Interventies voor cyberdaders

Zand, E. van 't; Matthijsse, S.; Fischer, T.; Wagen, W. van der; Oerlemans, J.J.; Weulen Kranenbarg, M.

8 Interventies voor cyberdaders

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

8.1 Inleiding

Net als bij het toepassen van traditionele verklaringen voor criminaliteit op cybercriminaliteit staan criminologen bij de aanpak ervan voor de vraag of we kunnen volstaan met traditionele interventies, of dat er aanpassingen of zelfs nieuwe interventies nodig zijn voor cyberdaders. In dit slothoofdstuk wordt licht geworpen op interventies die effectief kunnen zijn bij de bestrijding van cybercriminaliteit. Daarmee wordt voortgebouwd op de inzichten over verschillende verschijningsvormen van cybercriminaliteit (hoofdstuk 3), verschillende daderkenmerken (hoofdstuk 4) en verschillende verklaringen die hier vanuit de criminologie voor kunnen worden gegeven (hoofdstuk 6). In dit hoofdstuk richten wij ons specifiek op cybercriminaliteit in enge zin. De reden hiervoor is dat we kunnen aannemen dat deze daders qua motieven en factoren het meest afwijken van daders van traditionele criminaliteit, wat impliceert dat het vraagstuk over passende interventies juist hier extra relevant is. Bij de meeste vormen van gedigitaliseerde criminaliteit gaat het vooral om traditionele daders voor wie ICT een nieuw middel is.

In dit hoofdstuk worden mogelijk passende interventies voor cyberdaders geanalyseerd vanuit drie perspectieven: (1) de rationele-keuzebenadering; (2) de *What Works*-benadering en (3) de *desistance*-benadering. Dit zijn perspectieven die vooral focussen op de motieven en risico- en beschermende factoren die een rol spelen bij daderschap. Situationele preventiestrategieën die specifiek gericht zijn op doelbescherming (firewalls of antivirusbescherming) en op het voorkomen van misdrijven in specifieke situaties, worden in dit hoofdstuk niet behandeld (zie paragraaf 5.2.2). Waar we spreken over interventies, kan het enerzijds gaan om reactieve interventies (oftewel

* Dr. mr. E.G. van 't Zand is werkzaam als universitair docent bij de afdeling Criminologie van de Universiteit Leiden. S.R. Matthijsse MSc, dr. T.F.C. Fischer en dr. W. van der Wagen zijn verbonden aan de sectie Criminologie van de Erasmus Universiteit Rotterdam (Erasmus School of Law) en zijn respectievelijk werkzaam als tutor, universitair hoofddocent en universitair docent.

sancties), dat wil zeggen formele straffen of maatregelen die op basis van het Wetboek van Strafrecht in reactie op crimineel gedrag kunnen volgen. Anderzijds kunnen interventies ook een preventief karakter hebben, bijvoorbeeld in de vorm van voorlichting aan het algemene publiek, scholieren of aan ouders. In dit hoofdstuk zal de focus liggen op interventies die als doel hebben (herhaald) delictgedrag bij (potentiële) daders van cybercriminaliteit in enge zin te voorkomen. Naast interventies die ontwikkeld zijn voor daders van traditionele criminaliteit en als zodanig ook ingezet kunnen worden voor daders van cybercriminaliteit, wordt ook ingegaan op interventies die specifiek zijn ontwikkeld voor cyberdaders. De focus ligt hierbij op het bespreken van Nederlandse interventies en hun potentiële effectiviteit, alhoewel veel literatuur over interventies voor cyberdaders uit de Verenigde Staten afkomstig is.

Dit hoofdstuk is als volgt opgebouwd. Allereerst wordt in paragraaf 8.2 kort besproken wat de drie benaderingen – rationele keuze, What Works en desistance – inhouden en hoe ze zich tot elkaar verhouden. Vervolgens worden de benaderingen respectievelijk in paragraaf 8.3, 8.4 en 8.5 uitvoeriger besproken en worden de bestaande interventies die binnen elk van deze benaderingen passen besproken. Paragraaf 8.6 vat het hoofdstuk kort samen en in paragraaf 8.7 en 8.8 worden discussiepunten en kernbegrippen benoemd.

8.2 Perspectieven op interventies

8.2.1 Drie benaderingen

Interventies kunnen worden ingedeeld op basis van drie verschillende hoofdbenaderingen die ook elk verschillende assumpties hebben over wat effectieve interventies zijn (Van der Wagen et al., 2019). In de eerste plaats kan de rationele-keuzebenadering inzichten bieden in passende en effectieve interventies (Cornish & Clarke, 1986). Deze benadering gaat uit van een kosten-batenafweging die daders maken voordat zij overgaan tot het plegen van criminaliteit. Deze kosten-batenratio ligt ten grondslag aan zowel de theorie van afschrikking als de gelegenheidsbenadering (Cohen & Felson, 1979). In de tweede plaats kan de What Works-benadering waardevolle inzichten bieden over wat passende en effectieve interventies zijn (Andrews et al., 1990; Andrews, Bonta, & Wormith, 2006). Deze benadering gaat er vanuit dat om effectief te zijn interventies rekening dienen te houden met specifieke kenmerken die in het *Risk-Need-Responsivity*-model centraal staan (o.a. Lipsey & Cullen, 2007; Lowenkamp, Latessa, & Holsinger, 2006). In de derde plaats

kan de desistance-benadering inzichten leveren over wat passende en effectieve interventies zijn. Deze benadering beschouwt het stoppen met criminaliteit (desistance) als een dynamisch proces dat verloopt met vallen en opstaan, zodat aansluiting moet worden gezocht bij waar de dader zich in dit proces bevindt (McNeill et al., 2012). Alle drie de benaderingen sluiten aan bij de criminologische theorieën waarop zij zijn gebaseerd en hebben zo elk als het ware een andere 'aanvliegroute' voor de aanpak van (cyber)daders en het voorkomen van recidive.

Voordat in de volgende paragrafen dieper op deze benaderingen wordt ingegaan, is het belangrijk op te merken dat ze niet zozeer naast elkaar, maar in reactie op elkaar zijn ontstaan. De What Works-benadering is ontstaan vanuit het idee dat een exclusieve focus op afschrikking uitgaande van een puur calculerende dader niet werkt. Door risicofactoren, criminogene behoeften en responsiviteit centraal te stellen beoogt de What Works-benadering een betere bijdrage te leveren aan de resocialisatie van daders. De desistance-benadering is vervolgens ontstaan vanuit kritiek op de What Works-benadering vanwege de nadruk op 'interventieprogramma's' en 'behandeling' (*treatment*) van criminogene factoren. In de desistance-benadering ligt de nadruk niet zozeer op behandeling, maar op het faciliteren van en ondersteunen bij het dynamische proces van stoppen met criminaliteit. De aanname is dat de persoon zelf de verandering in gang moet zetten maar daartoe wel gestimuleerd moet worden. Interventies zouden hieraan kunnen bijdragen. Met andere woorden, in deze benadering is meer aandacht voor *agency* van de dader in het proces van stoppen.

In dit hoofdstuk gaan we ervan uit dat alle drie de benaderingen waardevolle inzichten kunnen bieden met betrekking tot de vraag wat mogelijk effectieve interventies kunnen zijn voor daders van cybercriminaliteit in enge zin. Een strikt onderscheid is echter lang niet altijd te maken en interventies dragen vaak elementen van verschillende benaderingen in zich.

8.2.2 Toepasbaarheid van de benaderingen op cyberdaders

De rationele-keuze-, de What Works- en de desistance-benadering zijn in algemene zin gericht op het leveren van inzichten met betrekking tot het terugdringen van criminaliteit en het tegengaan van de ontwikkeling van een criminele carrière. Deze benaderingen zijn echter niet specifiek ontwikkeld met het oog op daders van cybercriminaliteit (in enge zin). We weten bijvoorbeeld het een en ander over de risico- en beschermende factoren die een rol spelen

bij bepaalde traditionele vormen van criminaliteit, zoals zeden-, gewelds- of drugsdelicten, maar we weten nog vrij weinig over de risico- en beschermende factoren en, meer in het algemeen, de toepasbaarheid van deze drie genoemde benaderingen op cybercriminaliteit. Literatuur over interventies die mogelijk effectief zijn in het tegengaan van cybercriminaliteit, is schaars (Oosterwijk & Fischer, 2017; Van der Wagen et al., 2019). Hiervoor bestaan verschillende redenen.

Ten eerste bestaan er weinig interventies die specifiek ontworpen zijn voor daders van cybercriminaliteit. Ten tweede is het onderzoek vooral van Amerikaanse bodem afkomstig en is Nederlands onderzoek momenteel beperkt voorhanden. Een derde beperking in de huidige status van de literatuur omtrent interventies voor cyberdaders is dat onderzoek grotendeels ofwel beschrijvend van aard is, waaronder over opgelegde strafsoorten en -hoogten bij cybercriminaliteit, ofwel theoretisch van aard is, bijvoorbeeld door de potentiële effectiviteit van interventies te analyseren. Als laatste beperking geldt dat de weinige empirische studies vaak van een kleine onderzoekspopulatie gebruik (konden) maken en veelal uitsluitend hackers betreffen. Over interventies voor andere typen cyberdaders, zoals daders die zich bezighouden met ddos-aanvallen, phishing of het verspreiden van ransomware, is betrekkelijk weinig kennis voorhanden. Zodoende ontbreekt feitelijk evaluatieonderzoek naar de daadwerkelijke uitkomsten van interventies die zijn toegepast op cyberdaders in Nederland. In de volgende paragrafen gaan we dieper op de verschillende benaderingen in en passen we de inzichten toe op interventies die mogelijk effectief kunnen zijn voor cyberdaders.

