Een kijkje achter de schermen: een kwalitatieve studie over het ontstaan van cybercriminele carrières

Sifra Matthijsse, Wytske van der Wagen, Elina van 't Zand & Tamar Fischer

In deze kwalitatieve studie is onderzocht hoe criminele carrières in de cybercriminaliteit ontstaan en verklaard kunnen worden. Op basis van dader- en expertinterviews concluderen de auteurs dat traditionele factoren verbonden met de initiatie, zoals een maturatiekloof (voor jeugdige daders) en gelegenheid (voor volwassen daders), in combinatie met verschillende soorten online disinhibitie – sociaal, technisch, situationeel en psychologisch – de start van een criminele carrière kunnen verklaren. De grote rol van de digitale context bij de initiatie vraagt om meer online toezicht en voorlichting, onder andere over legale alternatieven en de risico's en grenzen van de online omgeving.

Inleiding

> 'Hij was de koning van de creditcardhackers, tot de Amerikanen hem arresteerden. (...) Een verhaal dat begint in het ouderlijke huis, onder de rook van Rotterdam. Daar, achter zijn toetsenbord, veranderde de teruggetrokken, stille puber in een gevreesde en gerespecteerde hacker. Daar waande hij zich onaantastbaar. Hij was er heer en meester van zijn eigen digitale universum.' (Lensink & Vuijst, 2015)

Teruggetrokken en stil in de 'normale wereld', maar gerespecteerd en gevaarlijk in de digitale wereld. Dat zijn elementen uit het script van veel 'succesverhalen' over criminele carrières van hackers. Het begint allemaal klein en onschuldig achter een toetsenbord, tot de dader steeds verder afglijdt naar de donkere kant van het internet en alleen een ontmaskering of arrestatie hem weer tot bezinning kan brengen. Het is echter nog onduidelijk in hoeverre dit beeld klopt. Zo wordt vaak verondersteld dat de criminele carrière van cyberdaders achter het toetsenbord begint, maar mogelijk kan ook de straat, de school of het werk een rol spelen bij de initiatie. Bovendien speelt het leven van cyberdaders zich niet 24/7 af achter het scherm (Van der Wagen e.a., 2019). Waarschijnlijker is dat cyberdaders een heterogene groep vormen qua motieven en kenmerken en, mede daarom, niet alle cybercriminele carrières hetzelfde beginnen (Hutchings, 2016).
Als het om verklaringen voor cyberdelinquentie gaat, lijken (deels) andere verklaringen een rol te spelen dan bij traditionele delinquentie. Cyberdaders zouden vaker gedreven worden door motieven als technologische nieuwsgierigheid, interesse en uitdaging (Aiken e.a., 2016; Van der Wagen e.a., 2016; Weulen Kranenbarg, 2018). Daarbij oefent de online omgeving waarin de delicten plaatsvinden

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

een belangrijke invloed uit (o.a. Hoek van Dijke, 2016; Kerstens & Veenstra, 2013; Zebel e.a., 2013).
Hoewel in toenemende mate kenmerken van cyberdaders worden onderzocht, ontbreekt kennis over hoe delictgedrag ontstaat. Dergelijke kennis is van groot belang, nu cybercriminaliteit nog steeds een in omvang toenemend probleem vormt. Terwijl traditionele criminaliteit daalt, valt een toename in cyberdelicten uit politiecijfers op te maken (CBS, 2020). Met kennis over het ontstaan van cyberdelinquent gedrag kunnen passende preventieve en reactieve interventies worden ontwikkeld, die deze toename een halt kunnen toeroepen. Daarom staat in deze bijdrage de volgende onderzoeksvraag centraal: hoe ontstaan criminele carrières in de cybercriminaliteit en hoe kan dit ontstaan verklaard worden? Daarbij focussen we op verklaringen verbonden met de (online) sociale, technische, situationele en psychologische context en richten we ons expliciet op de initiatiefase van de criminele carrière van daders van cybercriminaliteit in enge zin.[1]
Voor dit onderzoek is gebruik gemaakt van data bestaande uit dader- en expert-interviews. In dit artikel zal het accent liggen op de bevindingen uit de daderinterviews om verdiepende inzichten te bieden in wat zich 'achter de schermen' afspeelt bij deze daders.

Theoretisch kader

Uit een systematische zoekopdracht naar literatuur over daderkenmerken is gebleken dat er nog maar zeer weinig studies zijn gedaan op het gebied van criminele carrières van cyberdaders (Van der Wagen e.a., 2019). Wel is er in de literatuur aandacht voor persoonskenmerken, motieven en verklaringen die in algemene zin een rol spelen bij hun delictgedrag en dus ook inzichten kunnen bieden over de initiatiefase.
Voor de verklaring van de initiatie van de criminele carrière van jeugdige en volwassen cyberdaders gebruiken we in deze studie traditionele verklaringen over de totstandkoming van criminele carrières (Moffitt, 1993) en traditionele theorieën die cybercriminaliteit kunnen verklaren, zoals de leertheorieën, controlebenaderingen en gelegenheidstheorieën (o.a. Aiken e.a., 2016; Bae, 2017; Hutchings, 2016; Yar, 2005). Om specifiek de rol van de digitale context bij de initiatie te duiden wordt tevens gebruik gemaakt van twee aanvullende benaderingen die steeds meer aandacht krijgen in cybercriminologisch onderzoek, namelijk het online disinhibitie-effect (Suler, 2004) en de affordance-benadering (Goldsmith & Wall, 2019).

1 Onder cybercriminaliteit in enge zin worden delicten verstaan waarbij ICT zowel het middel als het doelwit is (zoals hacken, ddos-aanvallen en ransomware). 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.

Traditionele verklaringen

Een van de meest invloedrijke criminologische benaderingen over het ontstaan van criminele carrières bij verschillende typen (jeugdige) daders is het tweepadenmodel van Moffitt (1993). Hierin worden aanvankelijk twee categorieën daders onderscheiden. In de eerste plaats de *life-course-persistent* daders, die vanwege bepaalde neuropsychologische factoren in combinatie met negatieve omgevingsfactoren al op jonge leeftijd met hun criminele carrière starten en vaak steeds ernstigere delicten gaan plegen en daarmee doorgaan tot in de (late) volwassenheid. De tweede (meest omvangrijke) categorie daders betreft de *adolescence-limited* daders, bij wie het criminele gedrag zich beperkt tot de adolescentie. Volgens Moffitt ligt bij deze daders de discrepantie tussen biologische en sociale volwassenheid, beter bekend als de maturatiekloof, ten grondslag aan het plegen van delicten. Dit gaat enerzijds gepaard met het zich willen onttrekken aan het ouderlijk gezag, onafhankelijk willen zijn en zich minder van de regels aantrekken, en anderzijds met het op zoek zijn naar een eigen identiteit en daarbij extra gevoelig zijn voor de invloed van peers. Zoals beschreven in de differentiële-associatietheorie spelen peergroepen een belangrijke rol bij het overdragen en normaliseren van delinquent gedrag (Sutherland, 1947). In deze periode neemt de sociale controle van ouders geleidelijk aan af.

