# INTERVENTIES JEUGDIGE DADERS CYBERCRIME

K. Oosterwijk Msc
dr. T.F.C Fischer
Sectie Criminologie
Erasmus School of Law
Erasmus University Rotterdam
Datum: 5 Juni 2017

**COLOFON**

**Opdrachtgever**
Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC)
Afdeling Externe Betrekkingen (EWB)
Ministerie van Veiligheid en Justitie
Turfmarkt 147 2511 DP Den Haag

**Onderzoekers**
Het onderzoek is uitgevoerd door de sectie Criminologie van de Erasmus Universiteit Rotterdam
Kim Oosterwijk en Tamar Fischer, mmv Laura Heijnen

© 2017, WODC, Ministerie van Veiligheid en Justitie. Auteursrechten voorbehouden.

# Inhoud

# Samenvatting


## Aanleiding onderzoek en onderzoeksvragen

Met de sterke groei van de mogelijkheden en het gebruik van internet in de afgelopen decennia is ook de criminaliteit in de digitale wereld (cybercrime) aanzienlijk toegenomen. Jongeren zijn sterk vertegenwoordigd op het internet en uit onderzoek blijkt dat zij ook relatief vaak dader zijn van cybercrime. Er is echter nog weinig systematisch inzicht in mogelijke interventies die dit daderschap kunnen terugdringen. Dit onderzoek heeft als doel dit inzicht ter vergroten ten einde beter te kunnen voorkomen dat jongeren beginnen of doorgaan met het plegen van cybercrime. Daartoe wordt onderzocht wat bekend is over de opzet, (beoogde) werking en effecten van interventies gericht op het voorkomen en/of tegengaan van cybercrime onder jongeren.

De onderzoeksvragen zijn:

1. Welke interventies kunnen in de internationale literatuur worden onderscheiden die zich richten op daderschap van cybercrime onder jongeren?
2. In welke categorieën zijn deze interventies in te delen voor de volgende kenmerken:
   a. Het type cybercrime waarop de interventie zich richt.
   b. De populatie waarop de interventie zich richt.
   c. De achterliggende theorie op basis waarvan effectiviteit verwacht kan worden.
   d. De gebruikte methoden in de interventie.
   e. De betrokken uitvoerders.
3. Wat is er bekend over de programma integriteit bij de uitvoering van de interventies?
4. Wat is er bekend over de effectiviteit van de interventies voor het voorkomen van gedigitaliseerde en cybercriminaliteit onder jongeren en op welke wijze is dat onderzocht?
5. Op welke wijze onderscheiden de effectieve en veelbelovende interventies zich van de niet effectieve interventies voor de kenmerken uit de tweede onderzoeksvraag?

## Methoden van onderzoek

Het onderzoek vond plaats in twee fasen. In *fase 1* is onderzocht welke geëvalueerde interventies voor (potentiële) jeugdige daders van cybercrime er in de wetenschappelijke literatuur beschreven zijn. In *fase 2* is voor twee typen cybercrime namelijk cyberagressie en hacking een verdiepende studie uitgevoerd waarbij verder gekeken is dan de geëvalueerde interventies en beschreven is welke inzichten, ervaringen, en aanbevelingen uit literatuur en praktijk relevant kunnen zijn bij de ontwikkeling en selectie van interventies in de toekomst.

Om na te gaan welke interventies gericht op daderschap van cybercrime onder jongeren in de internationale literatuur kunnen worden onderscheiden is een uitgebreide systematische literatuurstudie uitgevoerd (fase 1). Deze was zowel gericht op bronnen die specifiek gaan over geëvalueerde interventies voor jeugdige cybercriminelen (recidivebeperking) als op geëvalueerde interventies gericht op de preventie van daderschap in algemene populaties (preventie cybercrime in het algemeen). Uit de eerste fase van het onderzoek kwam een groot aantal bronnen naar voren waarin geen specifieke interventie werd geëvalueerd maar waarin

wel bevindingen stonden over dadergroepen en delictgedrag. Deze studies zijn belangrijke input geweest voor de verdiepende studie naar aangrijpingspunten voor interventies voor cyberagressie en hacken (fase 2). Aan deze bronnen zijn voor fase 2 nog verschillende overzichtsstudies en bronnen over cyberdaderpopulaties toegevoegd. Daarnaast heeft raadpleging van experts (uit praktijk en onderzoek) plaatsgevonden tijdens twee discussiebijeenkomsten, enkele interviews, en e-mailcontact. Doelen van deze raadpleging waren het verkrijgen van *up to date* kennis betreffende recente en innovatieve interventies en reflectie op de resultaten uit de literatuurstudie.

# Resultaten

## Systematische literatuurstudie geëvalueerde interventies

De zoektocht naar evaluatiestudies leverde evaluaties van 39 verschillende interventies op. Dit betrof vrijwel uitsluitend interventies gericht op algemene populaties en dus op de preventie van daderschap onder potentiële daders en niet op recidivepreventie bij daders. Het overgrote deel van deze preventieve interventies was bovendien gericht op het systeem (zoals het geheel van actoren en interacties binnen klas of school) en is dus naast een directe beïnvloeding van het gedrag van (potentiële) daders ook gericht op beïnvloeding van het gedrag van (potentiële) slachtoffers en omstanders. Twee studies belichten interventies die wel specifiek gericht zijn op daders, dit betrof de inzet van *reintegrative shaming* bij hackers en van *restorative justice* bij daders van *stalking*. In beide gevallen ging het echter meer om een benadering en niet om vastomlijnde interventies. De evaluatiestudies betroffen dan ook geen effectstudies maar inhoudelijke evaluaties over mogelijke effectiviteit. Hieronder bespreken we de kenmerken van de gevonden interventies volgens de structuur van onderzoeksvragen 2 t/m 4. Er zal blijken dat voor het antwoord op onderzoeksvraag 5 informatie uit de verdiepende studie nodig is.

*Type cybercrime waarop de interventie zich richt*

De interventies uit de systematische literatuurstudie richten zich op de volgende typen cybercrime:

- cyberagressie (10)
- sexting (13)
- hacking (4)

Daarnaast zijn er 8 interventies gevonden die zich op online veiligheid in het algemeen richten waarbij ook het daderaspect aandacht krijgt (i.e. bewustwording van wat illegaal is en van wat de gevolgen van het gedrag kunnen zijn). Tot slot hebben we evaluaties van vier technische interventies gevonden die specifiek dadergericht zijn. De cyberagressie interventies richten zich grotendeels op vormen van cyberpesten en in één geval gaat het om *stalking*. Dit betekent dat maar voor een beperkt deel van voorkomende cyberagressie delicten interventies gevonden zijn. Ook zijn er dus geen interventies gevonden gericht op daderschapspreventie of het voorkomen van recidive bij financieel-economische criminaliteit in de cyberwereld.

*Populatie waarop de interventie zich richt*

De interventies voor online veiligheid en cyberagressie richten zich in de meeste gevallen op kinderen en jongeren op de basisschool en in het begin van het voortgezet onderwijs. Sexting

interventies zijn gericht op jongeren in het voortgezet onderwijs. Bij de hacking en de technische interventies is geen afgebakende leeftijdsgroep benoemd. De meeste interventies richten zich zoals beschreven op de hele groep kinderen of jongeren in de specifieke leeftijdsgroep en niet alleen op daders.