8.3 De rationele-keuzebenadering

8.3.1 Afschrikking en situationele criminaliteitspreventie

In relatief veel (theoretische) studies wordt de rationele-keuzebenadering toegepast op daders van cybercriminaliteit, zowel de op afschrikking gerichte theorieën als de gelegenheidstheorie met betrekking tot situationele criminaliteitspreventie. Centraal staat de calculerende mens, de perceptie van de mens als *homo economicus*, die zijn handelingen laat bepalen door een afweging van de kosten tegen de baten (Cornish & Clarke, 1986). Vanuit dit, ook wel als de 'klassieke' theorie aangeduide perspectief, geldt dat voor de calculerende dader interventies effectief zijn indien er sprake is van voldoende

afschrikking (Bentham, 1789). Anders gezegd: wanneer de baten niet opwegen tegen de kosten, zullen zij afzien van het plegen van criminaliteit.

De gelegenheidstheorie en de hiermee verbonden situationele criminaliteitspreventie leggen de nadruk op het verminderen van de gelegenheid tot het plegen van delicten en het beïnvloeden van de daarmee verbonden (rationele) keuze of motivatie van de dader (zie voor een uitgebreide bespreking hiervan hoofdstuk 6). Omgevingsgerichte interventies zouden mogelijk niet alleen voor de fysieke, maar ook voor de digitale omgeving kunnen werken (Leukfeldt & Yar, 2016). Daarvoor kunnen verschillende strategieën worden ingezet. Clarke en Felson (1993) hebben een specifiek model van situationele criminaliteitspreventie ontwikkeld, waarin 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. Door bijvoorbeeld het toezicht (en daarmee de moeite) te vergroten neemt de risicoperceptie toe en neemt dus mogelijk de motivatie om delicten te plegen af.

Binnen de afschrikkingstheorie wordt een onderscheid gemaakt tussen twee vormen van afschrikking, namelijk generale en speciale afschrikking. Generale afschrikking is gericht op het afschrikken van niet-gestraften (zowel criminelen als niet-criminelen) zodat zij ontmoedigd worden om criminaliteit te plegen. Speciale afschrikking is gericht op de gestrafte, die door de afschrikwekkende werking van de opgelegde straf niet opnieuw de fout ingaat (Kleck et al., 2005). Conform de rationele-keuzetheorie moeten de kosten worden verhoogd door enerzijds de strafdreiging (wettelijke sanctie) te verhogen 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).

De theorie van afschrikking gaat ervan uit dat de volgende elementen van straf invloed hebben op de mate van afschrikking: hoe groter de zekerheid (*certainty*), zwaarte (*severity*) en snelheid (*swiftness*) van de straf, hoe lager de criminaliteit (Gibbs, 1975; Kleck et al., 2005). De perceptie van de dader speelt hierbij een belangrijke rol. Om voldoende afschrikwekkend te zijn moeten daders dus de perceptie hebben dat interventies *zeker* en *snel* volgen op crimineel gedrag en voldoende *streng* zijn. Dit is bij cybercriminaliteit echter niet altijd het geval.

Ten eerste is niet alleen de pakkans laag (Boekhoorn, 2020), maar wordt deze pakkans ook als laag *ingeschat* door potentiële daders (Van der Wagen et al., 2019; National Crime Agency, 2017). In de literatuur wordt beschreven dat de gepercipieerde pakkans verhoogd kan worden door enerzijds het verbeteren van de opsporingscapaciteiten (Van der Wagen et al., 2019) en anderzijds meer te communiceren over de capaciteiten van de politie en cyberacties die uitgevoerd worden (Goldman & McCoy, 2016), zoals bijvoorbeeld gebeurd is bij de in hoofdstuk 7 besproken verstoring en takedown van Hansa Market (Van Wegberg & Verburgh, 2018). Door bepaalde zaken breed uit te meten in de media kan daar dus een zekere signaalfunctie van uitgaan, een strategie die overigens ook weleens bij witteboordencriminaliteit wordt toegepast (zie Huisman & Lesmeister, 2018).

Ten tweede blijft, naast een zekere reactie, ook een snelle reactie regelmatig uit. Het opsporingsonderzoek neemt bij cybercriminaliteit veel tijd in beslag en het duurt vaak lang (soms jaren) voordat de politie een verdachte in beeld heeft en/of er een strafrechtelijke sanctie of interventie volgt (Boekhoorn, 2020). Dit komt mede door het gebruik van anonimiseringstools, door verdachten die ontkennen of doordat technische vragen aan het NFI worden gesteld door (de verdediging van) verdachten, wat leidt tot vertragingen in het proces en uiteindelijk kan leiden tot lagere straffen of zelfs seponering van de zaak of vrijspraak (Van der Wagen et al., 2019).[1] Als een verdachte zich in het buitenland bevindt, is het daarnaast niet in alle gevallen mogelijk om tot een succesvolle vervolging en berechting te komen (zie hoofdstuk 7).

Ten derde bestaat nog discussie over wat een passende reactie is op cybercriminaliteit. Hoewel de impact bij cybercriminaliteit heel groot kan zijn, is het niet altijd mogelijk de omvang, het aantal slachtoffers of de schade vast te stellen (Marcum, Higgings, & Tewksbury, 2012; Van der Wagen et al., 2019). Daarbij is bij cybercriminaliteit, zoals in hoofdstuk 2 al werd besproken, vaak sprake van een groot aantal slachtoffers waarbij elk slachtoffer relatief geringe schade heeft geleden (Koops, 2010). Ook moet er een balans worden gevonden tussen zware straffen met voldoende generale en speciale afschrikking voor gevallen waarbij op grote schaal schade is aangericht, en mildere straffen voor jeugdigen en first offenders (zie bijvoorbeeld de in paragraaf 3.2.2.1 besproken CoinVault-zaak, waarbij twee daders betrokken bij afpersing met ransomware 'slechts' 240 uur taakstraf en een voorwaardelijke gevangenisstraf van twee jaar opgelegd kregen). Het is voor rechters dus een uitdaging

1 Het is ook de vraag of binnen de rechtspraak voldoende ervaring is om snel recht te spreken in de meer technisch complexe zaken.

om een goede afweging te maken tussen de aard en ernst van het delict, de persoon van de verdachte en eventuele strafverminderende omstandigheden (Smith, Grabosky, & Urbas, 2004). Een duidelijk generaal afschrikkend effect lijkt bovendien enigszins te ontbreken, niet altijd zozeer door de strafdreiging, dat wil zeggen de maximaal op te leggen straf, maar doordat de opgelegde straf regelmatig lager uitvalt dan de geëiste straf (Van der Wagen et al., 2019). In de volgende paragraaf worden specifieke interventies besproken die de rationele keuze kunnen beïnvloeden en zodoende potentieel effectief kunnen zijn in het afschrikken van cyberdaders.

8.3.2 Reactieve interventies die aansluiten bij de rationele-keuzebenadering

Gevangenisstraf

In de literatuur is weinig bekend over de toepassing van gevangenisstraffen bij cyberdaders. Daders van cybercriminaliteit krijgen volgens de internationale literatuur minder vaak dan daders van traditionele criminaliteit een gevangenisstraf opgelegd (Marcum et al., 2012). De gevangenisstraffen zijn daarnaast korter in geval van cybercriminaliteit in enge zin dan bij cybercriminaliteit in ruime zin, zoals kinderpornografie (Smith et al., 2004). Ook uit recent Nederlands onderzoek naar strafafdoeningen bij jeugdige cyberdaders in Nederland is gebleken dat de gevangenisstraf relatief weinig wordt opgelegd. In de 340 zaken werd deze 45 keer opgelegd, waarbij in 15 zaken sprake was van een volledig voorwaardelijke gevangenisstraf. De lengte van de gevangenisstraf varieerde van veertien dagen tot vijf jaar (Wieland, 2020). In een ander Nederlands onderzoek is door verschillende experts aangeduid dat een gevangenisstraf in Nederland niet snel wordt opgelegd bij *first offenders*. Bij delicten op grote schaal met verschillende slachtoffers wordt met grotere regelmaat een gevangenisstraf opgelegd. Het gaat dan bijvoorbeeld om phishers of daders die zich bezighouden met drugshandel op het dark web (Van der Wagen et al., 2019).

In Amerikaans onderzoek van Smith et al. (2004) is naar voren gekomen dat er in verschillende cyberzaken mogelijk onvoldoende specifiek afschrikkende werking uitging van de gevangenisstraf, aangezien deze daders het delictgedrag hebben voortgezet na het uitzitten van de straf. In Nederlands onderzoek is naar voren gekomen dat op jeugdige first offenders een aanhouding of voorarrest veel indruk kan maken en dat daar mogelijk al een voldoende afschrikwekkend effect van uitgaat (Van der Wagen et al., 2019; Wieland, 2020). Tegelijkertijd wordt verwacht dat reguliere straffen zoals de gevangenisstraf onvoldoende aansluiten bij criminogene behoeften en de responsivi-

teit van jeugdige cyberdaders, en dat alternatieve interventies zoals een leerstraf of Hack_Right nodig zijn (zie ook paragraaf 8.4.2). Ten slotte bestaat het risico dat cyberdaders nieuwe criminele connecties opdoen in de gevangenis of gerekruteerd worden door (leden van) criminele organisaties (Van der Wagen et al., 2019).