Tegelijkertijd beschikken jongeren tijdens de adolescentie over beperkt ontwikkelde cognitieve en psychosociale inzichten in normatieve kwesties, waardoor zij de gevolgen van hun acties op de langere termijn moeilijk kunnen overzien en impulsief gedrag kunnen vertonen (Moffitt, 1993; Warr, 2002). Er zijn weinig studies die de rol van de adolescentie en daarmee verbonden factoren bij cyberdaders in enge zin hebben onderzocht. Wel zijn er duidelijke aanwijzingen dat er sprake is van gebrekkig ethisch inzicht of morele onvolwassenheid bij jeugdige cyberdaders (Yar, 2005). Ook de rol van peers wordt van groot belang geacht bij de ontwikkeling van het delictgedrag van cyberdaders (Holt e.a., 2012; Rogers, 2010; Van der Toolen e.a., 2020). Tot slot wordt in de literatuur gewezen op een groot gebrek aan digitale kennis of interesse en onderschatting van ouders ten aanzien van de risico's die hun kind online loopt (zie o.a. Aiken e.a., 2016; Kerstens & Stol, 2012; Chiesa e.a., 2007).

Ook gelegenheidsbenaderingen zijn van belang om de initiatie van criminele carrières te kunnen duiden. Hoewel deze benadering zich doorgaans richt op de verklaring voor het plaatsvinden van delicten in een fysieke omgeving, maar niet op de ontwikkeling van criminele carrières, kan blootstelling aan veel geschikte doelwitten die onvoldoende beschermd of bewaakt worden (Cohen & Felson, 1979), bijdragen aan de kans dat startdelicten plaatsvinden en een vervolg krijgen doordat de beloning groot is en kosten uitblijven. Dit geldt des te meer voor de categorie daders die in latere studies als aanvulling op Moffitts tweepadenmodel zijn benoemd, namelijk de categorie van de late (volwassen) starters. Voor bijvoorbeeld witteboordencriminelen (Piquero & Benson, 2004) en daders actief in de georganiseerde misdaad (Kleemans & De Poot, 2008; Van Koppen e.a., 2010) wordt de verklaring voor de initiatie vooral gezocht in nieuwe gelegenheidsstructuren, die zich onder meer voordoen via sociale en beroepsgerelateerde contacten (de sociale gelegenheidsstructuur) (Kleemans & De Poot, 2008) en min-

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

der in individuele factoren. Gelegenheid wordt ook als een belangrijke factor gezien bij cyberdaders (Weulen Kranenbarg e.a., 2018), waarbij vooral gewezen wordt op de nieuwe mogelijkheden en kansen die de online wereld biedt om veel geld te verdienen in combinatie met de lage pakkans (Leukfeldt e.a., 2017b; Odinot e.a., 2017). Hutchings (2016) spreekt in dit kader van *innovators*. Deze daders zijn vanuit problematiek, zoals geldproblemen, begonnen met traditionele criminaliteit, maar maken opportunistisch de overstap naar cybercriminaliteit. De beschikbaarheid van tools en services draagt volgens de literatuur ook bij aan de gelegenheid tot het plegen van delicten voor zowel jeugdige als volwassen cyberdaders (o.a. Brewer e.a., 2018; Leukfeldt e.a., 2017a; Odinot e.a., 2017). Zodoende wordt het instapniveau verlaagd en – o.a. door globalisering en schaalvergroting – de toegang tot een geschikt doelwit vergroot (Broadhurst e.a., 2014; Hoek van Dijke, 2016; Kirwan & Power, 2013).

Cyberverklaringen

Naast de verklaringskracht van deze conventionele theorieën gaan wij ervan uit dat de aard van de criminaliteit en de specifieke digitale context waarin cyberdaders opereren nieuwe aspecten toevoegen aan de initiatie, die wij als criminologen moeten duiden. Hiervoor maken we allereerst gebruik van het online disinhibitie-effect: een (cyber)psychologisch concept dat benadrukt dat bepaalde kenmerken van het internet het plegen van cyberdelicten vereenvoudigen (Suler, 2004). Ons inziens is dit perspectief goed bruikbaar, omdat het aspecten uit het tweepadenmodel in verbinding kan brengen met de online omgeving.

Ten eerste zorgt de *anonimiteit* op het internet ervoor dat bepaalde remmingen wegvallen. Doordat er sprake is van gebrekkige controle op het gedrag, bijvoorbeeld door ouders of leraren, kan men online doen en laten wat men wil. Door gebruik van anonimiseringstools (zoals Tor en VPN), versleuteling van communicatie en het gebruik van nicknames is bovendien de pakkans erg laag. Online acties hebben ook geen ervaren consequenties in het fysieke leven. Mensen kunnen zich hierdoor online anders voordoen dan ze in het 'echte' leven zijn, ook wel *plasticiteit van de identiteit* genoemd (Goldsmith & Wall, 2019; Yar, 2005). Dit kan van positieve invloed zijn, in de zin dat mensen zich eenvoudiger kunnen uiten en meer durven te zeggen en te doen (*benign disinhibition*), maar ook van negatieve invloed, in de zin dat het tot delinquent gedrag kan leiden (*toxic disinhibition*). Ten tweede gaat Suler (2004) ervan uit dat daders online het gevoel kunnen hebben in een *hyperrealiteit* te bewegen, een 'make-believe play world that has nothing to do with reality' (p. 323). Het gaat dus om het bestaan, of beter gezegd het *creëren* van twee gespleten werelden, waarbij zij de online wereld achter zich kunnen laten wanneer zij zich achter hun beeldscherm vandaan begeven terug naar het echte leven. Dit proces wordt ook wel *dissociatieve verbeelding* genoemd (Suler, 2004).

Waar Suler (2004) vooral de nadruk legt op de psychologische dimensie van de online context, focussen Goldsmith en Wall (2019) zich meer op de sociale, situationele en technische dimensie en de interactie daartussen. Zij gaan ervan uit dat het internet bepaalde sociale en technische *affordances* biedt die het starten van een criminele carrière in de cybercriminaliteit verleidelijk maken en kunnen versnellen. Dit perspectief lijkt erg bruikbaar voor cyberdaders, omdat uit veel

studies blijkt dat daders met cybercriminaliteit starten vanwege of vanuit een sterke fascinatie voor digitale technologie en het willen experimenteren met de mogelijkheden en grenzen van deze techniek (zie o.a. Steinmetz, 2015; Van der Wagen, 2018; Xu e.a., 2013). Ook zijn er daders die heel expliciet via gaming met cybercriminaliteit in aanraking komen (o.a. Hutchings, 2016; NCA, 2017; Steinmetz, 2016). Het perspectief van Goldsmith en Wall (2019) is gebaseerd op inzichten uit de affordance-theorie, mens-computerstudies en de seductions of crime (*sneaky thrill*)-benadering van Katz (1988), die zich richt op verleidelijke aspecten van het plegen van criminaliteit. Hun perspectief is daarmee breder en omvattender dan een klassiek gelegenheidsperspectief. Affordances zijn handelingsmogelijkheden die voortkomen uit (c.q. 'uitgenodigd' worden door) de materiële eigenschappen van een object of technologie. Goldsmith en Wall (2019) onderscheiden de volgende zeven affordances: (1) *anonimiteit*: men kan online een andere identiteit aannemen; (2) *toegankelijkheid*: het internet is voor vrijwel iedereen toegankelijk, het beheersen van de techniek kan een gevoel van *mastery* geven en de snelheid ervan een gevoel van extase; (3) *betaalbaarheid*: veel functies en materiaal op het internet zijn eenvoudig en kosteloos toegankelijk; (4) *overvloed*: dit is nauw verbonden met de toegankelijkheid en betaalbaarheid; er is een grenzeloze overvloed aan verschillende content (ook van extreme of verontrustende aard) die 24/7 zoek- en vindbaar is; (5) *ambivalentie*: bestaande gedragsnormen worden in de afwezigheid van toezichthouders overschaduwd door online gedragsnormen, wat kan leiden tot het loslaten van persoonlijke normen (of normloosheid) en vermindering van zelfregulatie; hiermee hangt een gevoel van hyperrealiteit samen, waardoor de gepercipieerde schade en risico's worden verminderd; (6) *opwinding*: de blootstelling aan nieuw, aantrekkelijk en grensoverschrijdend materiaal kan zowel lichamelijk als intellectueel provoceren en opwinden; (7) *asymmetrie*: het internet en de techniek kunnen onvoorspelbaar zijn op het gebied van materiaal, timing en presentatie. Online heeft men nooit de volledige controle en dat aspect kan een bepaalde aantrekkingskracht uitoefenen (zie ook Van der Wagen, 2018).