*Achterliggende theorieën*

Een beperkt deel van de interventies beschrijft theorieën op basis waarvan effectiviteit kan worden verwacht. Het gaat dan vooral om sociale leer theorieën, de theorie over normatief sociaal gedrag, en de theorie van gepland gedrag. De interventies voor cyberagressie zijn grotendeels afgeleid van bestaande anti-pest programma's en gebruiken vooral systemische theorieën waarin de rol van groepsnormen (descriptief en injunctief) en invloed van die normen op het gedrag van individuen centraal staan. Voor dit type cyberagressie zou het verlagen van de sociale opbrengsten voor de daders, door het creëren van meer afkeurende normen op groepsniveau, de kans op agressie verlagen. De *sexting* interventies zijn weinig theoretisch onderbouwd en lijken vooral gebruik te maken van afschrikkingsgerichte theorieën. Bij de hacking interventies wordt een combinatie van uitgangspunten uit de rationele keuze benadering, *reintegrative shaming* en afschrikkingstheorieën gebruikt.

*Gebruikte methoden*

Voorlichting, Psycho-educatie, en cognitieve gedragstherapeutische methoden (waarbinnen positieve versterking en versterken moreel redeneren) zijn veel ingezette methoden in de geëvalueerde interventies. Daarbij worden ook rollenspellen ingezet om de normen van anderen te onderzoeken en om handelingsopties te trainen. In verschillende interventies wordt ook praktische training ingezet voor het vergroten van sociale vaardigheden en de cognitieve en affectieve empathie. De voorlichting en pyscho-educatie richt zich als het om voorkomen van daderschap gaat vooral op kennis over de aangerichte schade bij slachtoffers en eventuele strafrechtelijke gevolgen voor daders zelf. Deze laatste methode wordt ook ingezet bij hacking interventies. Overigens zijn de gebruikte methoden bij de hacking interventies beperkt beschreven.

*Betrokken uitvoerders*

Een logisch gevolg van de nadruk die ligt op interventies voor algemene populaties jongeren, is dat de uitvoering vooral plaatsvindt op scholen. De programma's worden soms door de leerkrachten zelf uitgevoerd en soms door externe trainers van (private) instanties die de programma's ontwikkeld hebben. Sommige programma's zijn volgens de programma-beschrijving ook beschikbaar voor toepassing binnen het strafrecht maar er zijn geen evaluatiestudies gevonden gericht op een dergelijke toepassing. Voor een van de mogelijk effectieve hacking interventies (de *hack-in-contests*) zijn bedrijven belangrijke uitvoerders. Een enkele keer worden de politie of ouders genoemd als uitvoerder bij een interventie.

*Programma integriteit*

Er is maar beperkt informatie beschikbaar over de mate waarin de programma's worden uitgevoerd zoals bedoeld. Wel blijken de actieve lesmethoden waarbij daadwerkelijk training en interactief leren plaatsvindt nog weinig centraal te staan in programmabeschrijvingen en feitelijke uitvoering. Daarmee zijn zowel de vertaling van de achterliggende werkzame

mechanismen naar de programmabeschrijving als de programma integriteit bij veel interventies nog beperkt. Effecten van de programma's zouden mogelijk groter zijn als dit beter wordt uitgewerkt.

*Effectiviteit*

Voor een derde van de interventies (13 van 39) was er daadwerkelijk een effectstudie beschikbaar. Dit zijn voornamelijk online veiligheid en cyberagressie interventies. Voor de overige interventies ging het om inhoudelijke evaluaties gericht op de potentiële effectiviteit van de interventie. Van de effectstudies hadden er 4 (voor cyberagressie en hacken) een daadwerkelijke experimenteel design en nog eens 5 een quasi-experimenteel design[1].

De cyberagressie-programma's blijken cyberdaderschap enigszins te beperken en zijn dus in zekere mate effectief. Dit geldt niet voor de op effectiviteit getoetste online veiligheid, sexting- en hacking interventies waarvoor effectevaluaties beschikbaar waren.

*Onderscheidende kenmerken effectieve en veelbelovende interventies*

Er is maar voor een type programma daadwerkelijk effectiviteit vastgesteld voor het inperken van daderschap namelijk de anti-cyberpestprogramma's. Deze programma's houden rekening met verschillende aspecten waarvan bekend is dat ze de effectiviteit van daderinterventies vergroten, zoals de inzet op dynamische criminogene factoren (i.e. groepsdruk, gebrek aan toezicht, en gebrek aan empathie voor het slachtoffer mede onder invloed van het online disinhibitie-effect) en het afstemmen van de interventie op de responsiviteit van de doelgroep (waarbij de systeem-aanpak met de nadruk op groepsnormen een belangrijke functie heeft). Interventies die hoofdzakelijk inzetten op voorlichting of afschrikking blijken weinig effectief.

Voor veel programma's zijn er echter geen effectevaluaties beschikbaar en we kunnen dus verder weinig definitieve conclusies trekken over de effectiviteit van de bestudeerde interventies. Wel zijn er op basis van inhoudelijke evaluaties positieve verwachtingen van op *reintegrative shaming* geïnspireerde interventies bij hacking. Hierbij gaat het om interventies waarin samen met de hackers veranderingen in de hackersubcultuur worden gecreëerd waarmee binnen de groep meer afkeurende normen tegen schadelijk hacken worden.

## Verdiepende studie potentiële interventies

De verdiepingsstudie die in de tweede fase van het onderzoek is uitgevoerd voor de delict typen cyberagressie en hacking maakt het mogelijk een iets uitgebreider antwoord te geven op de vraag naar kenmerken van en dus aangrijpingspunten voor effectieve interventies (onderzoeksvraag 5). Hoewel het antwoord op deze vraag voor cyberagressie en hacking verschillend is, blijkt er bij beide delict typen een grote behoefte te bestaan aan kennis en training bij de professionals in het veld. Naast kennis over het gedrag en de omstandigheden van cyberdaders gaat het daarbij ook om kennis over de mogelijkheden van technologische interventies die gebruikt kunnen worden bij de aanpak van jeugdige cyberplegers. Bij het

[1] Daarbij is wel sprake van een voor- en na-meting bij een interventie en een controle groep maar zijn de groepen niet op basis van random toewijzing samengesteld.

ontwikkelen van interventies moet er dus ook aandacht zijn voor de training van deze professionals[2].

*Cyberagressie*

Uit de literatuur blijkt dat jeugdige plegers van cyberagressie sterk lijken op plegers van offline agressie. Bestaande interventies bij de ketenpartners en zorgverleners (zoals agressie regulatietrainingen en cognitieve vaardigheden trainingen) kunnen dus mogelijk ook werken bij het terugdringen van de risico's op cyberagressie. De literatuur beschrijft echter ook diverse mogelijke verschillen waarmee rekening gehouden moet worden. In de eerste plaats beschrijft de literatuur over pesters dat online plegers gemiddeld minder hoog scoren op algemene agressie schalen terwijl zij online ernstige vormen van agressie laten zien. In de tweede plaats zijn online pesters vaker zelf slachtoffer van online of offline agressiviteit, de motieven voor het plegen van agressie zijn dus mogelijk deels anders. In de derde plaats zijn er verschillen gevonden in kenmerken die de responsiviteit voor interventies kunnen beïnvloeden zoals de sociale intelligentie, de mate van drugsgebruik en de mate van zelfcontrole. In de vierde plaats lijkt er een sterke rol te zijn van online disinhibitie. Door de anonimiteit van zowel dader als slachtoffer, kan de beleving van de consequenties van het gedrag bij de daders van online agressie fundamenteel anders zijn dan bij offline agressie. Mogelijk kunnen recente ontwikkelingen in *virtual reality* en *serious gaming* een bijdrage leveren aan interventies waarin jongeren de consequenties van hun gedrag beter onder ogen zien. De effecten van deze technieken zijn echter nog maar beperkt getest en zullen moeten worden aangepast voor verschillende typen daders, delicten en situaties.