Financiële straffen

Andere interventies die afschrikkend zouden kunnen werken, betreffen de geldboete als straf en financiële maatregelen zoals de schadevergoeding en het verbeurdverklaren van goederen. In zaken betreffende ransomware, banking malware en het witwassen met bitcoins wordt de opbrengst doorgaans verbeurd verklaard. Er is geen (evaluatie)onderzoek gevonden naar de effectiviteit van financiële straffen voor cyberdaders. In de Verenigde Staten worden schadevergoedingsmaatregelen regelmatig opgelegd bij financieel georiënteerde cybercriminaliteit. Financieel georiënteerde straffen of maatregelen kunnen het signaal afgeven dat misdaad niet loont en bovendien kunnen ze meer bewustzijn creëren van de financiële consequenties van cyberdelicten. Vooral de inbeslagname van apparatuur wordt door cyberdaders als een zware straf ervaren, niet alleen vanwege de materiële waarde van de apparatuur (bijvoorbeeld een dure laptop), maar ook om de gegevens die op het apparaat staan. Daarbij kan het gaan om grote databases met gegevens of om programma's die ze hebben geschreven (zie hierover ook Van der Wagen et al., 2019; Viersma, 2019).

Complicerende factoren bij het opleggen van financiële straffen of maatregelen zijn het vaststellen van de exacte omvang van de schade en – zoals in het algemeen geldt – de vraag of daders de schadebedragen kunnen terugbetalen (Smith et al., 2004). In Nederland spelen soortgelijke overwegingen een rol bij strafoplegging en is bij jeugdige cyberdaders tussen 2014 en 2019 in slechts 3% van de zaken een boete opgelegd (Wieland, 2020). Daders zijn niet altijd in staat om het boete- of schadebedrag te betalen, wat ertoe kan leiden dat zij met een financiële last opgescheept zitten. Dit kan op zijn beurt belemmerend werken voor het proces van desistance, omdat het criminele verleden hen dan als het ware blijft achtervolgen en dit hen hindert om een pro-sociaal bestaan op te bouwen. Daarnaast is het verhalen van schade mede afhankelijk van een schadevergoedingsverzoek door het slachtoffer. Slachtoffers van cybercriminaliteit vorderen niet altijd een schadevergoeding, onder andere omdat niet alle slachtoffers weten dat ze schade hebben geleden door een delict of omdat ze, bijvoorbeeld als bedrijf, geen negatieve publiciteit willen (Van der Wagen et al., 2019; zie ook hoofdstuk 5).

8.3.3 Preventieve interventies die aansluiten bij de rationele-keuzebenadering

Waarschuwingsgesprek

Naast voornoemde reactieve interventies zijn er ook preventieve interventies gericht op speciale afschrikking. Het eerste voorbeeld betreft een waarschuwingsgesprek (ook wel *knock and talk*-gesprek genoemd) waarbij de politie in gesprek gaat met (potentiële) verdachten over de strafbaarheid van hun gedrag. Dergelijke gesprekken vinden steeds vaker plaats bij cybercriminaliteit in onder andere Nederland (Vermaas, 2018) en het Verenigd Koninkrijk (National Crime Agency, 2017). In Nederland is dit bijvoorbeeld gedaan bij de in hoofdstuk 3 besproken Webstresser-zaak, waarbij een website waar ddos-aanvallen besteld konden worden, uit de lucht is gehaald. Diverse 'afnemers' van ddos-aanvallen kregen een bezoek van de politie. Het doel van een waarschuwingsgesprek is afschrikken door het signaal af te geven dat de politie toezicht houdt en dat daders minder anoniem zijn dan ze denken. In het geval van jongeren wordt ook in gesprek gegaan met de ouders, die naar aanleiding van een dergelijk gesprek bijvoorbeeld meer toezicht op hun kind kunnen houden.

Uit hoofdstuk 6 bleek al dat, overeenkomstig de gelegenheidstheorieën, de mate waarin potentiële daders denken dat formeel en informeel toezicht mogelijk is, van invloed is op de kans dat ze cyberdelicten plegen (Berenblum et al., 2019). Verder wordt door middel van een waarschuwingsgesprek ook bewustwording gecreëerd ten aanzien van de risico's en gevolgen van online (strafbaar) gedrag. Dit kan leiden tot een andere kosten-batenafweging en kan mogelijke excuses wegnemen (Van der Wagen et al., 2019), waarmee deze interventie zowel aansluit bij de rationele-keuzetheorie als bij situationele criminaliteitspreventie. Een ander positief aspect is dat deze gesprekken het mogelijk maken om in een vroeg stadium in te grijpen zonder dat potentiële daders in een strafrechtelijk traject terechtkomen (zodat consequenties die nadelig zijn voor het desistance-proces, zoals een strafblad, uitblijven). Daarnaast kunnen dergelijke gesprekken eventueel gepaard gaan met inbeslagname van apparatuur of software, wat de kosten ofwel de moeite voor het plegen van cybercriminaliteit kan verhogen.

Een mogelijk (negatief) neveneffect is dat het gesprek onvoldoende afschrikt en potentiële daders aanspoort extra maatregelen te nemen om hun identiteit of activiteiten te verhullen. Daarnaast kan een waarschuwingsgesprek als een beloning worden beschouwd, bijvoorbeeld doordat een dergelijk gesprek statusverhogend werkt of juist aan de behoefte aan uitdaging of spanning (*sneaky*

thrill) tegemoetkomt (Van der Wagen et al., 2019; Brewer et al., 2019; zie ook hoofdstuk 4). Meer empirisch onderzoek is nodig om de effectiviteit van dit soort interventies voor verschillende typen daders te kunnen bepalen.

Online policing

Naast waarschuwingsgesprekken door de politie in de offline wereld kan ook online policing potentieel effectief zijn in het tegengaan van cybercriminaliteit. Volgens Aiken et al. (2016) is de online aanwezigheid van de politie van groot belang voor niet alleen opsporingswerk, maar ook bewustwording, preventie en cybersecurity. Politieagenten kunnen bijvoorbeeld online aanwezig zijn op fora en in games, mensen aanspreken op hun gedrag en hen informeren over de mogelijkheden om ICT-vaardigheden op een legale manier in te zetten (Aiken et al., 2016).

Een andere manier van online policing betreft het plaatsen van digitale waarschuwingsberichten op websites, ook wel *surveillance banners* of *warning banners* genoemd. Door middel van dergelijke waarschuwingen kunnen individuen worden geïnformeerd over de aanwezigheid van surveillance op een computersysteem (Wilson et al., 2015), maar ook over het feit dat de handeling die ze op het punt staan te begaan strafbaar is en welke straffen erop staan (Maimon et al., 2014). Aansluitend op de theorie van situationele criminaliteitspreventie kan worden verwacht dat waarschuwingsberichten effectief zijn omdat deze de risico's vergroten, door de anonimiteit van de dader te verminderen en deze te informeren over de strafbaarheid van het gedrag, en tevens bewustzijn creëren en excuses wegnemen. Aansluitend op de rationele-keuzetheorie kan daarentegen ook worden verwacht dat een dergelijke interventie alleen werkt voor bepaalde daders, zoals jeugdigen, of dat de banner niet serieus wordt genomen.

Er zijn vier Amerikaanse experimentele studies verricht naar de effectiviteit van banners, met wisselende resultaten. Het gebruik van digitale waarschuwingsberichten leidt niet tot het onmiddellijk afbreken van de handeling of een vermindering in het aantal gevallen van computervredebreuk, maar vermindert de duur van het binnendringen wel significant (Maimon et al., 2014). Ook andere onderzoekers vonden slechts een gedeeltelijk effect van waarschuwingsberichten (Testa et al., 2017; Wilson et al., 2015). Het variëren met verschillende typen berichten met bijvoorbeeld een altruïstische boodschap gericht op morele overtuiging of dreiging met een officiële sanctie, leverde bovendien geen significante uitkomsten op (Howell et al., 2017). Er is dus slechts beperkt steun gevonden voor het afschrikwekkende effect van waar-

schuwingsberichten. Wederom kan de beperkte afschrikkende werking van deze berichten ook het gevolg zijn van het feit dat het risico om gepakt te worden juist een vorm van spanning (sneaky thrill) biedt voor cyberdaders en cybercriminaliteit dus juist stimuleert (Steinmetz, 2017; Van der Wagen, 2018a; 2018b). In de Nederlandse praktijk blijken dezelfde wisselende verwachtingen over het gebruik van waarschuwingsberichten aanwezig (Van der Wagen et al., 2019).

