reactie slachtoffer, eigen slachtofferschap?)/bewustzijn schade (bijv. financiële schade bedrijf)

- Op welke bronnen is uw beeld omtrent percepties & attitudes gebaseerd (daders gesproken, dossiers, collega's, media, anders?)
- In hoeverre zijn er volgens u qua percepties & attitudes verschillende 'profielen' of 'typologieën' van cyberdaders te onderscheiden?
- In hoeverre bent u bekend met de percepties & attitudes van daders van traditionele criminaliteit?
- In hoeverre zijn er qua percepties & attitudes overeenkomsten/verschillen tussen cyberdaders en plegers van traditionele criminaliteit?
- Met welke (subgroep) traditionele daders komen cyberdaders qua percepties & attitudes mogelijk het meest overeen?

3) Sancties en interventies

Wij zouden graag van u horen met welke sancties en interventies die worden toegepast op cyberdaders (in binnen- en buitenland) u bekend bent (sancties/interventies voor zowel daders in het algemeen, als enkel gericht op specifiek cyberdaders) en hoe u over deze verschillende aanpakken denkt. Wij zijn geïnteresseerd in zowel sancties/interventies vanuit de overheid als vanuit private partijen. Hierbij horen wij ook graag van interventies die nog in ontwikkeling zijn. Allereerst willen wij strafrechtelijke, reactieve sancties en interventies bespreken, daarna willen wij de aandacht verleggen naar preventieve interventies.

Strafbaarstelling en pakkans

- In hoeverre weten daders welk gedrag strafbaar is en welke straf kan worden opgelegd? In welke gevallen zijn zij hiervan wel/niet op de hoogte? Om welk type dader gaat het? Hoe vaak komt dat voor?
- Wat is de perceptie van daders omtrent de pakkans (afschrikking)? In welke gevallen zijn zij hiervan wel/niet op de hoogte? Om welk type dader gaat het? Hoe vaak komt dat voor?

Wat werkt, voor wie, onder welke omstandigheden

- In welke situaties zijn strafrechtelijke sancties of interventies volgens u wenselijk? Wat voor sancties/interventies betreft dit?
- Denkt u dat bepaalde sancties/interventies wel/niet helpen? Hoe vaak zijn die toegepast? Heeft u concrete voorbeelden interventies/maatregelen die wel/niet werkten? Hoe wist u dat het wel/niet werkte (voorbeelden)? Onder welke omstandigheden/in welke situatie was dat? Bij welk soort persoon was dat?
- In hoeverre sluiten deze sancties/interventies aan bij de (door u) geschetste karakteristieken van daders van cybercriminaliteit? Bij welke onderdelen van het 'profiel' of het 'type' sluiten bestaande sancties en interventies aan en bij welke niet? Waar zouden interventies zich specifiek op moeten richten?
- Welke aanvullingen/aanpassingen van bestaande sancties en interventies zijn volgens u nodig voor welk 'profiel' of 'type' cyberdader en waarom?

Alternatieve (preventieve) interventies ter voorkoming van recidive

- Van welke alternatieve, preventieve interventies bent u op de hoogte? (t.a.v. reeds veroordeelde cyberdaders, die beogen te voorkomen dat zij recidiveren)

- Heeft u concrete voorbeelden van dergelijke interventies en onder welke omstandigheden die wel/niet werkten? Hoe vaak zijn die ingezet? Bij welk soort persoon was dat?
- Hoe wist u dat het wel/niet werkte?
- In hoeverre sluiten deze preventieve interventies aan bij de geschetste karakteristieken van daders van cybercriminaliteit? Bij welke onderdelen van het profiel of de profielen sluiten bestaande preventieve interventies aan en bij welke niet?
- Waar zou preventie zich specifiek op moeten richten? Welke aanvullingen / aanpassingen zijn volgens u nodig voor welk type dader (of: het type dader waar u het meest mee in aanraking bent gekomen) en waarom?