*Hacking*

Hacking interventies zouden zich volgens experts en de literatuur niet gericht moeten zijn op de onderdrukken van al het hackgedrag maar op het voorkomen dat jongeren vanuit de meer 'goedaardige' vormen van hacken overgaan naar zwaardere vormen waarin financieel gewin of macht de belangrijkste motieven zijn. Hacking interventies moeten daarom gericht zijn op bewustwording over de schade van het gedrag en de gevolgen die het gedrag voor de eigen toekomst kan hebben. Ook het aanbieden van alternatieven waarmee legaal de gezochte uitdaging gevonden kan worden, wordt hierbij genoemd. Bij de groep van jeugdige hackers blijkt snel handelen en in contact blijven me de jeugdige hackers van essentieel belang. Experts en literatuur wijzen op de *peergroup* als belangrijke beïnvloedingsfactor en suggereren de *peergroup* dus ook een rol te laten spelen bij interventies. Er is echter nog weinig bekend over de mogelijkheden en risico's daarvan. Geautomatiseerde vormen van reageren zoals bij interventies als digigeren, kunnen mogelijk in de toekomst een rol spellen bij het tijdig aanspreken van jonge hackers. De inhoud en vorm van de boodschap lijken dan wel cruciaal voor de effectiviteit van de interventie. Vooralsnog zijn er geen effectstudies gevonden die de effectiviteit van dergelijke waarschuwingen ondersteunen.

[2] Het gaat daarbij dan zowel om training van professionals (uit bijv. het onderwijs, de jeugdzorg en de politie) die gericht is op preventie en signalering van criminele activiteiten door jongeren als om training van professionals (zoals bijv. de politie en (jeugd)reclassering) gericht op het daadwerkelijk opsporen en effectief straffen van de plegers van cybercriminaliteit.

Tot slot zijn er diverse technische interventies in ontwikkeling die kunnen helpen bij de handhaving van gedrag na veroordeling (i.e. biofeedback, of wifi-blocking door een armband). Ook van deze interventies is de effectiviteit nog niet bekend maar zij zullen net als technische interventies bij offline criminaliteit (denk aan de enkelband) alleen tot blijvende effecten kunnen leiden als ze in combinatie met gedrag veranderende maatregelen worden ingezet die gericht zijn op de aanwezige criminogene factoren.

## Conclusies

De belangrijkste conclusie uit dit onderzoek is dat er in de literatuur nog geen op effectiviteit getoetste interventies beschreven zijn die bedoeld zijn als (strafrechtelijke) reactie op het feitelijk plegen van cybercrime door jeugdigen. Omdat we hier spreken over een relatief nieuw terrein waarop delicten plaatsvinden, is dit niet verrassend. Om de juiste interventies te kiezen en ontwikkelen is het belangrijk dat uitgebreid rekening wordt gehouden met de specifieke problematiek die er speelt (bij daders, slachtoffers en met betrekking tot de situatie). Er is dus veel informatie over de problematiek nodig om de juiste interventies te kiezen en ontwikkelen. Studies naar de achtergronden en dynamiek van cybercrime zijn daarom erg belangrijk bij de ontwikkeling van interventies.

Enkele studies beschrijven benaderingen die mogelijk effectief kunnen zijn in de reactie op feitelijk daderschap (*reintegrative shaming* en *restorative justice*), maar de meeste interventies zijn gericht op de preventie van daderschap in algemene populaties jeugdigen. Van de preventieve programma's zijn alleen de programma's gericht op cyberagressie (voornamelijk cyberpesten) bewezen effectief bij het terugdringen van daderschap. Deze programma's gebruiken veelal een benadering waarbij het stimuleren van afkeurende groepsnormen en aanbieden van handelingsstrategieën voor omstanders en slachtoffers en belangrijke rol spelen. Daarnaast worden daders bewust gemaakt van de gevolgen van hun gedrag.

Uit de verdiepende studie blijkt dat recente studies meer zicht geven op de achtergronden en dynamiek van cybercrime. Op basis van die inzichten kan geconcludeerd worden dat bij cyberagressie mogelijk gebruik gemaakt kan worden van bestaande interventies voor gedragsverandering bij daders. Daarbij zijn echter wel aanpassingen noodzakelijk om rekening te houden met aspecten die een rol spelen bij cybercrime (i.e. afwijkende daderkenmerken ten opzichte van offline agressie en online disinhibitie en de gevolgen daarvan voor het gedrag en de contextinvloeden). Interventies die reageren op hacking moeten volgens de experts in staat zijn tot snel reageren. De precieze inhoud van een effectieve reactie kan echter nog niet bepaald worden op basis van bestaand onderzoek. In de preventieve sfeer is het creëeren van legale alternatieven die de hackers uitdaging bieden mogelijk een optie, maar ook van dergelijke interventies is weinig bekend over de feitelijke effectiviteit en reikwijdte.

Belangrijke kanttekening is dat er zowel bij daders van cyberagressie als bij hackers grote variatie blijkt te zijn binnen de plegersgroep. Ook lijken bepaalde subgroepen nog maar beperkt in beeld te zijn. Zo komt online agressie vaak voor bij plegers die ook offline agressieve delicten plegen maar is er ook een groep die juist alleen online agressief gedrag pleegt. Het is onduidelijk wat precies de criminogene factoren van deze groep zijn. Datzelfde geldt voor de hackers die vanaf het begin hacken met financieel gewin of macht als hoofddoel en dus niet

passen in het veel beschreven patroon van nieuwsgierige middelbare scholier die zich stap voor stap ontwikkelt naar criminele hacker.

De slotconclusie van de studie is dan ook dat voor de ontwikkeling van (strafrechtelijke) reacties op daders van cybercrime, het van belang is de kennis over de dadergroep en het verloop van de nu ingezette interventies verder te verfijnen. Dit is moeilijk omdat het darknumber voor deze delicten relatief groot is. Betere signalering van de delicten en opsporing van de daders heeft dus de eerste prioriteit. Daarnaast lijkt er ook winst te behalen door beter te monitoren hoe cyberdaders die nu al veroordeeld worden momenteel geregistreerd worden in de strafrechtelijke systemen[3], welke criminogene factoren en indicatoren voor responsiviteit er voor deze daders worden benoemd (op basis van bijvoorbeeld de RISc of andere screeningsinstrumenten) en welke straffen of maatregelen er vervolgens worden opgelegd. Meer systematische toegang tot dergelijke informatie maakt het mogelijk te leren van de initiatieven en interventies die nu ontwikkeld en toegepast worden.

[3] Is bijvoorbeeld altijd duidelijk dat het om cyberdelicten gaat of worden algemene delictcodes voor bijvoorbeeld bedreiging of stalking gebruikt?