Weer een andere vorm van online policing betreft de *verstoring* van criminele activiteiten, zoals ook kort aan bod is gekomen in hoofdstuk 7. Om de criminele activiteiten te verstoren worden barrières opgeworpen in verschillende fases van de uitvoering van de cyberdelicten. Dit gebeurt vooral in de context van financieel-georiënteerde cybercriminaliteit. Verstoring kan bijvoorbeeld plaatsvinden door de reputatie van kopers op illegale markten negatief te beïnvloeden door het achterlaten van negatieve feedback vanaf een groot aantal accounts ('Sybil-aanval'), door wantrouwen te creëren of door een server of markt offline te halen (Hutchings & Holt, 2017), zoals de politie heeft gedaan bij darknet markets als Silk Road of Hansa Market (Soska & Christin, 2015; Van Wegberg & Verburgh, 2018). Verstoring kan de drempel of de kosten voor het plegen van cybercriminaliteit verhogen en bovendien leiden tot een betere online zichtbaarheid van de politie, waarmee de perceptie van het risico (om te worden opgepakt) wordt vergroot (Van der Wagen et al., 2019; Goldman & McCoy, 2016). Hutchings en Holt (2017) wijzen er echter op dat verstoring ook kan leiden tot een waterbed-effect, waarbij daders zich bijvoorbeeld verplaatsen naar andere (beter afschermde) fora of markten, zoals het geval leek te zijn na het offline halen van Silk Road (Soska & Christin, 2015). Tegelijkertijd vereist dit meer inspanning van daders en wordt zodoende het aantal daders waarbij verplaatsing plaatsvindt beperkt (Hutchings & Holt, 2017). Deze inspanning is nog groter wanneer verkopers onder een nieuwe naam moeten beginnen en opnieuw een klantenbestand en reputatie moeten opbouwen, zoals het geval was na het offline halen van Hansa Market (Van Wegberg & Verburgh, 2018).

Voorlichting op scholen

Tot slot kan voorlichting op scholen aan jeugdigen over de gevolgen van het plegen van cybercriminaliteit ingrijpen op de rationele keuze (zie ook hoofdstuk 4 over de schoolcontext). Verschillende onderzoeken wijzen op het belang van voorlichting. Zo stellen meerdere auteurs dat scholen lessen moeten aanbieden over correct computer- en internetgebruik, de regels van cyberspace, welk gedrag strafbaar is en de consequenties van delinquent gedrag op

het internet (Aiken et al., 2016; Bae, 2017; Van der Wagen et al., 2019). De bewustwording over de strafbaarheid van gedrag en de gevolgen ervan kan tot generale afschrikking onder jeugdigen leiden en mogelijke excuses wegnemen. Mogelijke neveneffecten kunnen zijn dat de voorlichting juist nieuwsgierigheid opwekt en jeugdigen op ideeën brengt. Zodoende zal een dergelijke voorlichting meer potentie hebben bij daders met drijfveren als interesse en nieuwsgierigheid en minder bij daders die op zoek zijn naar spanning of uitdaging (Van der Wagen et al., 2019). Om voldoende generaal afschrikwekkende werking te creëren is het daarom van belang dat in combinatie met voorlichting crimineel gedrag voldoende zeker, snel en streng wordt bestraft.

8.4 De What Works-benadering

8.4.1 What Works en aangrijpingspunten voor behandeling

Uit de What Works-literatuur wordt duidelijk dat 'kale straffen' niet werken om recidive terug te dringen (Cullen, Johnson, & Nagin, 2011). Daarom richt deze benadering zich specifiek op interventies, die meestal in een strafrechtelijk kader worden opgelegd als voorwaarde bij een schorsing van voorlopige hechtenis, voorwaardelijke veroordeling of voorwaardelijke invrijheidstelling. Om te bepalen wat effectieve interventies zijn, gaat de What Works-benadering uit van een drietal beginselen: het risicobeginsel, het behoeftenbeginsel en het responsiviteitsbeginsel. Het risicobeginsel houdt in dat de intensiteit van de straf of interventie moet aansluiten bij het risico op en de ernst van de recidive van de dader (Lowenkamp et al., 2006). Daarbij geldt dat hoe hoger het risico is om te recidiveren, hoe intensiever de interventie moet zijn.

Het behoeftebeginsel houdt in dat de interventie zich specifiek moet richten op omstandigheden of gedrag dat potentieel veranderbaar is en direct gerelateerd aan het delictgedrag (Bonta & Andrews, 2007). In eerste instantie richtte de benadering zich vooral op *risicofactoren* (ook wel 'criminogene behoeften' genoemd) die moesten worden verminderd. Daarbij gaat het specifiek om *dynamische* risicofactoren zoals een pro-criminele attitude (die bijvoorbeeld het gevolg is van negatieve invloed van deviante peers), een lage zelfcontrole en gebrek aan ouderlijk toezicht. Dit zijn namelijk factoren die te veranderen zijn door middel van interventies. *Statische* factoren, zoals leeftijd en geslacht, zijn niet veranderbaar en interventies kunnen zich hier dus niet op

richten. Later ontstond steeds meer aandacht voor het inzetten en versterken van *beschermende* factoren in het individu of de omgeving van het individu (zoals een positief opvoedklimaat). Deze factoren kunnen in interventies actief worden ingezet om de effecten van de criminogene factoren of de criminogene factoren zelf te verminderen. Het hebben van werk wordt bijvoorbeeld vaak als een beschermende factor beschouwd die delictgedrag kan voorkomen (o.a. Verbruggen, Blokland, & Van der Geest, 2011). Interventies zouden in dit geval gericht kunnen zijn op hulp bij toetreding tot de arbeidsmarkt.

Het responsiviteitsbeginsel veronderstelt dat de interventie rekening moet houden met de vaardigheden, mogelijkheden en leerstijl van de dader. Bij de responsiviteit spelen cognitieve en emotionele aspecten een rol en is motivatie voor gedragsverandering een belangrijke factor (Andrews et al., 1990). In de What Works-benadering wordt een onderscheid gemaakt tussen *algemene* responsiviteit en *specifieke* responsiviteit. Daders zijn als het om gedragsverandering gaat in het algemeen responsief voor methoden die gebruikmaken van cognitieve gedragstherapie en sociaal leren (Andrews et al., 2006). Daarnaast wordt rekening gehouden met de specifieke responsiviteit. Daders verschillen in leerstijlen en capaciteiten en kunnen verschillende motivaties hebben voor het delictgedrag en dat heeft implicaties voor de noodzakelijke invulling van de interventies (McMurran & Ward, 2010).

Uit het bovenstaande volgt dat het in kaart brengen van de criminogene en beschermende factoren en van de responsiviteit een belangrijke voorwaarde is om tot de keuze voor een geschikte interventie te komen. Daartoe zijn diverse diagnose-instrumenten ontwikkeld, zoals de Recidive Inschattingsschalen (RISc).[2] Bij jeugdigen wordt via het Landelijk Instrumentarium Jeugd (LIJ) op tien leefdomeinen een dynamisch profiel opgesteld van criminogene en protectieve factoren.[3] Deze instrumenten zijn echter wel ontwikkeld voor traditionele daders en momenteel niet gevalideerd voor cyberdaders. Bovendien worden geen risicofactoren meegenomen die samenhangen met de online context waarin deze daders opereren (Van der Wagen et al., 2019).

2 Zie www.nji.nl/nl/Databank/Databank-Instrumenten/Zoek-een-instrument/Recidive-Inschattings-Schalen-(RISc) of www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc.

3 Zie https://wegwijzerjeugdenveiligheid.nl/fileadmin/user_upload/Bestanden/Documenten/Factsheet-LIJ.pdf.

In de volgende paragraaf bespreken we welke op de What Works-principes gebaseerde interventies in de literatuur worden beschreven die bruikbaar of speciaal ontwikkeld zijn voor cyberdaders.

8.4.2 Interventies die aansluiten bij de What Works-benadering

Versterken van de cognitieve en sociale vaardigheden

Het is nog maar beperkt duidelijk in welke mate antisociale persoonlijkheidskenmerken die bij traditionele criminaliteit een belangrijke rol spelen, zoals impulsiviteit, hang naar sensatie, gebrek aan inlevingsvermogen, gebrek aan moreel besef, agressiviteit en rusteloosheid, ook een rol spelen bij cybercriminaliteit. Bestaand onderzoek is daarover niet eenduidig (zie hoofdstuk 4). In recent onderzoek (Van der Wagen et al., 2019) geven experts echter wel aan dat er een groep cyberdaders is die baat zal hebben bij bestaande interventies gericht op het versterken van de cognitieve en (offline) sociale vaardigheden (zoals de CoVa-training). De interventies behoeven dan wel aanpassing zodat ze aansluiten bij de context waarin de cyberdelicten plaatsvinden. Aspecten als de anonimiteit van dader en slachtoffer in de online context en een gebrekkig zicht op gevolgen van het gedrag zijn belangrijke risicofactoren bij cyberdelinquentie (zie hoofdstuk 4). Daarnaast kan er bij daders als gevolg van de aard van de online activiteiten sprake zijn van een verstoord dag-nachtritme (Van der Wagen et al., 2019; Wieland, 2020), wat het aangaan van sociale relaties offline kan bemoeilijken. Ook hierop zouden bestaande cognitieve en gedragsinterventies kunnen inspelen, zoals de Tools4U-interventie die in de nu volgende paragraaf aan bod komt.

Ombuigen van pro-criminele attitudes en vergroten bewustzijn strafbaarheid en schade

Een pro-criminele attitude is een belangrijke criminogene factor waarop interventies zich moeten richten volgens de What Works-benadering (Bonta & Andrews, 2007). Daarbij moet worden gekeken naar de oorzaak van de pro-criminele houding. Zoals reeds naar voren kwam in hoofdstuk 4, is een deel van de (voornamelijk jonge) cyberdaders zich nauwelijks bewust van de strafbaarheid van hun gedrag. Interventies bij deze daders moeten zich dus richten op bewustwording, waarvoor kennis (via voorlichting of training) en het actief uitdagen van de daders om de eigen opvattingen te vergelijken met deze inzichten belangrijk zijn (Van der Wagen et al., 2019). Een ander deel van de daders weet wel dat het gedrag strafbaar is, maar realiseert zich niet welke schade het gedrag aanricht bij het slachtoffer, wat de mogelijke gevolgen zijn voor de eigen toekomst of bagatelliseert de schade (zie o.a. Zebel et al., 2013).