- Wat vindt u van de volgende mogelijkheden voor preventieve interventies die in de internationale literatuur worden aanbevolen?
- Online politietoezicht en verstoring
- *(denk aan: policing in cyberspace / verstoren online markten)*
- Offline politietoezicht
- *(denk aan: knock-and-talk gesprekken: lokale, informele reactie, aanspreken jongeren)*
- Voorlichting
- *(denk aan: bewust maken van gevaren en risico's online gedrag / stranger danger / leren wat wel/niet strafbaar is / bewustmaken van de (strafrechtelijke) consequenties / bewustmaken van schade / aanpreken op verantwoordelijkheid / peer-based leren (rol v/d hele groep) / rolmodellen (ethisch hackers)*
- Alternatieven bieden
- *(denk aan: morele besluitvorming sturen / self-challenge / aanbieden van alternatieve 'pathways' richting ethisch verantwoorde prestaties i.p.v. opklimmen in hiërarchie van hackers / nieuwsgierigheid aanmoedigen & skills op andere manier inzetten / eigenwaarde en sociale inbedding / gamification / hackathons / competities*
- Rol ouders
- *(denk aan: toezicht (op de hoogte van online gedrag) / voorlichting (op de hoogte van wat wel/niet strafbaar is)*
- Rol industrie
- *(denk aan: commerciële beveiligingsbedrijven of Internet Service Providers als 'capable guardians' / organiseren van wedstrijden, cyber-kampioenschappen, programma's en prijzen)*
- Denkt u dat bepaalde preventieve interventies wel/niet zouden helpen? Heeft u concrete voorbeelden waarop u die verwachting baseert? Onder welke omstandigheden verwacht u dat deze interventies wel/niet werken en voor welke personen zullen ze wel/niet werken?

Bijlage 3A: Discussiepunten expertmeeting

1. ‘Erkenning’ lijkt een belangrijke rol te spelen bij cyberdaders. Wat ligt hieraan ten grondslag en in hoeverre speelt dit een grotere/andere rol dan bij traditionele daders?

2. Een veelgehoorde ‘claim’ van experts en daders zelf is dat cyberdaders de gevolgen van hun online handelen niet goed kunnen overzien. Hoe kan het dat ze dit niet kunnen overzien?

3. Wat onderscheidt de cyberdader van de IT-er die WEL op het rechte pad blijft en/of die al heel snel de overstap maakt naar *responsible* hacks?

4. Welke factoren zorgen er voor dat cyberdaders die willen stoppen niet in staat zijn om te stoppen?

5. Er lijkt een relatie te bestaan tussen gaming en cybercriminaliteit. Wat moeten we hiermee qua interventies?

Bijlage 3B. Discussiepunten Roundtable

Deel 1: Toepassing bestaande interventies voor traditionele daders op cyberdaders:

1. In welke richting moeten we het zoeken als het gaat om de toepassing van bestaande sancties en interventies ontwikkeld voor ‘traditionele’ (typen) daders op cyberdaders?

    a. In hoeverre zijn beïnvloedingmechanismen die bewezen effectief zijn voor traditionele daders ook effectief voor cyberdaders?

    b. Hoe moeten we bestaande interventies aanpassen voor cyberdaders?

Deel 2: Toepassing interventies specifiek ontwikkeld voor cyberdaders

2. Wat zijn de belangrijkste werkzame mechanismen bij interventies gericht op cyberdaders: is dit het bieden van een alternatief, bewustmaking, afschrikking of een combinatie hiervan?

3. Moeten interventies voor cyberdaders zich vooral op hun offline of hun online werkelijkheid richten? Kunnen sociale vaardigheden/ethiek online geleerd worden, of moet daarmee offline geoefend worden? En, andersom, kunnen vaardigheden die online nodig zijn, offline geleerd worden?