# Voorwoord

In dit rapport presenteren wij een inventarisatie van bestaande kennis over interventies gericht op jeugdige daders van cybercrime en gedigitaliseerde criminaliteit. Voor dit onderzoek is een systematische literatuurstudie uitgevoerd. Daarnaast hebben wij in individuele interviews en expertgroepen met experts gesproken uit wetenschap en praktijk op het gebied van cybercrime. Al deze experts willen wij hartelijk danken voor het delen van hun kennis en ervaringen.

De auteurs, Kimberley Oosterwijk en Tamar Fischer zijn bij de totstandkoming van het onderzoek bijgestaan door de begeleidingscommissie onder voorzitterschap van Jessica Asscher (UvA). We danken haar en de overige leden van de commissie: Rutger Leukfeldt (NSCR), Ton Eijken (MinVenJ, DSJ) en Casper van Nassau (WODC) voor de adviezen, het naar voren brengen van literatuur en contactpersonen en de opbouwende commentaren op eerdere versies van dit rapport. Laura Heijnen (EUR) danken wij voor het snel en zeer nauwkeurig transcriberen van de expertgroep discussies en het helpen zoeken en documenteren van literatuur.

Rotterdam, 18 mei 2017

Kimberly Oosterwijk en Tamar Fischer

# 1. Inleiding

We leven in een tijd waarin nieuwe technologieën steeds sneller binnendringen in elk aspect van de sociale, economische en de persoonlijke levenssfeer (Katz, 1996; Facer & Furlong, 2001; Holt & Bossler, 2014; Yar, 2012). De mogelijkheden voor mensen om te communiceren zijn sterk toegenomen doordat de obstakels in termen van afstand, tijd en locatie zijn verdwenen (Capeller, 2001; Van de Hulst & Neve, 2008; Wall, 2007). Het gebruik van ICT zoals mobiele telefoons, computers en internet heeft onder jongeren een grote vlucht genomen (Mesch, 2012; Zebel, De Vries, Griebels, Kuttschreuter, & Stol, 2013; Korvorst & Sleijpen, 2014; Katz, 1996; Holt & Bossler, 2014). Zo is in Nederland het aandeel 12 – 15 jarigen dat dagelijks thuis internet gebruikt tussen 2005 en 2013 gestegen van 76% naar 93% (Van der Laan & Goudriaan, 2016). In de leeftijdscategorie 12-18 jarigen had 90% van de jongeren ook internettoegang buitenshuis (CBS, 2014). Internet en online communicatie zijn uitgegroeid tot een integraal onderdeel van de (jeugd)cultuur (Mesch, 2012; Korvorst & Sleijpen, 2014; Facer & Furlong, 2001).

De uitbreiding en diversificatie van de sociale netwerken van jongeren, evenals het altijd aanwezige contact met leeftijdsgenoten door internet, creëert nieuwe sociale eisen en mogelijkheden (Mesch, 2012; Capeller, 2001; Yar, 2012). Het ideaal van internet als open ruimte zonder autoriteit of controle (Barlow, 1996; Lodder & Schermer, 2014) brengt ook gevaren met zich mee. Bij de afwezigheid van externe druk van autoriteiten zal niet elke gebruiker van internet zelfregulatie tonen om de verleidingen en mogelijkheden te weerstaan die internet biedt voor het plegen van deviant of zelfs crimineel gedrag (Capeller, 2001; Van der Hulst & Neva, 2008; Schermer & Lodder, 2014). Internet biedt kinderen al op jonge leeftijd de mogelijkheid om zich te kunnen onttrekken aan de controle van hun ouders en de offline maatschappij (Katz, 1996; Mensch, 2012). Dit gebeurt op een leeftijd waarop zij vaak nog onvoldoende cognitieve of psychosociale inzichten hebben in normatieve vraagstukken (Eisenberg et al., 2005). Tevens is er veelvuldige blootstellingen aan nieuwe gelegenheden voor en verleidingen tot het plegen van criminaliteit (Holt & Bossler, 2014; Yar, 2005; Zebel et al, 2013).

In de wetenschappelijke literatuur wordt vaak onderscheid gemaakt tussen twee typen cybercrime: in brede en enge zin[4]. Cybercrime in brede zin wordt ook wel gedigitaliseerde criminaliteit genoemd. Dit type cybercrime wordt getypeerd door de menselijke handelingen, ICT is maar een klein element en faciliteert slechts de misdaad. Het zijn traditionele delicten gepleegd met een computer of computertechnologie. Cybercrime in enge zin wordt getypeerd door misdaden waarbij ICT het instrument en het doelwit is. Het zijn 'nieuwe delicten', delicten die niet bestonden of konden bestaan zonder ICT (De Cuyper & Weijters, 2016; Gordon & Ford, 2006; Brenner, 2004; Zebel et al, 2013; Fahey, 2014).

Uit de veiligheidsmonitor 2015 (CBS, 2016a) blijkt dat zo'n 1 op de 9 burgers in de 12 maanden voorafgaand aan de enquête slachtoffer was geworden van een of meer cyberdelicten. Van de jongeren (15 tot 25 jaar) rapporteert in 2015, 1 op de 6 slachtoffer te zijn

[4] Er is overigens veel wetenschappelijke discussie over wat de term precies inhoudt en de term is dan ook moeilijk te definiëren (o.a. Brenner, 2004; Fahey, 2014; Gorden & Ford, 2006; De Cuyper & Weijters, 2016; Holt & Bossler, 2014). Zo kent cybercrime veel verschillende aspecten, kan het plaatsvinden in een wijde variatie aan scenario's en is de invulling afhankelijk van de percepties die daders, slachtoffers en 'beschermers' hebben over wat cybercrime inhoudt (Gordon & Ford, 2006).

geweest van een online delict (CBS, 2016b). Jongeren blijken ook relatief vaak dader van cybercrime (Jansen, Junger, Montoya, Hartel, Stol & Jansen, 2013) maar er is nog weinig systematisch inzicht in mogelijke interventies die dit daderschap kunnen terugdringen. Dit onderzoek richt zich daarom op de vraag op welke wijze voorkomen kan worden dat jongeren beginnen of doorgaan met het plegen van cybercrime. Dit onderzoek beoogt een inventarisatie te geven van mogelijkheden voor de bestrijding van gedigitaliseerde criminaliteit en cybercrime onder jongeren. Meer precies wordt onderzocht: Wat bekend is over de opzet, (beoogde) werking en effecten van interventies gericht op het voorkomen en/of tegengaan van cybercrime onder jongeren.

De volgende onderzoeksvragen zullen worden beantwoord:

1. Welke interventies kunnen in de internationale literatuur worden onderscheiden die zich richten op daderschap van cybercrime onder jongeren?
2. In welke categorieën zijn deze interventies in te delen voor de volgende kenmerken:
   a. Het type cybercrime waarop de interventie zich richt.
   b. De populatie waarop de interventie zich richt.
   c. De achterliggende theorie op basis waarvan effectiviteit verwacht kan worden.
   d. De gebruikte methoden in de interventie.
   e. De betrokken uitvoerders.
3. Wat is er bekend over de programma integriteit bij de uitvoering van de interventies?
4. Wat is er bekend over de effectiviteit van de interventies voor het voorkomen van gedigitaliseerde en cybercriminaliteit onder jongeren en op welke wijze is dat onderzocht?
5. Op welke wijze onderscheiden de effectieve en veelbelovende interventies zich van de niet effectieve interventies voor de kenmerken uit de tweede onderzoeksvraag?