Indien we de verschillende dimensies die bij Suler (2004) en Goldsmith en Wall (2019) centraal staan met elkaar verbinden, komen we tot de volgende drie verklaringen voor het ontstaan van cybercriminele carrières: (1) sociale online disinhibitie (het wegvallen van sociale barrières), (2) situationele en technologische online disinhibitie (het wegvallen van situationele en technische beperkingen), en (3) psychologische online disinhibitie (het wegvallen van morele remmingen). Aan de hand van deze cybercriminologische concepten in combinatie met traditionele benaderingen zullen wij op basis van het empirisch materiaal uitdiepen hoe en waarom daders van cybercriminaliteit in enge zin met een criminele carrière starten.

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

Dataverzameling en analyse

Voor de beantwoording van de onderzoeksvraag is gebruik gemaakt van een bestaande dataset, die bestaat uit een literatuuronderzoek[2] en interviews met zowel cyberdaders als experts op het gebied van cybercriminaliteit. Deze data zijn verzameld in de periode november 2018 tot en met augustus 2019, in het kader van een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin (Van der Wagen e.a., 2019), in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). Het accent in dit artikel ligt op de bevindingen uit de daderinterviews. De expertinterviews hebben een meer complementaire rol en geven verdieping aan de informatie uit de daderinterviews, om bevindingen daaruit te bevestigen, contrasteren of nuanceren.

De dataset bestaat uit veertien daderinterviews. Deze daders zijn geworven via de reclassering[3] (n=8), hackfora en gerelateerde kanalen (n=2), eerdere onderzoekscontacten (n=1) en de sneeuwbalmethode (n=3). Voor de afname van de interviews is toestemming verkregen van de Ethics Review Board van Erasmus School of History, Culture and Communication (ESHCC).[4] Dertien van de veertien interviews zijn fysiek afgenomen en een interview heeft plaatsgevonden via Skype. Tijdens deze interviews, die gemiddeld 1,5 uur duurden, hebben wij de respondenten gevraagd naar onder meer hun achtergrond, motieven, aspecten betreffende de criminele carrière en percepties ten aanzien van de strafbaarheid en de schade van cyberdelicten. De respondenten zijn allen mannen tussen de 18 en 40 jaar oud (gemiddeld 26 jaar oud). Negen respondenten hebben een opleiding op hbo/wo-niveau afgerond of zijn daarmee bezig, vier respondenten hebben als hoogste genoten onderwijsniveau mbo en een van hen heeft het lbo doorlopen. Het merendeel van de respondenten heeft zich schuldig gemaakt aan computervredebreuk (art. 138ab Wetboek van Strafrecht (Sr)) – soms in combinatie met andere activiteiten, zoals het uitvoeren van een ddos-aanval, virtuele diefstal of fraude – en is veroordeeld voor cybercriminaliteit in enge zin. Een minderheid was weliswaar betrokken bij dergelijke delicten, maar is er nooit voor opgepakt of veroordeeld. De geïnterviewde groep daders betreft dus een vrij specifieke groep (mannen die voor het merendeel zijn veroordeeld wegens hacken), met als gevolg dat over de initiatie van andersoortige delictplegers, zoals phishers, minder gezegd kan worden.

Alle respondenten hebben ten tijde van het interview aangegeven te zijn gestopt met het plegen van (cyber)delicten. Het feit dat de respondenten retrospectief over hun betrokkenheid bij cybercriminaliteit spraken, heeft tot gevolg dat zij moesten reflecteren op zaken die zich in het verleden hebben afgespeeld. Voor

2 De bevindingen hieruit worden niet uitvoerig behandeld in dit artikel. Zie hiervoor Van der Wagen e.a., 2019.

3 De reclassering heeft medewerking verleend voor de werving van respondenten en heeft de interviews gefaciliteerd.

4 Een aantekening hierbij is dat de commissie ons 'approval with reservations' heeft gegeven, omdat zij nog wat verbeterpunten had bij het door ons reeds gebruikte informed-consentformulier.

sommigen van hen was de initiatie ook lang geleden. Desalniettemin hebben we de indruk dat we over het algemeen vrij betrouwbare informatie hebben verkregen en dat de daders de initiatie goed konden reconstrueren. Door te benadrukken dat het interview vertrouwelijk was, goed door te vragen, naar concrete voorbeelden te vragen en een vertrouwensband te creëren is getracht de validiteit van de bevindingen te vergroten. Hoewel deze veertien daderinterviews niet kunnen leiden tot generaliserende uitspraken over deze groep, kan middels de rijke data die de interviews opleverden inzage gegeven worden in het ontstaan van criminele carrières in de cybercriminaliteit.

De (volledige) dataset betreffende de experts bestaat uit 52 respondenten van uiteenlopende (publieke en private) partijen. Deze experts staan vanwege hun functie in contact met jeugdige en/of volwassen daders van cybercriminaliteit in enge zin. De expertdata bestaan uit 29 individuele interviews, twee focusgroepen, een expertmeeting en een roundtable. Hierbij is uitgebreid gevraagd naar dezelfde aspecten als bij de daderinterviews en is telkens zo veel mogelijk gevraagd naar concrete voorbeelden en casuïstiek. Voor het beantwoorden van de onderzoeksvraag van het huidige artikel is gebruik gemaakt van een selectie van zeventien interviews en twee focusgroepen. Het gaat om in totaal 32 experts: vanuit politie (13), justitie (4), reclassering (7), Halt (6), computersecurity (1) en wetenschap (1). De geselecteerde experts hebben relevante kennis van de initiatie van criminele carrières van cyberdaders en zijn bij ten minste tien (casussen van) cyberdaders betrokken geweest of hebben (in het geval van de interviews met de politie en de focusgroepen met de reclassering en Halt) in nauw contact gestaan met de dadergroep. De informatie uit de politie-interviews en focusgroepen is alleen gebruikt waar de experts hun ervaringen baseren op eigen casuïstiek. Bevindingen zijn bovendien alleen verwerkt indien deze door verschillende experts naar voren zijn gebracht. De meeste experts hadden voornamelijk zicht op cyberdaders die in beeld zijn gekomen bij politie en justitie, wat tot gevolg heeft dat uit de expertinterviews, net als uit de daderinterviews, weinig informatie naar voren kwam over de criminele carrière van cyberdaders van wie de delicten niet bekend of opgespoord zijn. Daarnaast moet ermee rekening worden gehouden dat de percepties van de experts ook beïnvloed kunnen zijn door wat zij van collega's horen of in de media lezen.

Voor het oorspronkelijke onderzoek zijn de daderinterviews en expertinterviews verbatim getranscribeerd, gecodeerd en geanalyseerd met het kwalitatieve-analyseprogramma Atlas.ti. Voor dit artikel zijn de interviews (aanvullend) geanalyseerd vanuit de concepten die uit het huidige theoretisch kader voortvloeien. Ook is in de analyse nader ingezoomd op wat de daders zeggen over de (pre-)initiatiefase, waarvoor de interviews zijn gecodeerd aan de hand van thema's als: het delict, interesse in techniek of gamen, vaardigheden, het ontstaan van de carrière, de rol van de online en offline omgeving, normatieve inzichten en psychologische aspecten.