Samengenomen zouden dus bewustwording van strafbaarheid en aangerichte schade moeten helpen om het neutraliseren van het eigen gedrag in te perken.

Een bestaande interventie in Nederland die zich hierop richt, is de interventie Tools4U,[4] gericht op jongeren tussen de 12 tot 23 jaar die sociale en cognitieve tekorten hebben. Via bijeenkomsten wordt getracht de jongeren cognitieve en sociale vaardigheden aan te leren. Daarbij is veel aandacht voor gemaakte keuzes en het gebruik van beter geïnformeerde kosten-batenafwegingen die aan de gemaakte keuzes ten grondslag liggen. Deze interventie zou mogelijk effectief kunnen zijn voor cyberdaders mits deze aangepast wordt aan de online context, bijvoorbeeld door rekening te houden met online disinhibitie en het wegvallen van grenzen in tijd en ruimte (Van der Wagen et al., 2019). Deze interventie is nog maar heel beperkt opgelegd in cyberzaken (Wieland, 2020).

Waar het gaat om de gebrekkige perceptie ten aanzien van de schade en het slachtoffer, zou een interventie geschikt kunnen zijn die gericht is op het zich inleven in het slachtoffer, ook wel 'mentaliseren' genoemd (Van der Wagen et al., 2019). Datzelfde geldt voor mediation met het slachtoffer, bijvoorbeeld in het kader van een Halt-straf[5] in de vorm van een excuusbrief of een herstelgesprek. Daardoor wordt de anonimiteit opgeheven en daarnaast kan mediation bijdragen aan het besef van de schade die is aangericht. Dit zou het inlevingsvermogen en moreel besef van de dader versterken en dus ook een rol kunnen spelen bij het ombuigen van een pro-criminele attitude. Uiteraard is het bij mediation belangrijk om het belang van het slachtoffer goed in het oog te houden.

Tot slot kan *gamification* worden ingezet als interventie(strategie) om pro-criminele attitudes om te buigen of te voorkomen (Aiken et al., 2016; Van der Wagen et al., 2019; *te verschijnen*). Gamification verwijst in deze context naar het aanleren van gepast (online) gedrag door middel van 'spelmechanismen', oftewel gaming (Power & Kirwan, 2014, p. 234). Dit soort spellen zouden (potentiële) daders op een speelse en competitieve manier kunnen leren over goede en slechte manieren van hacken. Bovendien kunnen zij met behulp

4 Zie www.nji.nl.

5 Een Haltstraf kan worden opgelegd aan jongeren tussen de 12 tot 18 jaar indien er sprake is van lichte vergrijpen. Ze krijgen dan geen aantekening in de justitiële documentatie. Van de 340 strafafdoeningen bleek dat 86 (25% van het totaal) werden afgedaan door middel van een Halt-afdoening (Wieland, 2020).

van deze games waardevolle cyberveiligheid-vaardigheden leren (zie bijvoorbeeld Švábenský et al., 2018), die ze op een pro-sociale manier leren toepassen (Van der Wagen et al., *te verschijnen*). Een recent voorbeeld van een initiatief dat onder gamification geschaard zou kunnen worden, is het door de politie gelanceerde Gamechangers.[6] Dit betreft een *challenge* waarbij jongeren uitgedaagd en gestimuleerd worden om hacking op een pro-sociale manier in te zetten. De campagne is tijdens de Coronacrisis gestart, mede vanuit de gedachte dat jongeren tijdens deze crisis veel tijd thuis spenderen, zich vervelen en mogelijk dus veel meer online zijn en blootgesteld kunnen worden aan pro-criminele attitudes. Ook wijkagenten doen mee aan het spel om zo contact te kunnen leggen met jongeren en hen er eventueel van te kunnen weerhouden om criminaliteit te plegen. Zoals bij veel van de interventies ontbreekt vooralsnog empirisch onderzoek naar de effectiviteit ervan voor cyberdaders.

Behandelen van persoonlijke problematiek

Net als bij daders van traditionele delicten kunnen bij daders van cybercriminaliteit ook specifieke problemen spelen die bijdragen aan het risico op delictgedrag, zoals psychische, relationele of financiële problemen of problemen thuis of op school (Van der Wagen et al., 2019; Wieland, 2020; zie ook hoofdstuk 4). Deze problemen hoeven niet direct aan de totstandkoming van cybercriminaliteit gerelateerd te zijn, maar het verhelpen ervan kan wel bijdragen aan het voorkomen van recidive. Hierbij valt in het bijzonder te denken aan het leren omgaan met kenmerken van een autismespectrumstoornis, sociale onhandigheid en eenzaamheid, het begeleiden bij het vinden van een geschikte baan of opleiding en het vergroten van de ouderlijke rol inzake het toezicht houden op online gedrag. Als dergelijke problematiek aanwezig is, dan zouden bestaande interventies en behandelingen, die nu vaak als bijzondere voorwaarde worden opgelegd, kunnen volstaan (Van der Wagen et al., 2019).

Hoewel nog maar beperkt duidelijk is of het arsenaal aan mogelijkheden voldoende is voor de problematiek van de verschillende typen cyberdaders, is uit onderzoek wel gebleken dat experts in Nederland zich positief uitlaten over de capaciteiten van de reclassering om op maat begeleiding te geven of te vinden (Van der Wagen et al., 2019). Wel wordt gesignaleerd dat door een gebrek aan de inzet van diagnose-instrumenten bij cyberdaders veel criminogene behoef-

6 De politie voert dit uit in samenwerking met Deloitte (de Hacklab challenges | Hackazone), WeFitter (de WeFitter challenge), ESL (de Gamechangers FIFA Cup) en Stichting Hack in the Class (Hack in the Class), zie 'Gamechangers: houd jongeren weg bij cybercrime', Politie.nl, 21 april 2020.

ten onopgemerkt blijven. Ook zijn er criminogene behoeften die minder voorkomen bij traditionele daders, maar die wel belangrijk lijken te zijn bij cyberdaders, zoals eenzaamheid bij oudere daders (Van der Wagen et al., 2019). Hier lijken dus niet zozeer nieuwe interventies nodig te zijn, maar wel adequatere diagnostisering van criminogene behoeften, zoals eerder in dit hoofdstuk reeds werd aangestipt.

Aanpassen van criminogene gelegenheidsfactoren

Een laatste categorie interventies gericht op criminogene factoren die we willen bespreken, betreft interventies die restricties of controle opleggen op computer- of internetgebruik. Dit kan in de eerste plaats in de vorm van een verbod op het gebruik van computers of internet tijdens het voorwaardelijk deel van een straf, of als voorwaarde bij een schorsing van de voorlopige hechtenis (Smith et al., 2004; Van der Wagen et al., 2019). Een dergelijk verbod kan een aanzet geven tot verandering in het gebruik van computers, vooral als het samengaat met behandeling of begeleiding door een hulpverlener of toezichthouder. Aandachtspunt is dat de kennis en technische vaardigheden op het gebied van computers en internet bij veel hulpverleners en toezichthouders nog zeer beperkt zijn, wat problemen oplevert bij de controle van de voorwaarden en begeleiding. Andere positieve aspecten van een dergelijke maatregel zijn dat het kan dienen als een 'cooling down'-periode waarin de dader ook meer offline activiteiten gaat ondernemen, nieuwe offline (intieme) relaties aangaat en zich realiseert dat er meer is dan alleen een 'leven achter het scherm' (Van der Wagen et al., *te verschijnen*).

De eerder besproken inbeslagname van apparatuur kan eveneens worden ingezet om de beschikbaarheid van instrumenten voor het delictgedrag in te perken of tijdelijk weg te nemen (Van der Wagen et al., 2019). Hoewel een dader uiteraard nieuwe apparatuur kan aanschaffen en nieuwe tools kan ontwikkelen, heeft hij hieraan veel kosten en kan de inbeslagname een momentum creëren waarin de dader tot nieuwe inzichten of nieuw gedrag komt. Die inzichten en dat gedrag kunnen tot andere keuzes en ervaringen leiden en er kan ruimte ontstaan voor nieuwe mogelijkheden. Zo kan het delinquente gedrag ook op de langere termijn mogelijk afnemen. Daarbij is een belangrijke rol voor ouders weggelegd. Zij zouden toezicht kunnen houden op het online gedrag van hun kinderen en kunnen voorkomen dat hun kind (opnieuw) afglijdt in de cybercriminaliteit. Ouderlijk toezicht op online gedrag is echter complex, mede doordat ouders niet de vaardigheden hebben om het online gedrag te controleren, ouders vaak fulltime werken, jongeren eventueel delinquent gedrag goed verborgen weten te houden en jongeren

tegenwoordig nu eenmaal veel online (moeten) zijn, ook voor veel pro-sociale activiteiten (Van der Wagen et al., 2019; *te verschijnen*; Zebel et al., 2013).

Hack_Right

Hack_Right is een interventie in de vorm van een alternatief of aanvullend straftraject voor jeugdige beginnende cyberdelinquenten waarin een aantal van de hierboven genoemde categorieën van criminogene factoren aan bod komen en die bovendien specifiek rekening houdt met de cybercontext en specifieke responsiviteit van de daders (De Bruijne, 2018; Wieland, 2020). In deze interventie wordt zowel gewerkt aan de risicofactoren als aan de kansen en mogelijkheden die de jongeren hebben. De interventie wordt uitgevoerd in een samenwerking tussen de strafrechtketen, cybersecuritybedrijven en de hackergemeenschap.