# 2. Theoretisch kader

Er is veel discussie in de cybercrime literatuur of de criminele handelingen in de digitale wereld wel echt 'nieuwe' criminele handelingen zijn en daarom anders aangepakt moeten worden dan traditionele delicten (o.a. Yar, 2012; Zebel et al, 2013). Zo stellen sommige wetenschappers dat cybercrime alleen verschilt van traditionele criminaliteit in het feit dat het zich afspeelt op internet, maar dat bestaande theorieën voor het grootste deel onverminderd toepaspaar zijn (o.a. Grabosky, 2001; Skinner & Fream, 1997; Pontell & Rosoff, 2008). Andere wetenschappers stellen dat internet een nieuwe sociale omgeving is, met een eigen structuur, interactie-vormen, beperkingen en mogelijkheden, die zich zodanig onderscheidt van de offline wereld dat er nieuwe theorieën ontwikkeld moeten worden voor het verklaren van de criminaliteit (o.a. Yar, 2012; Zebel et al, 2013; Holt & Bossler, 2014; Suler, 2004; Snyder, 2001; Brenner, 2004). Een laatste groep wetenschappers wijst erop dat het bij deze discussie uitmaakt over welke vorm van cybercrime je het hebt en daarbij in welk type cybercrime (brede of enge vorm) deze criminele handeling geplaatst wordt (Leukfeldt & Yar, 2016; Van der Hulst & Neve, 2008).

Wat vaststaat, is dat ten opzichte van de traditionele (fysieke) criminaliteitsvormen de nieuwe (virtuele) varianten een aantal voordelen hebben. Zo zijn de barrières van tijd en ruimte verdwenen waardoor binnen enkele seconden direct contact mogelijk is met personen overal ter wereld. Daardoor zijn de mogelijkheden voor het bereiken van potentiële slachtoffers groter geworden. Verder kunnen activiteiten relatief gemakkelijk en veelvuldig worden herhaald of gelijktijdig plaatsvinden. Internet of wel ICT wordt dan ook wel aangeduid als een *force multiplier*. Hiernaast hebben individuen online een zekere vorm van anonimiteit (inclusief de mogelijkheid om een andere identiteit aan te nemen) wat kan leiden tot 'disinhibitie'. Dit houdt in dat jongeren (en volwassenen) zich minder geremd gedragen en vrijer met elkaar communiceren (Yar, 2012; Van der Hulst & Neve, 2008; Zebel et al, 2013).

## 2.1 Cybercrime interventies

Voor een goede analyse betreffende interventies die uitgevoerd kunnen worden om te voorkomen dat jongeren cybercrime plegen is het van belang om rekening te houden met de specifieke kenmerken van internet. Ook de heterogeniteit in vormen van cybercrime is van belang (Gorden & Ford, 2006; Yar, 2012; Van der Hulst & Neve, 2008; Zebel et al, 2013; Suler, 2004). Preventieliteratuur, zowel vanuit de situationele als vanuit de dadergerichte preventie, heeft immers overtuigend laten zien dat een aanpak alleen effectief kan zijn als hij gericht is op het specifieke probleem (Clarke, 2009; Lipsey & Cullen, 2007). Naast een concrete probleemanalyse en doelgroep afbakening, nemen daarom in de preventieliteratuur de theoretische onderbouwing voor de werkzaamheid van een interventie en de daarbij passende methodologische aanpak een steeds centralere rol in (Fischer & Zwirs, 2013). In dit onderzoek zullen deze aspecten dan ook centraal staan bij de inventarisatie en analyse van de bestaande interventies. Hieronder wordt dit kort verder toegelicht.

Bij dadergerichte interventies ter preventie van offline delicten is de '*What Works*' benadering (Andrews, Bonta, & Hoge, 1990) het meest dominant als het gaat om de ontwikkeling van effectieve interventies. Volgens deze benadering kunnen interventies gericht op de preventie van recidive alleen effectief zijn wanneer zij rekening houden met het risico op recidive (risicoprincipe), de dynamische factoren die tot het criminele gedrag leiden

(criminogene factoren) en de capaciteiten, leerstijl en leerbaarheid van de dader (responsiviteit) (a.o. Lipsey & Cullen, 2007; Lowenkamp, Latesssa, & Holsinger, 2006). Een belangrijke factor voor het tot stand komen van houding- en gedragsverandering, is de aanwezigheid van motivatie (McMurran & Ward, 2010). Deze benadering heeft geleid tot de ontwikkeling van interventies waarvan daadwerkelijk een verlaging van recidive uitgaat (Lipsey & Cullen, 2007). Indien voldoende informatie beschikbaar is, zal bij het analyseren van de methodologische aanpak van dadergerichte interventies in deze studie worden nagegaan of en zo ja hoe met de kernfactoren uit de *What Works* literatuur rekening is gehouden.

Tot slot is het van belang na te gaan of uitvoerders erin slagen de interventies zo uit te voeren als ze waren bedoeld, de zogenoemde programma integriteit (zie o.a. Andrews & Dowden, 2005). Als de programma's afwijken van het plan dan is het de vraag op welke elementen de interventies afwijken. Hierbij kan gedacht worden aan de bereikte doelgroep, de kwaliteit van de professionals die de interventie uitvoeren, de feitelijke toepassing van de effectief veronderstelde methoden, en de feitelijke blootstelling van de doelgroep aan de interventie. Vervolgens moet worden beschreven wat de mogelijke consequenties daarvan zijn.

# 3. Methoden

Het eerste gedeelte van het onderzoek betrof een uitgebreide systematische literatuurstudie gericht op bronnen die specifiek gaan over geëvalueerde interventies voor jeugdige cybercriminelen (zie figuur 3.1). Het doel daarvan was om in kaart te brengen welke getoetste interventies er bestaan gericht op jeugdige plegers van cybercrime en in welke mate ze effectief blijken of lijken te zijn. We hebben ons daarbij zowel gericht op feitelijke effectstudies, als op inhoudelijke beoordelingen die nagaan of interventies in theorie effectief kunnen zijn[5].

In de tweede fase van het onderzoek is geïnventariseerd welke kennis er in de literatuur en praktijk beschikbaar is die relevant is bij de ontwikkeling en selectie van interventies in de toekomst (zie figuur 3.1). In deze verdiepende fase van het onderzoek is gefocust op een beperkte selectie van cybercrime delicten namelijk cyberagressie en hacken (zie paragraaf 5.1 Verantwoording selectie cyberdelicten). Voor deze verdieping is er gebruik gemaakt van bronnen uit de systematische search (fase 1) die daar niet bruikbaar bleken omdat geen specifieke interventie werd geëvalueerd, maar die wel de dadergroepen en/of het delictsgedrag onderzochten. In deze bronnen werden vaak op basis daarvan ook aanbevelingen over interventies gedaan. Daarnaast zijn bronnen over cyberdaderpopulaties in Nederland en verschillende overzichtsstudies over onderzoek naar cybercrime geanalyseerd. De literatuurstudie in deze fase is aangevuld met informatie uit twee discussiebijeenkomsten met experts uit het veld. Deze sessies hadden als doel de meest *up to date* kennis te verkrijgen betreffende recente en innovatieve interventies. De sessies dienden ook als expertreflectie op de resultaten uit de literatuurstudie[6].