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

Empirische bevindingen

Paden in de (pre-)initiatie

Als het gaat om de vraag hoe en waarom daders starten met een cybercriminele carrière blijken uit onze data in de eerste plaats dat er duidelijke verschillen bestaan tussen jeugdige en volwassen starters wat betreft de drijfveren en de context die het gedrag tot stand brengen. Daarbinnen zien we variatie als het gaat om de legale of illegale setting van waaruit men in de cybercriminaliteit terechtkomt. In onze data zijn verschillende ontwikkelingspaden zichtbaar, zowel bij jeugdige daders als bij daders die in de volwassenheid starten met het plegen van cyberdelicten.

- *Jeugdige starters*

Elf van de geïnterviewde daders pleegden het eerste cyberdelict toen zij tussen de 10 en 18 jaar oud waren. Daarbinnen kunnen op basis van ons onderzoek drie ontwikkelingspaden onderscheiden worden.

Allereerst zien we jeugdige daders die heel nadrukkelijk vanuit een technisch exploratieve fase in aanraking komen met cybercriminaliteit. Negen van de geïnterviewde daders hebben van jongs af aan (basisschoolleeftijd) al veel interesse in (de werking van) ICT en computers. Zij groeiden er letterlijk mee op en computers, internet en programmeren waren meestal reeds op jonge leeftijd een onderdeel van hun dagelijkse leven. Deze daders leggen hun motivatie uit in termen als 'gewoon kijken hoe ver we konden komen' (RD10) en 'ik probeerde het gewoon en het werkte' (RD8). Het opzettelijk misbruik maken van digitale systemen of gegevens en het hebben van financiële motieven lijken nauwelijks een rol te spelen bij de initiatie. Zij gaan steeds een klein stapje verder en de initiatie wordt echt beschreven als een proces. Een ander deel van de jeugdige starters lijkt wel een concreet transitiepunt te herkennen waarbij een specifieke interesse ontstond voor illegale vormen van hacken, waarna de jeugdige zich bewust is gaan bezighouden met dit soort praktijken. De deelname aan hackerfora wordt in dit kader als een belangrijke factor genoemd. De centrale motieven van de meer technologisch georiënteerde starters, of ze nu meer of minder bewust in de cybercriminaliteit zijn gerold, zijn uitdaging, erkenning (voor talenten), spanning en macht over een persoon, machine of systeem. Volgens tien van de experts lijken deze daders niet doelbewust de online grenzen te willen overschrijden, maar laten zij zich meeslepen in de opwinding en de mogelijkheden c.q. toegankelijkheden van de techniek.

Een ander ontwikkelingspad dat uit de data naar voren komt, is dat van daders die heel expliciet via gamen bij cybercriminaliteit terechtkomen. De interesse in cybercriminaliteit kan volgens daders en zes van de experts in de eerste plaats ontstaan via gaming, omdat spelers binnen de setting van de game in aanraking komen met cybercriminaliteit. Drie geïnterviewde daders beschrijven dat ze op jonge leeftijd gehackt zijn in een spel via onder meer social engineering[5] en dat zo

5 Bij social engineering worden mensen misleid om persoonlijke gegevens te verstrekken, zoals wachtwoorden.

hun interesse is gewekt. Zo beschrijft een van hen: 'Toen dacht ik maar hé, als het zo makkelijk is voor iemand om mijn wachtwoord te krijgen, dan ben ik ook benieuwd hoe makkelijk ik iemand anders wachtwoord kan krijgen' (RD4). Verschillende daders geven aan dat het plegen van delicten begint in de spelsetting (bijvoorbeeld elkaar ddos'en), maar dat het zich op een gegeven moment verplaatst naar andere settingen. In de tweede plaats kan de interesse in gamen daders op online (game)fora brengen, waar ze in aanraking komen met illegale handelingen. Gamen kan echter, afgaande op de daderinterviews, ook hand in hand gaan met een technisch exploratieve fase (vooraf, gelijktijdig of erna). In dat opzicht zijn de twee initiatiepaden niet helemaal separaat en kan er sprake zijn van een overlap. Motieven die in het tweede initiatiepad centraal staan, zijn – afgaande op de daderinterviews – vrij divers, variërend van spanning, plezier en uitdaging tot financieel gewin (zoals bij virtuele diefstal in een spel).
Tot slot suggereren de bevindingen nog een derde ontwikkelingspad bij jeugdige starters, namelijk daders bij wie de interesse voor cybercriminaliteit in een offline setting ontstaat, bijvoorbeeld op school. In dat geval is het verkrijgen van status of het uithalen van 'kattenkwaad' het voornaamste motief. Een van de geïnterviewde daders geeft aan dit pad bewandeld te hebben. Hij wilde de school hacken om hierover te kunnen opscheppen tegen vrienden en is online gaan opzoeken hoe dit gedaan kan worden. Een andere dader had een soortgelijk motief en pleegde het delict in eenzelfde soort setting, maar was ook zelf al jarenlang bezig met computers en IT (technisch exploratieve fase) en had dus goede vaardigheden. Ook hier kan er een overlap zijn tussen de ontwikkelingspaden.

- *Volwassen starters*

Niet alle cyberdaders starten op jeugdige leeftijd. Ook volwassenen kunnen een carrière beginnen in de cybercriminaliteit. Als het gaat om de setting van waaruit zij starten, kunnen op basis van de data twee ontwikkelingspaden onderscheiden worden.
Ten eerste bestaat er een ontwikkelingspad waarbij daders de overstap maken van traditionele criminaliteit naar cybercriminaliteit of het werkterrein uitbreiden naar het digitale domein. Slechts één geïnterviewde dader lijkt deels in dit initiatiepad te passen. Voor deze opportunistische dader was het internet een uitbreiding van de (traditionele) fraudedelicten waarmee hij in die periode al bezig was. Het gaf hem naar eigen zeggen toegang tot een grotere 'vijver' van potentiële slachtoffers. Het begon met dingen uitproberen, maar toen het lukte, is hij steeds verder gegaan, steeds meer gaan verdienen, en is hij de delicten (phishing en fraude) ook in georganiseerd verband gaan uitvoeren. Door met name de politie-experts wordt gewezen op dit ontwikkelingspad. Sommigen van hen beschrijven een aparte 'dadercategorie' van 'echte boeven' of 'streetwise' criminelen, voor wie het plegen van criminaliteit en het af en toe vastzitten een levensstijl is. Ze hebben vaak al een criminele carrière op het gebied van traditionele criminaliteit (met name fraude en oplichting) achter de rug en/of blijven daar soms ook nog deels in actief.
Ten tweede komt een ontwikkelingspad naar voren waarbij de volwassen (traditionele) dader een cyberdelict pleegt in het kader van een klassiek delict, bijvoor-

doi: 10.5553/TvC/0165182X2021063001002

beeld in de zedensfeer. Daarbij gaat het om motieven zoals wraak of lust. Het cyberdelict is daarbij vooral een middel (denk aan het stelen van foto's van de expartner door middel van hacken) en niet een doel op zich. Het gaat hier in veel gevallen om laagdrempelige vormen van hacken, zoals het raden van het wachtwoord. Twee van de geïnterviewde daders waren verdacht van of veroordeeld voor computervredebreuk in de persoonlijke en zedensfeer. Zij gaven aan hiervoor nooit cyber- of andere delicten te hebben gepleegd en zagen zichzelf ook niet als cybercrimineel, omdat ze nauwelijks verstand hebben van computers. Door enkele politie-experts wordt op basis van verdachtenregistraties aangegeven dat een redelijk grote groep volwassen cyberdaders dit pad lijkt te volgen. Ook reclasseringsmedewerkers en advocaten komen dit ontwikkelingspad geregeld tegen.
Kortom, de bevindingen suggereren dat zowel bij jeugdige als bij volwassen starters variatie bestaat als het gaat om hoe de criminele carrière begint. In de volgende paragrafen zullen we nader ingaan op de verschillende verklaringen die het ontstaan van de criminele carrière van (verschillende) jeugdige en volwassen starters nader kunnen duiden. We maken hierbij onderscheid tussen drie soorten verklaringen: (1) sociale online disinhibitie, (2) technische en situationele online disinhibitie en (3) psychologische online disinhibitie, waarbinnen ook de koppeling wordt gemaakt met traditionele theorieën. Belangrijk om aan te geven is dat de drie vormen van online disinhibitie met elkaar verbonden zijn en dus niet helemaal los van elkaar beschouwd kunnen worden.