Bijlage 4 Wetsartikelen benadering respondenten

Wetsartikel	Naam	Omschrijving
138ab Sr	Computervredebreuk	1. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven: a) door het doorbreken van een beveiliging, b) door een technische ingreep, c) met behulp van valse signalen of een valse sleutel, of d) door het aannemen van een valse hoedanigheid. 2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt. 3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens a) met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk; b) door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde
138b Sr	Spam of bombing	1. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden. 2. Indien het feit wordt gepleegd met behulp van een aanzienlijk aantal geautomatiseerde werken die getroffen zijn door het gebruik van een middel als bedoeld in artikel 139d, tweede lid, dat hoofdzakelijk daarvoor geschikt is gemaakt of ontworpen, wordt de schuldige gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie. 3. Indien het feit ernstige schade veroorzaakt, of is gepleegd tegen een geautomatiseerd werk behorende tot de vitale infrastructuur, wordt de schuldige gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vierde categorie.
139c Sr	Aftappen gegevens overgedragen via telecommunicatie	1.Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk. 2. Het eerste lid is niet van toepassing op het aftappen of opnemen: **1°.** van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt. **2°.** door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik; **3°.** ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan

		wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002 .
139d Sr	Plaatsen opname-, aftap- c.q. afluisterapparatuur	1.Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn. 2.Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c wordt gepleegd: a) een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of b) een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden gekregen tot een geautomatiseerd werk of een deel daarvan, vervaardigt verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.
139e Sr	Hebben bekendmaken, overdragen van d oor wederrechtelijk afluisteren, aftappen of opnemen verkregen gegevens	Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft: **1°.** hij die de beschikking heeft over een voorwerp waarop, naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk zijn verkregen; **2°.** hij die gegevens die hij door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk heeft verkregen of die, naar hij weet of redelijkerwijs moet vermoeden, ten gevolge van zulk afluisteren, aftappen of opnemen te zijner kennis zijn gekomen, opzettelijk aan een ander bekend maakt; **3°.** hij die een voorwerp als omschreven onder 1° opzettelijk ter beschikking stelt van een ander.
161sexies Sr	Geautomatiseerd werk of werk voor telecommucatie vernielen, beschadigen, onbruikbaar maken, verstoren	Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft: **1°.** met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is; **2°.** met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is; **3°.** met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.
161septies Sr	Culpoos delict	Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar gemaakt, dat stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld, wordt gestraft: **1°.** met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie, indien daardoor verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemenen nutte, stoornis in een openbaar telecommunicatienetwerk of in de

		uitvoering van een openbare telecommunicatiedienst, of gemeen gevaar voor goederen of voor de verlening van diensten ontstaat; **2°.** met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie, indien daardoor levensgevaar voor een ander ontstaat; **3°.** met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie, indien het feit iemands dood ten gevolge heeft.
350a Sr	Computergegevens veranderen, wissen, onbruikbaar maken	1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. 2. Artikel 138b, tweede en derde lid, is van overeenkomstige toepassing. 3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie. 4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.
350b Sr	Culpoos delict	1. Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, wordt, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt, gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie. 2. Hij aan wiens schuld te wijten is dat gegevens wederrechtelijk ter beschikking gesteld of verspreid worden die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.
317 Sr	Afpersing dwangmiddelen	1. Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door geweld of bedreiging met geweld iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt, als schuldig aan afpersing, gestraft met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie. 2. Met dezelfde straf wordt gestraft hij die de dwang, bedoeld in het eerste lid, uitoefent door de bedreiging dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist.
231b Sr	Identificerende persoonsgegevens	Hij die opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruikt met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan, wordt gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vijfde categorie.

Bijlage 5 Online wervingstekst

Gezocht: deelnemers onderzoek

Ben jij of ken jij iemand die wel eens een systeem heeft gehackt, malware heeft verspreid, een DDoS heeft uitgevoerd of iets soortgelijks heeft gedaan? Help dan mee aan ons onderzoek.

Wij, onderzoekers van de Erasmus Universiteit, willen jou graag interviewen over jouw ervaringen. Hoe en waarom raakte je hierbij betrokken? Wat vind je van de aanpak van justitie? Hoe kijk je naar jezelf en naar de toekomst?

Door de kennis die jij met ons deelt, kunnen wij een beter beeld krijgen van de 'persoon achter cybercrime' en voor justitie in kaart brengen wat belangrijke verbeterpunten zijn in de omgang met cybercrime.

Wat je met ons deelt, is 100% vertrouwelijk en anoniem en is alleen voor ons beschikbaar (dus niet voor de politie, OM, reclassering of andere partijen).

Wil je meewerken? Dan nodigen we je graag uit voor een interview. Dat kan face to face, telefonisch of via skype.