De interventie bestaat uit vier modules waarvan de eerste twee, 'herstel' en 'training', zich vooral op de criminogene factoren richten (De Bruine, 2018; Wieland, 2020). De herstelmodule betreft een vorm van mediation en de module 'training' richt zich op de specifieke cognitieve en sociale vaardigheden die bij de dader onvoldoende zijn ontwikkeld. Deze module zou moeten leiden tot een beter beeld van de gevolgen van het handelen voor de toekomst en tot meer vertrouwen in de eigen mogelijkheden buiten de cybercriminaliteit. Bovendien wordt in deze module, anders dan in de meeste moderne gedragsinterventies voor daders van traditionele criminaliteit, ook veel aan kennisoverdracht gedaan, bijvoorbeeld over wat wel en niet mag volgens de Nederlandse wetgeving en waar de grenzen van ethisch hacken liggen. Dergelijke kennisoverdracht kan bijdragen aan het beter afwegen van kosten en baten en aan het verminderen van het gebruik van neutralisaties voor het gedrag (Xu et al., 2013). De derde en vierde module passen vooral in de desistance-benadering en komen in de nu volgende paragraaf aan bod.

8.5 De desistance-benadering

8.5.1 Perspectief op stoppen

Volgens de desistance-benadering is het stoppen met criminaliteit meer dan het niet langer plegen van delicten. Het dient gepaard te gaan met een positieve verandering van identiteit, waardoor iemand gecommitteerd is om zich ook op de lange termijn aan de wet te houden (McNeill et al., 2012). Daarbij kan een onderscheid worden gemaakt tussen *primaire desistance* (een periode

zonder recidive) en *secundaire desistance* (een verandering in de manier waarop de ex-delinquent tegen zichzelf aankijkt, oftewel het ondergaan van een identiteitstransformatie) (Maruna & Farrall, 2004; Maruna & Toch, 2005). Ook kan *tertiaire desistance* nog van belang zijn in het proces van desistance. Dit verwijst naar de mate waarin de maatschappij de dader weer opneemt, waardoor de dader een sterkere *sense of belonging* krijgt (McNeill, 2016; Nugent & Schinkel, 2016).

Desistance heeft vooral het karakter van een natuurlijk, dynamisch proces dat, net als andere gedragsveranderingen, verloopt via ambivalentie en aarzeling, vallen en opstaan, en hoop en wanhoop (Laub & Sampson, 2003; McNeill et al., 2012). Om effectief te zijn moeten interventies bij dat proces aansluiten, in plaats van te veel nadruk leggen op risicofactoren en geïsoleerde behandelprotocollen, zoals de kritiek op de What Works-benadering luidt.

De desistance-benadering focust dus niet zozeer op het uiterlijke gedrag van het wel of niet plegen van delicten, maar op gebeurtenissen in de levensloop van delinquenten, waarmee veranderingen in identiteit, sociale rollen en toekomstperspectief gepaard gaan. Interventies dienen aan belangrijke levensloopgebeurtenissen en levensdoelen bij te dragen en hiervoor kansen te creëren; zodoende wordt van *strength-based* interventies gesproken (Hampson, 2018; McNeill et al., 2012). Het (uiterlijk) stoppen met delictgedrag dient dus samen te gaan met het (innerlijk) ontwikkelen van een pro-sociale identiteit, alsook met externe mogelijkheden en kansen om aan deze veranderde identiteit uitdrukking te kunnen geven en een positieve toekomst te kunnen realiseren (ook wel uitgedrukt als 'hoop voor verandering'). McNeill et al. (2012) stellen in dit kader dat het belangrijk is dat daders daadwerkelijk de mogelijkheid krijgen *to desist into something* – waarmee het belang van niet-crimineel sociaal kapitaal wordt benadrukt.

De empirische onderbouwing voor de effectiviteit van op deze benadering gebaseerde interventies is nog beperkt, aangezien de benadering nog relatief jong is en de uitwerking ervan in specifieke interventies nog niet wijdverspreid is. Een andere beperking bij het doen van effectonderzoek hiernaar is dat door de aard van strength-based interventies, die multidimensionaler en langduriger zijn en niet direct gericht op recidivebeperking, het isoleren van de effecten van de specifieke aanpak complex is.

Hoewel evenmin evaluatieonderzoek naar interventies voor cyberdaders gebaseerd op de desistance-benadering voorhanden is, kan wel voorzichtig uit de

literatuur worden opgemaakt dat hiervan veel te verwachten valt. De kenmerken en motieven van cyberdaders (zie hoofdstuk 4) kunnen namelijk verschillende *hooks for change* bieden voor desistance (Giordano, Cernkovich, & Rudolph, 2002). Wat betreft achtergrondkenmerken wordt over het algemeen aangenomen dat cyberdaders over een sterker sociaal kapitaal beschikken dan traditionele daders, doordat zij bijvoorbeeld uit gezinnen met een hogere sociaaleconomische status komen en beschikken over zekere, met name technische talenten, een hoger opleidingsniveau en/of een loopbaan in de ICT-wereld.

Wat betreft drijfveren lijkt voor een relatief groot deel van de cyberdaders te gelden dat sprake is van motieven of behoeften die in beginsel niet-criminogeen zijn, waaronder de behoefte aan uitdaging en spanning (thrill), status en peer respect in combinatie met een interesse in IT, een nieuwsgierige, leergierige houding en behoefte aan ontwikkeling van skills (self-challenge). Hoewel sommige van deze drijfveren evenzeer belangrijk zijn bij traditionele criminaliteit, ligt bij cyberdaders doorgaans een sterkere nadruk op het 'kunnen', waarvoor (technische) vaardigheden en discipline nodig zijn (Steinmetz, 2015a; Van der Wagen et al., 2019). Deze kenmerken en drijfveren bieden expliciete aanknopingspunten voor het desistance-proces waar het gaat om positieve bekrachtiging (pro-sociale identiteit) en het bieden van kansen om sociale rollen en toekomstplannen (pro-sociaal kapitaal) te versterken. Prosociaal kapitaal is echter ook belangrijk in het geval de dader een expliciet financieel motief heeft; er zal namelijk wat tegenover dienen te staan wil deze zijn (of haar) criminele carrière vaarwel (kunnen) zeggen. Hierin tekenen zich duidelijke hooks for change af, die op basis van strength-based interventies versterkt zouden kunnen worden.

8.5.2 Interventies die aansluiten bij de desistance-benadering

Hierna worden vier (elementen van) interventies besproken die aansluiten bij de desistance-benadering en volgens de literatuur succesvol zouden kunnen zijn bij cyberdaders. Drie elementen kunnen direct bijdragen aan het creëren van hooks for change in de levensloop van cyberdaders, zoals het ethisch leren hacken, het ontwikkelen van talent en het bieden van een toekomstsperspectief in de vorm van baan of opleiding. Een vierde element, namelijk de inzet van rolmodellen, kan gedurende dit proces ondersteuning bieden.

Ethisch hacken

Ethisch hacken houdt in dat volgens bepaalde richtlijnen (zoals geformuleerd in het Coordinated Vulnerability Disclosure (CVD)-beleid) en onder bepaalde voorwaarden hacken is toegestaan om kwetsbaarheden in systemen aan het licht te brengen (NCSC, 2013; 2018; Weulen Kranenbarg, Holt, & Van der Ham, 2018; zie ook hoofdstuk 3). Hiervoor dient het CVD-beleid uiteraard wel voldoende bekend én duidelijk te zijn voor (potentiële) daders als het gaat om wat wel en niet strafbaar is, zodat daarover zo weinig mogelijk onzekerheid bestaat. In de praktijk blijkt dat dit echter lang niet altijd het geval is (Harms, 2017). Hackers verkeren soms in de veronderstelling dat onveilige systemen legaal gehackt mogen worden, zolang het lek maar achteraf wordt gemeld (Van der Wagen et al., 2019). In dat geval loopt de hacker het risico om door het Openbaar Ministerie te worden vervolgd en moet worden aangetoond dat er sprake was van een algemeen belang (zie ook hoofdstuk 3).

Hoewel empirisch onderzoek naar het CVD-beleid nog nauwelijks beschikbaar is, worden in de literatuur wel een aantal aspecten beschreven die potentieel effectief kunnen zijn, met name ten aanzien van de Amerikaanse variant hiervan, namelijk *Duty to Report* of *look-and-see* hacken. In de eerste plaats kan ethisch hacken een bijdrage leveren aan het vergroten van internetveiligheid doordat melding wordt gemaakt van kwetsbaarheden (Chatfield & Reddick, 2018). Daarnaast stimuleert ethisch hacken de ontwikkeling van creativiteit en technische vaardigheden (Wible, 2003). Ook worden met behulp van ethisch hacken online normen en grenzen (zowel juridische als ethische) duidelijk, waardoor de behoefte aan uitdaging op een pro-sociale wijze (als white hat hacker) kan worden ingezet (Siponen, Vance, & Willison, 2012; Van der Wagen et al., 2019; Spronk & Weulen Kranenbarg, 2020). Tot slot gelden als verwachte effecten dat samenwerking en wederzijds vertrouwen tussen hackers en politie en justitie toeneemt, evenals de zelfregulatie onder hackers (Siponen et al., 2012). Onderzoek onder jongeren wees er in dit verband op dat enerzijds morele overtuigingen en schaamte sterke voorspellers zijn voor de neiging tot het plegen van cybercriminaliteit (dit betrof overigens specifiek het illegaal downloaden) (Siponen et al., 2012) en dat anderzijds geldt dat hoe jonger de leeftijd is waarop hackersethiek wordt aangeleerd, des te beter hackers tijdens hun tienerjaren bestand zullen zijn tegen druk van buitenaf om de grenzen over te gaan (Kao et al., 2009).