Sociale online disinhibitie

Op verschillende manieren zorgt het internet voor een zekere sociale laagdrempeligheid, wat inhoudt dat er via online gemeenschappen eenvoudige toegang is tot gelijkgestemde (delinquente) peers. De online gemeenschappen vervullen volgens acht van de veertien daders een belangrijke sociale functie. Het wordt door hen beschreven als 'een stukje sociaal contact' en de relatie met peers als een vriendschap of een band. Het stelt hen in staat om met gelijkgestemden te praten die dezelfde interesses hebben. Deze aansluiting vinden ze niet altijd in hun offline netwerk, en evenmin vinden ze op school de uitdaging of erkenning die ze zoeken op technisch vlak. Een dader beschrijft het forum dan ook als 'mijn wereldje waar ik me wel thuis voelde. Het was een ontsnapping' (RD11). Hoewel dit in de daderinterviews minder naar voren is gekomen, wijzen negen van de experts daarnaast op jeugdige cyberdaders die sociaal geïsoleerd zijn en online *wel* aansluiting vinden, waardoor tijd doorbrengen in de online omgeving voor hen veel aantrekkelijker wordt. Tegelijkertijd wijzen de daders op de competitieve aard van online gemeenschappen waarin ze actief waren en op de noodzaak om jezelf te bewijzen en je vaardigheden te tonen als je wilt doorgroeien in de hiërarchie. In dat opzicht kunnen we veronderstellen dat de competitieve aard die inherent is aan dit soort gemeenschappen bepaalde (deviante) groepsprocessen, zoals elkaar opjutten, kan versterken. (Offline) sociale geïsoleerdheid en een (offline) gebrek aan erkenning voor talent kunnen daarbij een versterkend effect hebben, hoewel dit niet bij iedere jeugdige dader een rol speelt.

De online gemeenschappen zijn tegelijkertijd plekken waar normen, waarden en procriminele attitudes kunnen worden overgedragen, gevormd en bekrachtigd, iets wat in zowel de dader- als de expertinterviews naar voren komt als een belangrijke verklaring voor het ontstaan van een criminele carrière. Hoewel sommige online platformen illegale activiteiten afkeuren in hun regels of richtlijnen, blijkt uit de daderinterviews dat men op dergelijke plekken niettemin op grote schaal blootgesteld kan worden aan illegale activiteiten. Naast het uitvoeren van ddos-aanvallen of het hacken van medespelers, zijn zij op fora in aanraking gekomen met lijsten met gestolen creditcardgegevens, remote access tools, instructies voor SQL-injecties en social-engineeringtechnieken om te frauderen. Spatiotemporele barrières spelen bovendien geen rol, zodat zij op deze platformen 24/7 met mensen over de hele wereld over (al dan niet illegale) zaken kunnen communiceren. Online ontstaat sneller het gevoel dat niets verboden is, en worden bestaande gedragsnormen overschaduwd door online gedragsnormen. De overvloed aan deviante attitudes waaraan zij worden blootgesteld, leidt vervolgens tot normalisering.

> '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.' (RD14)

De normalisering van deviante online gedragsnormen kan zodoende worden versterkt door de omvang van het aantal like-minded peers dat crimineel gedrag schijnt te bevestigen en goed te praten (de duizenden bezoekers op een forum, bijvoorbeeld). Ook de eerder besproken competitieve aard van de online gemeenschappen kan processen van normalisering en normvervaging versterken, door het feit dat daders elkaar opjutten om iets te hacken (en hierbij altijd om bewijs vragen), opscheppen over hun daden en ook onderling 'scores' vergelijken. Op die manier wordt een eigen werkelijkheid of eigen moraal gecreëerd binnen het online netwerk.

Ten slotte speelt bij jeugdige cyberdaders ook het gebrek aan ouderlijk toezicht een rol. Acht daders stellen dat hun ouders zich niet met hun online gedrag bemoeiden en dat zij niet wisten wat zij online allemaal uitspookten, of dat ze de online problematiek wel signaleerden, maar hier weinig adequaat op wisten te reageren vanwege een kennisachterstand. Het blijft vaak bij een waarschuwing, want echte controle op de online activiteiten van hun kind is nauwelijks uit te voeren. Opvallend is dat bij twee daders het strafbare gedrag door familieleden niet werd afgekeurd en de technische prestatie juist werd gewaardeerd. 'Mijn opa die vond het op zich ook wel grappig' (RD6). Uit geen van de daderinterviews kwam naar voren dat zij door hun ouders voor het delictgedrag zijn gestraft.

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

Technische en situationele online disinhibitie

Naast een sociale laagdrempeligheid laten de bevindingen zien dat het internet op verschillende manieren ook een technische en situationele laagdrempeligheid biedt. Hier gaat het om het feit dat doelwitten niet altijd goed beschermd zijn. Ook is er eenvoudige toegang tot informatie en (kant-en-klare) tools die nodig zijn om cyberdelicten te plegen, en is sprake van afwezigheid van adequaat toezicht.

Negen daders geven aan gebruik te hebben gemaakt van instructies op fora of in video's, waarin bijvoorbeeld wordt uitgelegd hoe je delicten pleegt of hoe je een IP-adres kunt vinden (waar dan de ddos-aanval op gericht wordt). Daarnaast wijzen zowel de daders als de experts op de grote variëteit aan kant-en-klare tools die beschikbaar is op het internet, die vaak tegen geringe betaling worden aangeboden en makkelijk in gebruik zijn, zonder dat dit veel technische vaardigheden vereist. Het gemak van de handelingen wordt beschreven in termen als 'click and go' (RD12) of 'plug and play' (RE13, OM). Dergelijke kant-en-klare tools spelen volgens de daders een faciliterende rol, maar slechts bij één dader had de toegang tot dit soort tools een doorslaggevende rol. Het lage instapniveau als gevolg van tools, diensten en instructies heeft volgens enkele experts ertoe geleid dat er een nieuwe categorie cyberdaders is opgekomen waarbij technologische fascinatie of verkenningsdrift nauwelijks een rol speelt. Dit laatste zou betrekking kunnen hebben op de eerder besproken ontwikkelingspaden van gamers en jeugdige daders die via het schoolplein in aanraking komen met cybercriminaliteit. Ook kan dit van toepassing zijn op de ontwikkelingstrajecten van volwassen starters.