Figuur 3.1: Schematische weergave methode

| Methode | | |
|---|---|---|
| | Fase 1 | Systematische literatuurstudie naar geëvalueerd interventies. |
| | Fase 2 | Verdiepende informatie uit de literatuurstudie en Expertbijeenkomsten |

## 3.1 Systematische literatuurstudie

Voor de literatuurstudie zijn sociaalwetenschappelijke en juridische databanken geraadpleegd. Sociaalwetenschappelijke literatuur komt uit de volgende databanken: Scopus, Web of Science, Pubmed, PsycInfo, ProQuest, WODC-site en de mediatheek van de Politie Academie. Tevens zijn Boom Juridische Tijdschriften (met onder andere Tijdschrift voor Criminologie, Tijdschrift voor Cultuur en Criminologie, Tijdschrift voor Veiligheid, Tijdschrift voor Toezichthouders) als extra specifieke tijdschriften geraadpleegd. Daarnaast is de zoekmachine SSRN geraadpleegd

[5] Vergelijk ex-ante evaluaties erkenningscommissie justitiële interventies (Fischer, 2015), of het erkenningsniveau 'goed onderbouwd' van de erkenningscommissie jeugdinterventies NJI (http://www.nji.nl/nl/Databank/Geslaagde-Introductie-nieuwe-Erkenningscommissie-Justitiele-Interventies).

[6] Naast de expertbijeenkomsten zijn er nog enkele interviews (telefonisch en face-to-face) gehouden met cybercrime onderzoekers, is er een bijeenkomst bijgewoond van het Lectoraat Cybersafety en is er e-mail contact geweest met een medewerker van HALT en met medewerkers van de jeugdreclassering. Deze informatie is ook in de expertreflectie meegenomen.

voor ‘grijze’ literatuur en lopende onderzoeken. Juridische literatuur is gezocht in de volgende databanken: de Praktizijns bibliotheek, Kluwer navigator, HEINONLINE[7].

Bij het zoeken van bronnen is een uitgebreide verzameling zoektermen gebruikt die was samengesteld op basis van enkele kernpublicaties. Na de eerste zoektocht is door middel van een VOSviewer zoektermen analyse gekeken of er aanvulling van de zoektermen nodig was, dit bleek niet nodig te zijn. De gebruikte zoektermen zijn door Booleaanse operatoren en truncaties in meerde zoektermen sets verwerkt. De eerste zoektermen set ‘cyber’ betreft zoektermen die het criminele gedrag beschrijven. De tweede zoektermen set richt zich op de doelgroep ‘jongeren’, met de derde zoektermen set worden bronnen geselecteerd die gericht zijn op ‘interventies’ en de vierde zoektermen set ‘dader’ om er voor te zorgen dat er specifiek geselecteerd wordt op interventies voor jeugdige cybercriminelen en niet op alleen slachtoffers (zie bijlage 2).

Uit deze criminologische en juridische systematische zoektocht[8] kwamen in totaal 746 bronnen naar voren. Na het verwijderen van dubbele bronnen en na beoordeling op basis van de titels, bleven 390 bronnen over. Van deze 390 bronnen zijn de abstracts gelezen en werd bepaald of de inhoud concreet gericht was op cyberdelicten door jeugdige plegers en er in het artikel informatie over concrete interventies stond. Dit resulteerde in een selectie van 124 bronnen waarvan 108 bronnen beschikbaar waren. Van deze 108 bronnen bleken er maar 8 een feitelijke evaluatiestudie (voor 8 verschillende interventies). Vervolgens is in de referentielijsten van de 108 bronnen gezocht en tevens is voor alle in de 108 bronnen genoemde interventies (totaal 75) op naam van de interventie gezocht naar meer evaluatiestudies, in de databanken en aan de hand van de websites van de interventies. Dat leverde 118 nieuwe bronnen op waarvan 26 feitelijke evaluaties over in totaal 31 interventies voor jeugdige cybercrime plegers. Alles bij elkaar zijn er dus evaluaties gevonden voor 39 interventies gericht op cybercrime bij jeugdige plegers (zie figuur 3.2).[9]

De 39 geëvalueerde interventies betreffen 3 technische interventies om cyberdelicten te voorkomen en 36 interventies gericht op menselijke actoren binnen cyberdelicten (zie bijlage 2). In hoofdstuk 4 zal uiteindelijk blijken dat het overgrote deel van deze geëvalueerde interventies gericht is op algemene populaties potentiële plegers van schadelijk online gedrag waarbij geen duidelijke afbakening in strafrechtelijke zin gemaakt wordt. Geen van deze 39 geëvalueerde interventies zijn specifiek ontwikkeld voor jeugdige cybercrime daders van specifieke strafrechtelijk gedefinieerde cyberdelicten.

## 3.2 Experts

De participanten voor de expertsessies zijn doelgericht geselecteerd, ook wel *purposeful sampling* genoemd (Evers, 2015). De participanten zijn geselecteerd op grond van hun kennis

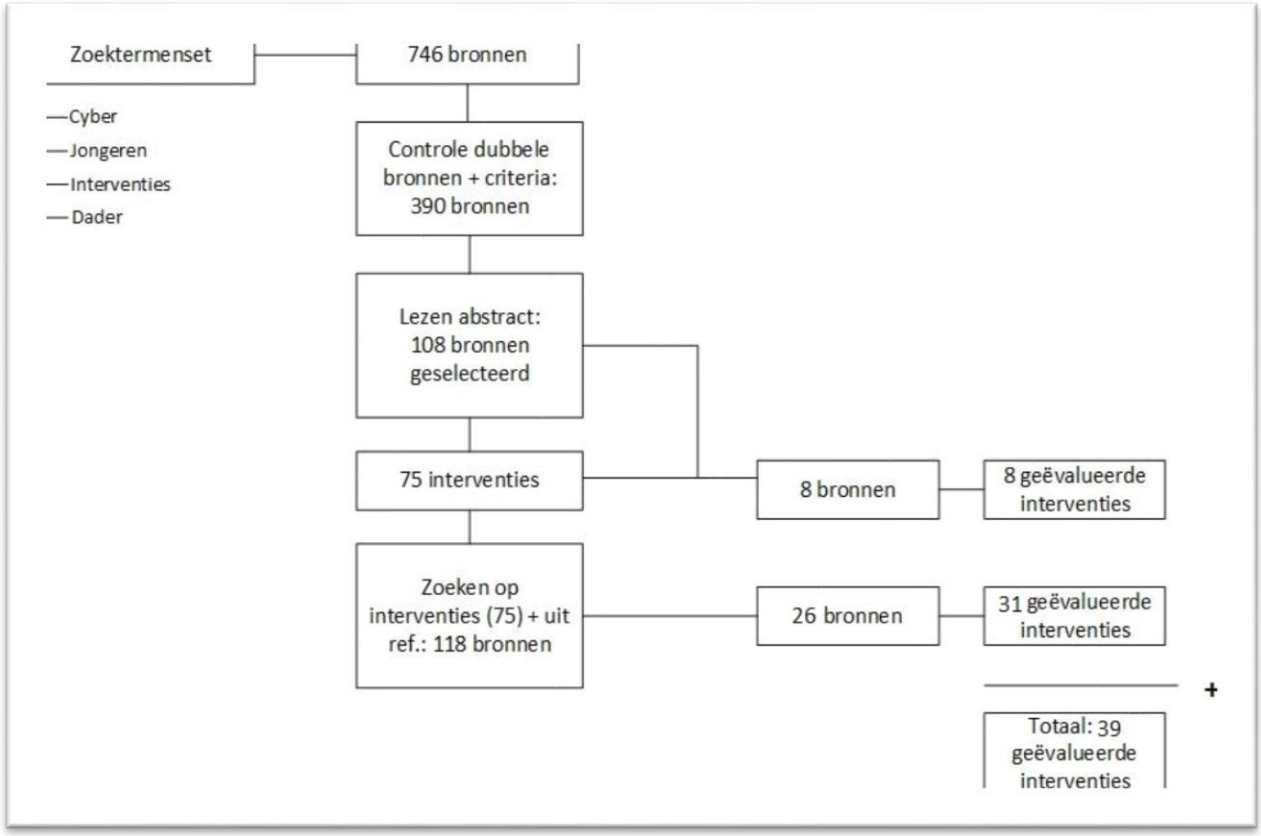
[7] Ook Legal intelligence, Rechts Orde en EUR-Lex zijn bekeken, maar is er besloten deze niet mee te nemen, omdat deze alleen jurisprudentie weergeeft en geen wetenschappelijke literatuur.