Om bij te dragen aan het proces van stoppen met criminaliteit wordt wel gesteld dat op ethisch hacken een beloning dient te volgen; vandaar dat ook wel gesproken wordt over 'vulnerability reward program' (VRP) of 'bug

bounty program' (Chatfield & Reddick, 2018). Deze beloning hoeft echter niet per se uit een financiële tegenprestatie, in de vorm van *bug bounties*, te bestaan. Ook status en erkenning of bijvoorbeeld persoonlijke coaching en kennisdeling door ervaren hackers (wat kan bijdragen aan de ontwikkeling van skills) worden belangrijk geacht (Van der Wagen et al., 2019; Spronk & Weulen Kranenbarg, 2020). Zo wordt op het online platform HackerOne aan beide behoeften tegemoetgekomen, doordat er enerzijds door middel van ethisch hacken geld (bug bounties) valt te verdienen en er anderzijds ook wat te leren valt en erkenning voor prestaties wordt verkregen via een leaderboard.

Rolmodellen

Het verkrijgen van erkenning, status en persoonlijke betrokkenheid van meer ervaren hackers sluit goed aan bij de desistance-benadering, waarin het belang van rolmodellen bij het ondergaan van identiteitsverandering wordt benadrukt. Hoewel ook hiernaar weinig onderzoek is gedaan ten aanzien van cyberdaders, wordt bijvoorbeeld bij interventies door de politie in Nederland en het Verenigd Koninkrijk wel duidelijk rekening gehouden met de bijdrage die rolmodellen, coaches of mentoren kunnen leveren aan het ondersteunen van jonge hackers om op het goede pad te blijven (National Crime Agency, 2017). In het kader van de Hack_Right-interventie vindt, binnen de module 'coaching', training en coaching plaats door ervaren hackers en IT-professionals of cybersecurityspecialisten, waarmee cyberdaders in het kader van een leer-werkplek bij bedrijven kennismaken.

Ook in een minder formeel kader kan worden verwacht dat van de hackergemeenschap (bijvoorbeeld 'old guard' hackers; Rogers, 2006) in het algemeen een voorbeeldfunctie uitgaat, evenals een zeker zelfreinigend vermogen (Steinmetz, 2015a; Van der Wagen et al., 2019). Rolmodellen of coaches kunnen in het desistance-proces van belang zijn, enerzijds door cyberdaders een voorbeeld te bieden en uit te dagen in de ontplooiing van hun talent op een pro-sociale wijze, anderzijds door het geven van erkenning, waarmee de eigenwaarde en identiteit kunnen groeien. Bovendien betreffen rolmodellen belangrijke personen om zich aan vast te houden in het proces van stoppen met criminaliteit nu dit proces zich immers niet van de ene op de andere dag voltrekt en via ups en downs verloopt. Hoewel ondersteuning en coaching ook door 'reguliere' begeleiders, zoals reclasseringswerkers, zouden kunnen worden aangeboden, kan bij cyberdaders juist een extra effect worden verwacht van de inzet van 'technische' coaches naar wie zij kunnen opkijken.

Talentontwikkeling

Bij het ontwikkelen van (technisch) talent en erkenning van prestaties kunnen hackwedstrijden een belangrijke rol spelen. Hoewel deze niet als zodanig ontwikkeld zijn, kunnen zij als preventieve interventie worden aangemerkt, vanwege de bijdrage die zij kunnen leveren aan het ontwikkelen van pro-sociale attitudes en relaties evenals een pro-sociale identiteit. In de internationale literatuur wordt wel gesproken van *hack-in-contest* of *hackathon* (Wible, 2013), of, in bredere zin, van de eerder besproken variant van gamification (Aiken et al., 2016). Het gaat om wedstrijden waarbij hackers op verzoek systemen hacken, vaak door private partijen gesponsord (Oosterwijk & Fischer, 2017). Ook kan worden samengewerkt met publieke instanties, zoals bij 'Hâck The Hague' (een hackwedstrijd georganiseerd door de gemeente Den Haag en het Haagse cybersecuritybedrijf 'Cybersprint').

Een ander voorbeeld betreft de door de politie opgezette website 'crimediggers.nl', waarbij hackers uitgedaagd worden hun vaardigheden te testen om te zien of zij wellicht kunnen komen werken bij de digitale recherche. Evenzo organiseert de National Crime Agency (NCA) van het Verenigd Koninkrijk een 'Rehab For Hackers'-weekend,[7] waarbij ingezet wordt op voorlichting en preventieve adviezen, waarvoor ook de ouders of opvoeders van de jongeren uitgenodigd worden, en een lesplan voor leraren wordt ontwikkeld (Keizer, 2019; Stanton, 2019).[8] Voor cyberdaders voor wie erkenning en uitdaging belangrijke drijfveren zijn, zouden dit soort wedstrijden een alternatief kunnen bieden voor het plegen van cybercriminaliteit. Een ander voordeel van hackwedstrijden is dat zij (net als wordt verwacht bij ethisch hacken) een effectieve bijdrage kunnen leveren aan (verbeterde) relaties tussen hackers en professionals op het gebied van handhaving en cybersecurity (Oosterwijk & Fischer, 2017).

Naast hackwedstrijden zouden ook initiatieven als hackerspaces of cyberwerkplaatsen een belangrijke bijdrage kunnen leveren aan niet alleen het ontwikkelen van vaardigheden, maar ook het opbouwen van pro-sociale relaties en mogelijk aan het verwerven van een stageplek of baan in de IT- of cybersecuritywereld (pro-sociale rollen en toekomstplannen) (Van der Wagen et al., 2019). Daarnaast kan het ook een positieve dagbesteding bieden (Wieland, 2020). In Nederland kennen we de 'Cyberwerkplaats Rotterdam' en 'Hacklab Friesland',

7 Zie M. Ward, 'Rehab camp aims to put young cyber-crooks on right track', *BBC.com*, 24 juli 2017.

8 Zie ook K. Collins, 'Inside the boot camp reforming teenage hackers', *CNET.com*, 6 augustus 2018.

die worden gerund door vrijwilligers en gesponsord door maatschappelijke partners en bedrijven. Jongeren kunnen daar op vrijwillige basis terecht om les te krijgen van experts en tegelijkertijd op een ethische manier te leren hacken. Net als hackwedstrijden bieden dergelijke initiatieven de mogelijkheid dat hackers elkaar niet alleen online, maar ook fysiek ontmoeten en prosociale relaties met anderen opbouwen, wat behulpzaam kan zijn voor daders die vooral solistisch opereren of voor wie (offline) sociaal contact aangaan problematisch is en die met eenzaamheid te kampen hebben. De vraag is echter wel of cyberdaders bij wie sprake is van sociale geïsoleerdheid, met dergelijke interventies voldoende worden bereikt (Van der Wagen et al., 2019).

Tot slot kunnen ook scholen een rol spelen bij het stimuleren van talent. Enerzijds kan dit door onderwijs op maat aan te bieden dat aansluit bij de technische interesses van jongeren. Cyberdaders blijken immers over het algemeen (zie ook hoofdstuk 4) minder interesse te hebben in het reguliere curriculum en juist een specifieke interesse te hebben voor ICT, terwijl ICT-gerelateerde vakken nauwelijks worden aangeboden of van slechte kwaliteit zijn (Árpád, 2013; Chiesa et al., 2009; Xu et al., 2013). Anderzijds kunnen scholen jongeren een tweede kans bieden wanneer zij over de schreef zijn gegaan (door bijvoorbeeld het schoolsysteem te hacken) waarbij hun technisch talent juist wordt benut. Deze jongeren zouden kunnen worden ingezet om voorlichting te geven over veilig online gedrag, om een bijdrage te leveren aan lessen over een IT-gerelateerd onderwerp, of om kwetsbaarheden in het online schoolsysteem bloot te leggen op basis van het CVD-beleid (zie voor een eerste empirisch onderzoek naar gebruik van CVD onder jongeren Spronk & Weulen Kranenbarg, 2020).

Net als het aanleren van hackersethiek bieden voornoemde initiatieven ruimte voor online uitdaging, competitie en talentontwikkeling, wat wordt beloond in de vorm van erkenning, status en eigenwaarde (positieve bekrachtiging), maar ook compensatie in financiële of prestige-vorm of simpelweg een 'cv' (in de vorm van opgedane vaardigheden en prestaties) dat klaarstoomt voor de IT-wereld (Aiken et al., 2016; Van der Wagen et al., 2019). Tegelijkertijd kan ook worden verwacht dat het daders niet zal weghouden bij illegale activiteiten die door de spanning ervan (ook) dat pad worden opgetrokken. Het legale en illegale hacken hoeven elkaar namelijk niet uit te sluiten. Men verwacht echter dat een zeker deel van de cyberdaders door het aanleren van hackersethiek en alternatieven voor het inzetten van hun technische vaardigheden wordt gemotiveerd om het illegale pad te verlaten (Wible, 2003; Oosterwijk & Fischer, 2017; Van der Wagen et al., 2019).