Negen daders beschrijven dat bestaande tools, scripts, bots en keyloggers in de beginfase een grote rol spelen als onderdeel van het leerproces, maar ook later in de criminele carrière zijn ze van belang. De tools beschouwen zij vooral als een onderdeel van de gereedschapskist die zij gebruiken; sommige stappen doen zij liever handmatig (bijvoorbeeld een bepaalde kwetsbaarheid zoeken), om daarna het programma voor een vervolghandeling te gebruiken (bijvoorbeeld de kwetsbaarheid misbruiken). Soms passen ze de code aan (wat vereist dat zij de sourcecode doorgronden om deze te kunnen 'finetunen'), of ze schrijven zelf een programma. Het maken van eigen tools is volgens sommige daders niet per se een kwestie van vaardigheden, maar ook een kwestie van voorkeur: 'Ik heb zelf heel veel tooltjes gemaakt, ik hield er ook niet echt van om dingen te gebruiken die andere mensen maakten. Eigenlijk wilde ik altijd zelf alles maken' (RD8).

Het belang van kant-en-klare tools, zoals phishing kits, wordt ook door experts onderstreept, met name als het gaat om volwassen starters met een financieel motief. Dit soort tool(kits) maakt het relatief eenvoudig om een switch te maken van offline criminaliteit naar online criminaliteit. Daarnaast wordt gewezen op de rol van crime-as-a-service, wat verwijst naar het feit dat er online tal van actoren actief zijn die verschillende (illegale) diensten aanbieden, zoals bulletproof hosting, het versturen van spam, het beheren van botnets of het regelen van money mules. Ook het bestaan van dit soort services – zodat allerlei handelingen uitbesteed kunnen worden – maakt het instapniveau volgens experts lager.

Naast toegang tot informatie en tools kunnen de afwezigheid van toezicht en de geringe pakkans een rol spelen bij de initiatie, omdat er weinig barrières worden opgelegd om te experimenteren dan wel kwetsbaarheden te exploiteren. Een opvallende uitkomst is dat drie daders tijdens het plegen van het delict geen maatregelen hebben genomen om hun identiteit te verbergen, omdat ze niet bewust met anonimisering bezig waren. Dit zou erop kunnen wijzen dat daders zich anoniemer of onaantastbaarder waanden dan ze daadwerkelijk waren. Het zou er ook op kunnen duiden dat zij enkel wilden uitproberen hoever ze zouden komen, vanuit nieuwsgierigheid of kattenkwaad in plaats van het willens en wetens overtreden van de online grenzen.

Psychologische online disinhibitie

Terwijl peergroepen van hackers en gamers, evenals de beschikbaarheid van kant-en-klare tools als sterke aanjagers gelden voor het ontstaan van een cybercriminele carrière, ontbreekt het tegelijkertijd in de online omgeving voor zowel jeugdige als volwassen daders in veel gevallen aan adequate (psychologische) inhibitie en morele verantwoordelijkheid voor hun gedrag. Hiervoor zijn traditionele verklaringen toepasbaar, maar deze moeten worden gezien in het licht van de online omgeving. Ten eerste lijkt bij de jonge daders de ontwikkeling van de cognitieve en psychosociale inzichten in morele kwesties onvoldoende ontwikkeld. Daders benoemen dit expliciet als zodanig en benadrukken hun 'kind zijn' en 'onvolwassenheid': 'Omdat ik een kind was. Dat soort dingen deed je gewoon. Het is dezelfde periode dat ik met mijn broertje naar een verlaten schoolgebouw ging om in te breken, dat is leuk, dat is spelen' (RD12). Dat jongeren de gevolgen van hun daden (voor zichzelf en anderen) nog onvoldoende kunnen overzien, wordt door twaalf van de experts bevestigd.

Ten tweede versterken de anonimiteit, de beperkte zichtbaarheid van de schade en de afstand tot het slachtoffer bij zowel jeugdige als volwassen daders de psychologische online disinhibitie. Door de beschikbaarheid van anonimiseringstools, zoals VPN of Tor (technische online disinhibitie), of middels nicknames kunnen daders zich anonimiseren. Dat het delict 'achter de schermen' plaatsvindt, heeft een tweeledige uitwerking. Enerzijds vereist online crimineel gedrag geen fysieke handeling (ergens binnenstappen, een object weg moeten nemen); er is sprake van 'veilig achter een beeldscherm zitten'. Online kan het ervaren van fysieke consequenties worden beperkt, wat een gevoel geeft van privacy en veiligheid. Anderzijds geldt dat niet alleen het delict, maar ook de gevolgen ervan zich 'achter het scherm' voltrekken. Sommige daders zeggen zich niet of nauwelijks bewust te zijn geweest van de schade en/of het slachtoffer. Tussen de dader en het slachtoffer c.q. de schade bestaat een grote afstand en vindt geen directe confrontatie plaats, wat volgens de daders het plegen van een delict vergemakkelijkt. 'Je zag die mensen niet, of het uiteindelijke slachtoffer zag je niet. Dus dat maakt het misschien ietwat drempelverlagend' (RD1). Een andere dader (RD8) beschrijft de slachtoffers als een paar willekeurige vissen in een grote oceaan; hij

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

had geen idee wie hij precies hackte. Ook hij werd niet direct met de schade geconfronteerd. Dit laatste speelt ook sterk bij ddos-aanvallen.

> '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.' (RD6)

De afstandsinteractie maakt het volgens experts lastig voor daders om zich te verplaatsen in het slachtoffer en de gevolgen van hun daden. Hier komt bij dat specifiek voor adolescenten geldt dat zij doorgaans nog niet voldoende in staat zijn de langetermijngevolgen van hun handelen te overzien. Aanvullend is er sprake van een zeker spelelement of alternatieve realiteit. De virtuele en fysieke wereld worden als twee losse werelden ervaren en in de online wereld gelden andere regels en normen dan in het alledaagse leven. Vijf daders zien computervredebreuk niet als iets schadelijks, omdat het systeem 'slechts' is binnengedrongen: 'Alleen als ik gewoon sec kijk, zijn er eigenlijk niet slachtoffers in de zin van er is nooit van andere mensen iets gepubliceerd' (RD3). Deze alternatieve realiteit wordt nog eens versterkt door het gemak waarmee sommige systemen binnen te treden zijn en de opwinding die dat teweeg kan brengen.

> '[De buren] hadden geen wachtwoord op hun wifi. Maar ze verstuurden allemaal onversleutelde wachtwoorden over het netwerk (...) Ja wat doe je daarmee als 15-jarige scriptkiddie: die gaat inloggen. Ja, je ziet die wachtwoorden in plaintext voorbij komen, wat doe je anders, het is zo verleidelijk, niet nadenkend over de gevolgen. Dus ja ik was ingelogd, van geen kwaad bewust, het is zo makkelijk in te komen, dat was niks. Het is zo makkelijk, ze laten de sleutel er gewoon in.' (RD11)

Er zijn dan ook verschillende daders (vijf) die niet zozeer ontkennen dat er een slachtoffer is, maar wel de schuld bij het slachtoffer leggen of het slachtoffer juist als 'dader' van het (data)lek zien. Slachtoffers gebruiken volgens daders bijvoorbeeld makkelijke wachtwoorden, hebben onvoldoende beveiligingsmaatregelen getroffen of werken met verouderde systemen, waardoor ze de aanval op hun systemen als het ware over zichzelf hebben afgeroepen.
Anonimiteit en het spelelement kunnen er bovendien toe leiden dat iemand zich online de identiteit kan aanmeten die hij of zij wil. Deze zelf vormgegeven online identiteit lijkt vooral ten grondslag te liggen aan delictgedrag bij jongeren die sterk op zoek zijn naar een eigen identiteit en voor wie delinquent gedrag statusverhogend kan werken. Zo vertellen zeven daders dat het delict hun status of trots opleverde (bijvoorbeeld als er in de media aandacht aan werd besteed). Soms werd er bovendien door vrienden of familieleden waardering geuit. Ook kan de online identiteit een gevoel van macht opleveren. Een jonge dader duidt die macht (terugblikkend op zijn delictgedrag, waardoor hij toegang had tot informatie van medescholieren die hem pestten) als 'een soort payback gevoel', 'leveling the playing field' en 'ik ben uiteindelijk de baas hier' (RD10). Een expert

van het Openbaar Ministerie (OM) legt uit dat je online een ideaalbeeld van jezelf kunt creëren, waarbij het de vraag is hoever je gaat (psychologische disinhibitie) om dat beeld bevestigd te krijgen:

> 'En als het contrast tussen wie jij bent en jouw alter ego, als dat heel groot is, waarbij je digitale alter ego dichterbij je ideaalbeeld komt van hoe jij wilt zijn, dat je misschien de neiging hebt om je meer daarop te richten dan op je fysieke ego. Dat kan ik me goed voorstellen. Dat je dan toch vlucht in dat ideaalbeeld. Dan ga je opzoek naar de omgeving, of je bevindt je in een online omgeving, waarin je wordt bevestigd in dat beeld.' (RE13, OM)

Tot slot lijkt bij daders niet altijd goed duidelijk te zijn welk gedrag strafbaar is. Zes daders beschrijven hun handelingen als een 'kwajongensstreek', 'kattenkwaad' of 'een spelletje'. Zij kijken uit nieuwsgierigheid rond in systemen en zien dit als een soort spel, zonder zich direct de strafbaarheid te realiseren. Ook is niet altijd duidelijk waar precies de grenzen liggen. In dit kader kwam in veel interviews het thema Coordinated Vulnerability Disclosure (CVD) naar voren.[6] Een van de daders, die zichzelf inmiddels als ethische hacker beschouwt (RD4), zegt te begrijpen dat jongeren geen idee hebben wat wel of niet mag, omdat voor hem ook niet altijd duidelijk is wat er precies onder CVD valt. Twee van de volwassen daders geven daarentegen aan dat zij zich wel goed realiseerden dat ze dingen deden die strafbaar zijn. Dit zou te maken kunnen hebben met de aard van de gedraging (fraude en virtuele diefstal) of met het feit dat deze daders ouder zijn en een beter inzicht hebben in normatieve kwesties. Ook de experts denken hier onderling verschillend over: een deel meent dat er (nog steeds) een groot grijs gebied bestaat ten aanzien van de juridische gevolgen (inclusief een strafblad) die aan cybercriminaliteit verbonden zijn. Dit geldt vooral voor jeugdige daders die door (de intrinsieke motivaties) interesse en uitdaging worden gedreven. Volgens experts zouden sommige daders in de veronderstelling 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. Volgens een ander deel zijn de online grenzen ondertussen uitgekristalliseerd en in hackersgemeenschappen duidelijk bekend.

Conclusie

In deze bijdrage is op basis van dader- en expertinterviews onderzocht hoe criminele carrières in cybercriminaliteit in enge zin ontstaan en welke verklaringen daarbij een rol spelen. Hieruit volgt dat een onderscheid gemaakt kan worden tussen drie ontwikkelingspaden van jeugdige starters en twee ontwikkelingspaden van volwassen starters. De initiatie bij de drie ontwikkelingspaden van jeugdige daders vindt plaats via respectievelijk een technische exploratieve fase, via

6 Op basis van het CVD-beleid is hacken toegestaan als is voldaan aan het op een gecoördineerde wijze bekendmaken van ICT-kwetsbaarheden op basis van door organisaties hiervoor vastgesteld beleid (NCSC, 2018).

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

gaming, of in een offline setting zoals de school. Ook kan er sprake zijn van combinaties van initiatietrajecten. Bij volwassen starters kan het in de eerste plaats gaan om opportunistische daders die zijn doorgestroomd vanuit de traditionele misdaad, en in de tweede plaats om traditionele daders met psychologische drijfveren (bijvoorbeeld wraak), voor wie cybercriminaliteit slechts een nieuw middel is. Vervolgonderzoek zou moeten uitwijzen of de door ons beschreven ontwikkelingspaden ook breder van toepassing zijn.

Wat betreft verklaringen zien we dat de traditionele theorieën, leertheorieën en sociale controletheorieën, gelegenheidsbenaderingen en het tweepadenmodel van Moffitt (1993) zeker verklaringskracht hebben voor cyberdaders. De bevindingen tonen aan dat jeugdige cyberdaders zich, net als *adolescence-limited* daders, onttrekken aan het ouderlijk gezag of toezicht, gevoelig zijn voor de invloed van peers, op zoek zijn naar status of erkenning, en dat ze onvoldoende inzicht in normatieve kwesties of de gevolgen van hun handelingen hebben. Bij de volwassen daders speelt gelegenheid een belangrijke rol, in de vorm van toegang op grotere schaal tot slachtoffers en een lager instapniveau als gevolg van kant-en-klare tools, instructies en diensten. Met name politie-experts zien, hoewel niet bevestigd in onze daderinterviews, dat juist in deze groep ook een aantal *life-course-persistent* daders actief zijn. Het is echter niet duidelijk of de daders op wie deze experts wijzen, tijdens de initiatiefase van hun criminele carrière ook in de cybercriminaliteit actief waren. In de meeste gevallen maakten zij hun initiatiefase in de traditionele criminaliteit door.

De online omgeving versterkt of verzwakt echter bepaalde mechanismen uit deze traditionele verklaringen. Zo is – in overeenstemming met de affordance-benadering van Goldsmith en Wall (2019) en het online disinhibitie-effect van Suler (2004) – gebleken dat toegang tot het internet het mogelijk maakt dat (met name jeugdige) daders frequenter en op een grotere schaal blootgesteld worden aan (ambivalentie ten aanzien van) deviant gedrag. Een proces dat geleidelijk aan leidt tot normalisering van cybercriminaliteit (*sociale online disinhibitie*). Daarnaast is het instapniveau van cybercriminaliteit voor zowel jeugdige als volwassen daders laag door onder meer de toegankelijkheid en betaalbaarheid van tools en instructies die in overvloed aanwezig zijn, en het beperkte toezicht op online gedrag (*technische en situationele online disinhibitie*). Tegelijkertijd maken de digitale context en ervaren anonimiteit dat het plegen van het delict kan voelen als een spel of hyperrealiteit, zonder dat een link wordt ervaren met de fysieke identiteit (*plasticiteit van de identiteit*) of gevolgen in de fysieke wereld (*dissociatieve verbeelding*). Doordat het delict zich 'achter de schermen' voltrekt, staan daders slechts beperkt stil bij het slachtoffer en de schade. Gecombineerd met het feit dat de grenzen van wat strafbaar is online niet altijd duidelijk zijn, zijn er weinig psychologische remmingen (*psychologische online disinhibitie*).

Het onderzoek laat dus zien dat er online niet alleen sprake is van psychologische disinhibitie – waar in de cybercriminologie relatief veel aandacht voor is –, maar ook van sociale, technische en situationele disinhibitie. Het duiden van de samenhang en wisselwerking tussen deze verschillende vormen van disinhibitie is ons inziens essentieel om de initiatie volledig te begrijpen. Voor toekomstig onderzoek zou het interessant zijn om de verschillende vormen van disinhibitie

te onderzoeken voor andere fasen van de criminele carrière en zou onderzocht kunnen worden in hoeverre het effect van de verschillende vormen van disinhibitie over tijd verandert. Tevens zou er nog meer onderzoek gedaan kunnen worden naar de rol van de verschillende soorten disinhibitie bij volwassen starters, waar in het huidige onderzoek vrij beperkt zicht op is verkregen. Naast technische en situationele disinhibitie spelen sociale en psychologische disinhibitie naar alle waarschijnlijkheid ook een rol bij deze groep(en) daders.