[8] Er is een extra (criminologische & juridische) zoektocht gedaan om te controleren of alle onderzoeken betreffende hacken en financieel economische criminaliteit zijn meegenomen. Dit door de zoektermen set ‘dader’ weg te laten. Hier zijn geen nieuwe bronnen uitgekomen.

[9] Zoals in de introductie van dit hoofdstuk al genoemd, beschrijven veel van de afgevallen bronnen wel factoren waar rekening mee gehouden moet worden bij interventies of zelfs concrete suggesties voor interventies. Die informatie is meegenomen in de tweede fase van dit onderzoek.

over cybercrime, over interventies, of omdat ze werkzaam zijn in een veld waarbij zij in aanraking komen met cybercriminelen. De bijeenkomst over Hacken bestond uit 13 experts, afkomstig uit: de wetenschap, beleid en praktijk (politie, ethische hackers, OM en reclassering). Bij de bijeenkomst cyberagressie waren er 11 experts aanwezig. Ook zij waren afkomstig uit: de wetenschap, beleid, en de praktijk (reclassering, bedrijven die zich bezighouden met technologische innovaties). Van de bijeenkomsten zijn geluidsopnamen gemaakt, die vervolgens volledig getranscribeerd en gecodeerd zijn. Respondenten zullen in dit rapport per expertsessie worden geciteerd met een R, een nummer en een omschrijving 'onderzoeker', 'beleidsexpert', of 'praktijkexpert'. De respondenten van losse interviews die expliciet behandeld worden zijn op dezelfde manier aangegeven, maar krijgen daarbij de toevoeging 'a'.

Figuur 3.2 Stroomdiagram literatuurstudie



# 4. Literatuurstudie naar geëvalueerde interventies

Uit de literatuurstudie is geen enkele geëvalueerde interventie naar voren gekomen die zich specifiek richt op jeugdige daders van gedigitaliseerde criminaliteit of cybercriminaliteit (i.e. veroordeelde jeugdige daders van cyberdelicten). In twee studies werden theoretische uiteenzettingen gevonden over de mogelijkheid van het gebruik van *Re-intergratieve Shaming* voor Hackers en de beschrijving van de inzet van *Restorative justice* (voor stalking als onderdeel van cyberagressie) voor cyberdaders in het algemeen (dus van alle leeftijden). Deze laatste benadering lijkt goed toepasbaar voor jeugdige daders, maar er was hier geen sprake van een vastomlijnde interventie. Daarnaast is een diversiteit aan interventies gevonden voor algemene populaties potentiële daders. Deze interventies richten zich op diverse vormen van schadelijk online gedrag waarbij geen duidelijke afbakening in strafrechtelijke zin gemaakt wordt. Zo blijken interventies voor het terugdringen van cyberagressie zich te richten op een grote variëteit aan gedragingen: van online roddelen of buitensluiten tot ernstige bedreiging of smaad (zie ook: Kerstens en Stol, 2012). Ditzelfde geldt voor hacken, en sexting. Wellicht nog meer dan bij offline criminaliteit is er voor gedragingen in de cyberwereld nog veel onduidelijkheid en discussie over de strafbaarheid van bepaald gedrag (Holt & Bossler, 2014; Fahey, 2014). Bovendien zijn daders zich, ook als bepaald gedrag wel duidelijk strafbaar is gesteld, vaak niet bewust van de strafbaarheid van hun handelen. Goed voorbeeld hiervan is het downloaden van software en muziek (Zebel et al., 2013).

Omdat de afbakening tussen wel en niet strafbaar gedrag binnen de meeste interventies niet wordt gemaakt, bevat de in dit hoofdstuk gepresenteerde selectie van interventies dus ook dit grijze gebied van online gedrag dat wel schade oplevert maar niet strafbaar is gesteld. De wijze waarop de beschreven interventies criminaliteit proberen te beperken kan worden ingedeeld in drie hoofdstrategieën, deze zijn:

1) het beperken van de toegang tot of beschikbaarheid van criminele doelen (door technische maatregelen of via het gedrag van de potentiële slachtoffers).
2) het opleggen van beperkingen op, of directe controle van potentiële daders (door technische maatregelen, via formeel toezicht of via informeel toezicht op de daders).
3) het vergroten van de bewustwording bij daders over welke gevolgen hun handelen heeft voor zichzelf, de slachtoffers, en de samenleving (zoals educatie of cognitieve programma's, automatische berichten in de online omgeving, of door personen in de online omgeving).

In de verschillende interventies die tijdens de literatuurstudie zijn gevonden zijn deze drie strategieën soms apart en soms in combinatie aanwezig. Het uitgangspunt van dit onderzoek was om dadergerichte en niet op het delict gerichte interventies te onderzoeken. Daarom is de inventarisatie hoofdzakelijk gericht op interventies uit de tweede en derde strategie. Een deel van de interventies (voornamelijk interventies voor online veiligheid en tegen cyberagressie) blijkt echter slachtoffer- en daderschapspreventie te integreren. Als slachtofferschapspreventie effectief is dan zou dit indirect (via strategie 1) ook implicaties kunnen hebben voor daderschap. Afhankelijk van de manier waarop de effecten gemeten zijn, kunnen directe en indirecte effecten (via de weerbaarheid van het slachtoffer) beter uit elkaar

worden gehouden. Bij het bespreken van deze interventies zal hier bij worden stilgestaan. De focus zal steeds liggen op de effecten van de interventies op het terugdringen van daderschap.