Carrièreperspectief

Uit onderzoek onder experts die met cyberdaders werken, is naar voren gekomen dat binnen bepaalde leefgebieden, zoals opleiding en werk, problemen kunnen spelen die niet direct als criminogene factoren (dat wil zeggen factoren die verband houden met het delictgedrag) uit een risicotaxatie naar voren komen, omdat deze zich bij cyberdaders bijvoorbeeld op een andere manier manifesteren (Van der Wagen et al., 2019). Toch kunnen interventies in dergelijke gevallen, volgens onder andere reclasseringswerkers, bijdragen aan het creëren van 'succeservaringen' op deze gebieden evenals aan het versterken van een pro-sociale identiteit en pro-sociale relaties, wat nauw aansluit bij de strength-based benadering. Professionals in de strafrechtketen beschouwen het bieden van baankansen als een belangrijk element in het desistance-proces (Van der Wagen et al., 2019). Binnen de Hack_Right-interventie kunnen jonge hackers, op basis van de vierde module 'alternatief', worden verplicht om een leerwerktraject te doorlopen bij een cybersecuritybedrijf of IT-afdeling van bijvoorbeeld een bank of accountantskantoor, waardoor ze leren hoe ze hun talenten op een positieve manier kunnen inzetten.

Dergelijke initiatieven sluiten aan op de desistance-benadering vanwege het idee dat hackers over (sterke) vaardigheden, talenten, ambities en creativiteit beschikken die de samenleving juist hard nodig heeft en aan hen duidelijk moet worden gemaakt dat zij deze (ook) op een legale manier kunnen inzetten, bijvoorbeeld in het kader van een (goede) baan, waarmee ook een (goede) boterham te verdienen valt. Daarnaast kan hun dit de erkenning, status en uitdaging opleveren waarnaar zij op zoek zijn. Hiermee wordt voldaan aan een belangrijke voorwaarde in het desistance-proces, namelijk dat de kans wordt gecreëerd 'to desist into something' (McNeill et al., 2012).

Wel zou op basis van de gelegenheidstheorie ook rekening moeten worden gehouden met de gelegenheid die dergelijke banen scheppen voor het plegen van cybercriminaliteit. Longitudinaal onderzoek onder Nederlandse cyberdaders toonde namelijk aan dat van werk in het algemeen wel, maar werk in de IT-sector niet een beschermend effect uitgaat, hoewel deze effecten niet-significant waren (Weulen Kranenbarg, Ruiter et al., 2018).

Tot slot is nog van belang dat bij strafrechtelijke interventies rekening wordt gehouden met eventuele schadelijke gevolgen voor de baankansen van cyberdaders, bijvoorbeeld in de vorm van het krijgen van een strafblad. Juist bij overheidsinstellingen, zoals de politie, of grote cybersecuritybedrijven die voor overheidsinstellingen opdrachten uitvoeren, worden werknemers vaak

gescreend op een eventueel justitieel verleden, bijvoorbeeld in de vorm van een Verklaring Omtrent het Gedrag (Van 't Zand-Kurtovic, 2017). Hiermee kan binnen Hack_Right tot op zekere hoogte rekening worden gehouden, bijvoorbeeld door de interventie op te leggen als voorwaarde bij een voorwaardelijke seponering van de strafzaak.

8.6 Tot besluit

In dit hoofdstuk is stilgestaan bij de vraag wat passende en effectieve interventies voor daders van cybercriminaliteit (in enge zin) zouden kunnen zijn. Op basis van drie verschillende benaderingen van interventies zijn verschillende typen (preventieve en reactieve) interventies besproken die verwacht worden effectief te zijn in het bestrijden van cybercriminaliteit.

In bestaand onderzoek wordt ten aanzien van interventies die aansluiten bij de rationele-keuzebenadering vaak gewezen op de verwachte effectiviteit van (het versterken van) op afschrikking gerichte interventies. Het probleem is echter dat momenteel aan geen van de drie basisvoorwaarden voor afschrikking (zeker, snel en streng) in voldoende mate lijkt te worden voldaan: de pakkans is laag, het opsporings- en vervolgingsonderzoek duurt vaak lang en de straf valt relatief mild uit. Om deze reden kan mogelijk meer worden verwacht van het potentiële succes van situationele criminaliteitspreventie, waaronder het verstoren van online markten, online policing, digitale waarschuwingsberichten en voorlichting.

De What Works-benadering gaat ervan uit dat interventies effectief zijn als zij zich richten op criminogene behoeften. Op dit moment is er echter een gebrek aan adequate diagnoses van de risicofactoren van cyberdaders en de manier waarop deze in online gedrag tot uiting komen. Bestaande diagnose-instrumenten (en interventies) zouden bijvoorbeeld meer rekening moeten houden met de unieke drijfveren voor cybercriminaliteit en het feit dat daders zich vaak niet voldoende bewust zijn van de strafbaarheid en schade. Van interventies die zich richten op het aspect van bewustwording, zouden van mentaliseren (het inleven in een ander) en mediation positieve effecten kunnen worden verwacht. Dit soort interventies zorgen ervoor dat schade en slachtoffer minder afstandelijk of abstract lijken.

De desistance-benadering is vooral voorstander van een strength-based aanpak. Cyberdaders lijken, meer dan traditionele daders, over een zeker sociaal

kapitaal en sociale bindingen te beschikken, waaraan met (te) hoge straffen afbreuk kan worden gedaan. Ook zijn vaak talenten aanwezig (strengths) die duidelijk waarde hebben voor de samenleving, mits ze op een pro-sociale manier worden ingezet. Verwacht wordt dat aan deze strengths een bijdrage kan worden geleverd door interventies als hackwedstrijden en cyberwerkplaatsen, waar wordt geïnvesteerd in het aanleren van ethisch hacken en in het vergroten van technische vaardigheden evenals in het opbouwen van een carrièreperspectief. Rolmodellen kunnen in het hele desistance-proces van toegevoegde waarde zijn.

Van belang is dat waar mogelijk elementen die aansluiten bij het risicobeginsel (risks), criminogene behoeften (needs) en strengths in combinatie terugkomen in de interventies. De Hack_Right-interventie betreft een voorbeeld van een interventie waarin een risk- en een strength-based aanpak worden gecombineerd. Alleen het vergroten van de IT-vaardigheden en carrièrekansen en het bieden van een ondersteunend netwerk (rolmodellen of coaches), zonder dat gewerkt wordt aan het moreel besef en het ombuigen van een procriminele houding, kunnen immers tot meer cybercriminaliteit leiden.

Afsluitend kan worden opgemerkt dat er nog veel te winnen valt op het terrein van passende interventies voor cyberdaders. Behalve dat bestaande diagnose-instrumenten zouden moeten worden gevalideerd en aangevuld voor crimineel gedrag in een online context, zou goed in kaart moeten worden gebracht voor welke groepen of typen cyberdaders bestaande interventies mogelijk effectief zijn en voor welke deze mogelijk een averechts effect hebben. Tot slot is cruciaal dat rekening wordt gehouden met de uiteenlopende capaciteiten, leerstijlen en motivaties (responsiviteit) van cyberdaders. Vanwege de online context en het technische karakter van cybercriminaliteit in enge zin zijn er immers aanzienlijke verschillen met traditionele criminaliteit waar te nemen. Een op maat gesneden aanpak is in elk geval onontbeerlijk.

8.7 Discussievragen

1. Welke beperkingen gelden ten aanzien van de huidige status van het onderzoek naar (potentieel) effectieve interventies voor cyberdaders?
2. Welke averechtse effecten zouden, gezien de drijfveren van daders van cybercriminaliteit, kunnen optreden bij interventies die beogen in te grijpen op het rationele-keuzeproces?

3. Welke redenen zijn te bedenken voor het beperkte succes van waarschuwingsberichten, zoals uit onderzoek in de Verenigde Staten naar voren is gekomen?
4. Op welke manieren kan verstoring als interventie succesvol zijn, ook indien rekening wordt gehouden met het verplaatsingseffect?
5. Waarom lijkt, gezien de drie basisvoorwaarden van afschrikking, onvoldoende sprake te zijn van zowel generale als speciale afschrikking bij cybercriminaliteit?
6. Waarom bestaat er (nog) weinig inzicht in de risicofactoren en criminogene behoeften die bij cyberdaders een rol spelen?
7. Op welke manier zouden bestaande interventies kunnen worden aangepast om aan te sluiten op de online context waarin cybercriminaliteit plaatsvindt?
8. Welke aanknopingspunten bieden kenmerken en drijfveren van cyberdaders voor een strength-based benadering van interventies?
9. Welke voor- en nadelen zouden kunnen kleven aan strength-based interventies, zoals de Hack_Right-interventie?

8.8 Kernbegrippen

- Desistance-benadering
- Dynamische en statische risicofactoren
- Ethisch hacken
- Financiële straffen
- Gamification
- (Generale en speciale) afschrikking
- Gevangenisstaf
- Hack_Right
- Hooks for change
- Interventies
- Knock and talk
- Online policing
- Rationele-keuzebenadering
- Recidive
- Risk-needs-responsivity-model
- Rolmodellen
- Situationele criminaliteitspreventie
- Strength-based interventies
- Talentontwikkeling

- Verstoring
- Waarschuwingsbanners
- What Works-benadering