Belangstelling en/of vragen over het onderzoek? Mail naar: (emailadres)

Bijlage 6 Interviewprotocol daderinterviews

Interviewprotocol daderinterviews

Nogmaals heel erg fijn dat je bereid bent om mee te werken aan dit interview. Zoals ik in mijn mail aangaf: het doel van het onderzoek is om meer te weten te komen over jongeren en volwassenen die op enigerlei wijze betrokken zijn of betrokken zijn geweest bij cybercrime, zoals hacking/cracking, DDoS aanvallen of het verspreiden van malware. Ook willen we in dit onderzoek meer te weten komen over je ervaringen met de aanpak van of met interventies tegen cybercrime.

In dit interview willen we je graag wat vragen stellen over je achtergrond, hoe je in aanraking bent gekomen met cybercrime, je beweegredenen en ervaringen en tot slot horen we ook graag jouw ideeën over wat passende reacties van politie en justitie zouden kunnen zijn. In dit interview staat echt jouw verhaal centraal. Als er vragen zijn die je niet wilt beantwoorden, geef het aan. Als er dingen zijn die je zelf graag wilt vertellen, maar waar niet naar wordt gevraagd, geef het ook aan. Het interview zal ongeveer 1 uur tot 1,5 uur duren.

Belangrijk is om aan te geven dat jouw gegevens en alles wat je tijdens het interview vertelt vertrouwelijk wordt behandeld. De informatie uit het interview wordt anoniem en vertrouwelijk verwerkt. Er zal op geen enkele manier herleidbaar zijn dat het jouw antwoorden of verhaal betreft.

Deel 1) Achtergrond

a. Wat is je leeftijd?
b. Waar kom je vandaan?
c. Kun je iets vertellen over je huidige/afgeronde studie?
d. Kun je iets vertellen over je werk/loopbaan en wat je droombaan is? Kun je hiervan rondkomen? Zo nee, waar inkomen vandaan?
e. Kun je iets vertellen over je huidige thuissituatie (alleen, partner, kind)?
f. Kun je iets vertellen over het gezin waarin je bent opgegroeid? (werk ouders, gezinssamenstelling, afkomst)
g. Kun je iets vertellen over je interesses en dagelijkse bezigheden (zowel online als offline)? Hoe vaak en hoe lang ben je per dag gemiddeld online?
h. Kun je iets vertellen over jouw sociale contacten (online en offline)? Zijn er verschillen in jouw online en offline vriendschappen?
i. Kun je iets vertellen over jezelf? Hoe zou je jezelf als persoon beschrijven? [*introvert/extravert, onzeker of heel zelfverzekerd, avontuurlijk of teruggetrokken, sociaal vaardig of sociaal onhandig (ongepaste dingen zeggen), gedisciplineerd of impulsief, lui/actief*?]
j. Hoe denk je dat andere mensen jou zouden omschrijven?

Deel 2) Betrokkenheid bij cybercrime en de ontwikkelingen hierbij:

a) Initiatie:
   - *Eerst algemeen:*
   - Dit onderzoek gaat zoals gezegd over cybercrime. Kun je mij/ons iets vertellen over jouw ervaring hiermee/betrokkenheid hierbij?
   - Kun je iets vertellen over wanneer en hoe je voor het eerst met cyber-gerelateerde activiteiten in aanraking bent gekomen? Kun je beschrijven hoe dat ging?
   - Met welke activiteiten hield je je toen bezig en hoe vaak deed je dat?
   - Kun je iets vertellen over de ICT vaardigheden die je daar voor nodig had en hoe je deze vaardigheden hebt aangeleerd? (fora, mentor, experimenteren, etc)
   - Hoe ging je toen te werk? (modus operandi, alleen gepleegd of in groep, locatie, doelwitselectie, gebruik anonimiseringstools)
   - Kun je iets vertellen over je motivatie/drijfveren/doel toen je hiermee begon *[nieuwsgierigheid, uitdaging, kick, spanning, trots, macht, respect/aanzien, zichzelf bewijzen/competitie, erkenning, hebzucht, wraak, boosheid, politieke ideologie, financieel, rationeel versus irrationeel]?*
   - (Verbonden met voorgaande vraag): Wat sprak/trok je zo aan (beleving/gepaard emoties)? Hoe ervoer je het om te X-en (hacken, een bedrijf te DDoSen, etc)?
   - Zijn er volgens jou ook bepaalde omstandigheden of gebeurtenissen geweest die een rol hebben gespeeld bij jouw betrokkenheid bij activiteit(en) X? Bijvoorbeeld op het persoonlijke, financiële of sociale vlak?) [*negatieve levensgebeurtenissen, thuissituatie, toezicht ouders, rol partner/kind, invloed van (online/offline) vrienden, persoonlijke factoren/psychische problemen, verslavingen, schulden etcetera*]