De bevindingen uit het onderzoek bieden ook aanknopingspunten voor de praktijk. Ten eerste is gebleken dat sociale en situationele online disinhibitie een belangrijke rol spelen in het ontstaan van een criminele carrière, o.a. door gebrek aan (ouderlijk) toezicht, deviante leerprocessen en normvervaging. Gekeken zou kunnen worden naar effectieve manieren van toezicht en bijsturing in de online sociale context. Een voorbeeld hiervan is de pilot 'Gamen met de politie', die tijdens de coronacrisis is gestart.[7] Voor volwassen daders zou een combinatie van meer online toezicht en meer verstoringsmaatregelen (bijvoorbeeld gericht op criminele serviceproviders) effectief kunnen zijn, juist om de overstap naar cybercriminaliteit minder aantrekkelijk te maken. Ten tweede blijkt er met name bij jeugdige daders door psychologische online disinhibitie beperkt inzicht te zijn in de strafbaarheid, het slachtoffer en de schade. Er dient bij jeugdige daders meer ingezet te worden op communicatie en bewustwording van de risico's van de online omgeving, de financiële en emotionele schade van cybercriminaliteit en de wettelijke grenzen. Een voorbeeld hiervan is de voorlichtingscampagne van de politie 'Je bent slechts één klik verwijderd van cybercrime' waarbij jongeren gewezen worden op de strafbaarheid van cybercriminaliteit.[8] Ook is hierin een rol weggelegd voor ouders, scholen en de overheid, evenals voor de (legale) online (hacker)gemeenschap zelf. Ethische hackers, die eventueel in het verleden zelf cyberdelicten hebben gepleegd, zouden juist goed als rolmodel kunnen fungeren en het morele kompas van jonge daders kunnen bijschaven. Ten derde blijkt dat een vrij groot deel van de jeugdige daders verzeild raakt in cybercriminaliteit vanwege nieuwsgierige exploratie en een interesse in techniek of gamen. Door dergelijke jongeren te informeren over alternatieven, zoals ethisch leren hacken of hackwedstrijden, wordt hun de gelegenheid geboden op een prosociale manier de sterk aanwezige drijfveren (nieuwsgierigheid, uitdaging, status) te realiseren. Ten slotte is noodzakelijk dat ambivalentie over wat wel en niet onder CVD valt door overheid en bedrijven zo veel mogelijk wordt weggenomen. Zo kan wellicht de start van een cybercriminele carrière worden voorkomen en de start van een legale carrière in de cybersecurity bevorderd worden.

7 Zie www.vraaghetdepolitie.nl/pesten-en-online/gamen-met-de-politie.html (laatst geraadpleegd 27 januari 2021).

8 Zie www.politie.nl/nieuws/2019/februari/13/00-9456-jongeren-een-klik-verwijderd-van-cyber crime.html (laatst geraadpleegd 27 januari 2021).

Tijdschrift voor Criminologie 2021 (63) 1
doi: 10.5553/TvC/0165182X2021063001002

Literatuur

Aiken, M., Davidson, J. & Amann, D. (2016). *Youth Pathways into Cybercrime.* Europol: European Cybercrime Centre/UCD Geary Institute for Public Policy/Middlesex University.

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.

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 cybercrime: an analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology, 8*(1), 1-20.

CBS (Centraal Bureau voor de Statistiek). (2020). *Minder traditionele criminaliteit, meer cybercrime.* Geraadpleegd op www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime.

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.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44*(4), 588-608.

Goldsmith, A. & Wall, D.S. (2019). The seductions of cybercrime: adolescence and the thrills of digital transgression. *European Journal of Criminology*, 1-20.

Hoek van Dijke, N. (2016). *Onderzoeksrapportage. Jongeren over cybercrime en gedigitaliseerde criminaliteit.* Den Haag: Ministerie van Justitie en Veiligheid.

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.

Hutchings, A. (2016). Cybercrime trajectories: an integrated theory of initiation, maintenance and desistance. In: T.J. Holt (ed.). *Crime Online: Correlates, Causes, and Context*. Durham: Carolina Academic Press, 117-140.

Katz, J. (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil.* New York: Basic Books.

Kerstens, J. & Stol, W. (2012). *Jeugd en cybersafety. Online slachtoffer- en daderschap onder Nederlandse jongeren.* Den Haag: Boom Lemma uitgevers.

Kerstens, J. & Veenstra, S. (2013). Cyberpesten vanuit een criminologisch perspectief. *Tijdschrift voor Criminologie, 55*(4), 375-393.

Kirwan, G. & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders.* Cambridge: Cambridge University Press.

Kleemans, E.R. & Poot, C.J. de (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology, 5*(1), 69-98.

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.

Lensink, H. & Vuijst, F. (2015, 1 februari). Hoe hacker David Schrooten afgleed naar de donkere kant. *Vrij Nederland.* Geraadpleegd op www.vn.nl/hoe-hacker-david-schrootenafgleed-naar-de-donkere-kant/ .

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.

Moffitt, T.E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: a developmental taxonomy. *Psychological Review, 100*(4), 674-701.

NCA (National Crime Agency). (2017). *Pathways into Cyber Crime.* Retrieved from www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file/.

NCSC (Nationaal Cyber Security Centrum). (2018). *Coordinated Vulnerability Disclosure: De leidraad.* Den Haag.

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.

Piquero, N.L. & Benson, M.L. (2004). White-collar crime and criminal careers: specifying a trajectory of punctuated situational offending. *Journal of Contemporary Criminal Justice, 20*(2), 148-165.

Rogers, M.K. (2010). The psyche of cybercriminals: a psycho-social perspective. In: S. Ghosh & E. Turrini (eds.). *Cybercrimes: A Multidisciplinary Analysis.* Heidelberg: Springer, 217-235.

Steinmetz, K.F. (2015). Craft(y)ness. An ethnographic study of hacking. *The British Journal of Criminology, 55*(1), 125-145.

Steinmetz, K.F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime.* New York: New York University Press.

Suler, H. (2004). The online disinhibition effect. *Cyberpsychology & Behavior,* 7(3), 321-236.

Sutherland, E.H. (1947). *Principles of Criminology.* Oxford: J.B. Lippincott.

Toolen, Y. van der, Weulen Kranenbarg, M. & Weerman, F.M. (2020). Online jeugdcriminaliteit en 'verkeerde vrienden': wanneer is de samenhang het sterkst? *Tijdschrift voor Criminologie, 62*(2-3), 153-179.

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 Rijksuniversiteit Groningen. Geraadpleegd op 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.

Wagen, W. van der, Zand-Kurtovic, E.G. van 't, Matthijsse, S.R. & Fischer, T.F.C. (2019). *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin.* Den Haag: WODC.

Warr, M. (2002). *Companions in Crime. The Social Aspects of Criminal Conduct.* New York: Cambridge University Press.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus Traditional Offenders: An Empirical Comparison.* Proefschrift Vrije Universiteit Amsterdam. Geraadpleegd op http://dare.ubvu.vu.nl/handle/1871/55530?show=full.

Weulen Kranenbarg, M., Ruiter, S., Gelder, J.L. van & 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.

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.

Zebel, S., Vries, P. de, Giebels, E., Kuttschreuter, M. & Stol, W. (2013). *Jeugdige daders van cybercrime in Nederland: een empirische verkenning.* Den Haag: WODC.