b) Ontwikkeling over tijd
   - *Eerst algemeen*: Je bent begonnen met (*refereren naar hetgeen besproken bij 2a*), hoe ging het verder?

   - *Dan specifiek:* Zijn er over tijd dingen veranderd als het gaat om:
   - de activiteiten waar je je mee bezighield
   - Je vaardigheden
   - Je werkwijze
   - Je motivatie/beweegredenen/doel en wat je zo aansprak (beleving)
   - De (rol van) omstandigheden en gebeurtenissen

c) Stoppen (en eventuele rol van opgelegde sanctie of interventie hierbij)
   - Ben je gestopt?
   - **Zo ja:** waarom/waardoor? Kun je beschrijven hoe dat is gegaan?
   - **Zo nee**, waarom niet? Ben je van plan om te stoppen en zo ja/nee waarom?
   - Wat zou jou eventueel helpen om te stoppen?

   - Heb je ooit een sanctie of interventie opgelegd gekregen? Zo ja, welke en waarvoor?
   - Wat vond je daarvan? (*terecht/onterecht, wel/niet te zwaar*)
   - Hoe heb jij dit ervaren?

- Heb jij er iets aan gehad?
- Is er door de sanctie iets veranderd ten aanzien van je kijk op cybercrime, jezelf, je toekomstplannen? Wat heeft precies voor deze verandering gezorgd?
- Heeft deze sanctie/interventie een rol gespeeld bij het wel/niet stoppen?

Deel 3) Morele percepties, attitudes & neutralisatie & rol van online disinhibitie

- In hoeverre bestaan er voor jou grenzen met betrekking tot hoe ver je gaat met bepaalde online/cyber gedragingen: dit doe ik wel en dit doe ik niet? Dit is goed en dit is slecht? Wat zijn je afwegingen hierbij? [*kan gaan om motieven, gevolgen, specifieke handelingen*]?
- Zijn er dingen die je online zou zeggen of doen die je offline nooit zou doen of durven? Waarom wel/niet? (*rol van anonimiteit, niet geconfronteerd worden met slachtoffer*)
- Zijn mensen die cybergedragingen plegen (zoals hacking & DDoS) volgens jou te vergelijken met mensen die bijvoorbeeld een woninginbraak doen of iets vernielen? Wat zijn volgens jou overeenkomsten en verschillen?

- Wie is volgens jou het slachtoffer van cybercrime (hacking, DDoS, malware etc)? Is er volgens jou een slachtoffer aan te wijzen? Is er volgens jou sprake van schade als gevolg van (jouw) acties/cybergedragingen?
- Denk je daar veel over na tijdens of na het plegen van een X (DDoS, hack, etc)? Wat zijn jouw gedachten hierover?
- Ben je weleens geconfronteerd met een reactie van een slachtoffer, weet je wat de impact van jouw acties was?

Heb je nog dingen toe te voegen aan het inteview die je graag kwijt wilt? Opmerkingen, aanvullingen?

Afsluiting

Bijlage 7 Leden van de begeleidingscommissie

De volgende leden namen deel aan de begeleidingscommissie:

- De heer em. prof. mr. T.A. (Theo) de Roos (voorzitter) – Universiteit Tilburg
- De heer drs. A.W. M (Ton) Eijken - MinJenV - DG Straffen en Beschermen (DG SenB)
- Mw. Dr. Marleen Weulen Kranenbarg (Vrije Universiteit)
- De heer drs. L.F. Heuts (projectbegeleider) - Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)