In onderstaande bespreking laten we technische interventies die gericht zijn op de algemene bescherming van doelwitten buiten beschouwing. Het gaat dan om interventies zoals anti virussoftware en firewalls die potentiële slachtoffers moeten beschermen tegen infecties van malware (schadelijke software zoals virussen, wormen, of *trojans*) (Burguera, Zurutuz & Nadjm-Tehrani, 2011; Louk, Lim, & Lee, 2014; Oberoi, 2014). Deze interventies vallen binnen de eerste strategie van preventiemaatregelen, maar het is binnen de kaders van dit onderzoek onmogelijk om in beeld te brengen welke rol deze interventies specifiek spelen bij het terugdringen van cybercrime binnen de populatie jeugdigen. Eerder onderzoek liet zien dat deze interventies de kans op slachtofferschap veelal niet verlagen (Leukfeldt & Yar, 2016). Omdat het wel om een breed toegepast type interventie gaat, is het belangrijk deze categorie interventies niet te vergeten in de algemene discussie over effectieve interventies

De interventies die wij wel bespreken, richten zich dus meer direct op de menselijke factor. Daaronder vallen ook technische interventies zoals internetfilters die door ouders of andere toezichthoudende actoren kunnen worden ingesteld, *community policing* en *virtual neighbourhood watch*. Omdat voor deze interventies nog geen feitelijke toepassingen op jeugdige daders zijn geëvalueerd, bespreken we deze interventies aan het einde van dit hoofdstuk, dat geldt ook voor interventies gebaseerd op *virtual neighbourhood watch.* We beginnen opvolgend met de bespreking van de interventies die zich richten op online veiligheid, cyberagressie, sexting en hacken.

Met deze bredere afbakening waarbij naast interventies voor jeugdige overtreders van specifieke wetsartikelen ook preventieve interventies zijn meegenomen die gericht zijn op het grijze gebied van schadelijk gedrag in de cyberwereld en algemene populaties potentiële plegers, zijn de volgende aantallen geëvalueerde interventies gevonden: acht interventies die gericht zijn op veilig internet gebruik, tien interventies voor cyberagressie, dertien voor sexting, vier voor hacken en vier technische interventies (zie tabel 4.1). Totaal gaat het om 39 verschillende interventies.

Tabel 4.1 Aantal geëvalueerde interventies uit de literatuurstudie

| *Interventietype* | *Aantal geëvalueerde interventies in literatuur* |
|---|---|
| Online Veiligheid | 8 |
| Cyberagressie | 10 |
| Sexting | 13 |
| Hacken | 4 |
| Technisch | 4 |

## 4.1 Online Veiligheid: bewustwording en vaardigheden

De acht interventies die als doel hebben om veilig internetgebruik te stimuleren, richten zich allemaal op jongeren in de algemene populatie (zie bijlage 3, tabel 1). Het gaat dan dus om potentiële slachtoffers, daders en omstanders. De programma's richten zich vrijwel allemaal op

kinderen en jongeren in het basis- en voortgezet onderwijs. Alleen het programma Net-detectives van KidSmart (Wishart, et al., 2007) richt zich uitsluitend op het basisonderwijs.

Tabel 4.2 Korte beschrijving van de online veiligheidsprogramma's

| |
|---|
| Het **Cybersmart programma** helpt scholen (PO/VO) om risico's van cyberveiligheid te identificeren en te beheren. Dit gebeurt door *empowerment* van leraren, leerlingen en ouders met de kennis, vaardigheden en strategieën voor het effectief aanpakken van cyberveiligheid kwesties. Het programma bevat een interactief, online klaslokaal curriculum over de belangrijkste aspecten van het internet, waaronder: veiligheid, omgangsvormen, reclame, onderzoek en technologie. (Beavis, et al., 2011) |
| Het **iKeepSafe** programma omvat educatief materiaal voor scholen (PO/VO) dat is gericht op de gehele gemeenschap (opvoeders/scholen/strafrechtelijk apparaat). Het programma verstrekt informatie over wat ongepaste inhoud, contact en gedrag online zijn en hoe het kan worden herkend en voorkomen. Het bevat bovendien een interactief programma gericht op online reputatie en privacy. (Jones, Mitchell, & Walsch, 2014) |
| **ISafe** moet leerlingen (PO/VO) het bewustzijn en de kennis bijbrengen voor het herkennen en voorkomen van gevaarlijk, schadelijk online gedrag bijbrengen. Het bevordert het idee dat het internet een gemeenschap is en daarom vereist dat leden verantwoordelijk handelen en verantwoordelijk worden gesteld voor hun daden. Ook bij dit programma worden schoolleiders, ouders en leerlingen betrokken in de interventie. (Jones, Mitchell, & Walsch, 2014; Chibnall, Wallace, Leicht, & Lunghofe, 2006) |
| **NetSmartz** is een onderwijsprogramma voor jeugd van 6 tot 18 jaar (PO/VO) om hen kennis te geven en vaardigheden te leren over de potentiële risico's van het internet en om te voorkomen dat ze slachtoffer worden van online exploitatie. De onderwijsprogramma's voor oudere leerlingen omvatten een scala aan onderwerpen, online agressoren (*predators*), ongepaste online relaties, cyberpesten, privacy, online reputaties en respectvol gedrag bij het gamen. (Jones, Mitchell, & Walsch, 2014) |
| **WebWiseKids** een programma met interactieve geautomatiseerde games die betrekking hebben op de onderwerpen: piraterij, e-fraude, online-romances, cyberstalking, online criminelen en identiteitsfraude. (Jones, Mitchell, & Walsch, 2014; 2012) |
| **KnowItAll** een interactieve multimedia diashow gericht op *empowerment* van middelbare scholieren, leraren en ouders om hun computer te beveiligen, zich online veilig te gedragen en te weten waar ze heen kunnen gaan voor hulp. (Wishart, Andrews, & Ching Yee, 2005) |
| **Net-Detectives van KidSmart** een creatief online rollenspel. Waar kinderen door sociaal leren via virtuele simulaties van situaties voor potentiële slachtoffers gemotiveerd, in staat worden gesteld om te discussiëren en te leren over veiligheid (Wishart, Oades, & Morris, 2007) |
| **Social Networking Safety Promotion and Cyberbullying Prevention** is een presentatie die verschillende aspecten van online veiligheid aan de kaak stelt, waarbij er een combinatie tussen educatie en afschrikking wordt gebruikt. (Roberto, Eden, Savage, Ramos-Salazar, & Deiss, 2014) |

*Programmadoelen*

Wanneer er gekeken wordt naar de programmadoelen van online veiligheidsinterventies blijkt de nadruk te liggen op het voorkomen dat jongeren slachtoffer worden. Maar er zijn ook programmadoelen die zich richten op het voorkomen van daderschap (vetgedrukt in tabel 1 bijlage 3). Daarbij gaat het vooral om bewustwording van wat illegaal gedrag op internet is en om het opdoen van kennis en inzicht over de mogelijke gevolgen van hun handelen (zoals schade bij het slachtoffer en negatieve effecten op het eigen leven). De interventies zetten daarmee vrijwel altijd in op intermediaire (tussenliggende) doelen[10]. Het feitelijk terugdringen van daderschap is maar bij één interventie een programmadoel (namelijk: NetSmartz).

[10] Zie voor een themabijeenkomst over zulke intermediaire doelen: http://www.knaw.nl/nl/actueel/beeld-geluid/themabijeenkomst-tasten-in-het-duister-het-gebruik.

Concrete intermediaire doelen uit de interventies gericht op het terugdringen van daderschap zijn (zie: Beavis, et al. 2011; Chibnall, et al., 2006; Jones, Mitchell, & Walsch, 2014):

1) Versterken kritisch denken
2) Vergroten kennis over internetethiek
3) Vergroten kennis over intellectueel eigendom / piraterij
4) Vergroten kennis over (on)acceptabel online gedrag
5) Voorkomen van risicovol gedrag online

Deze doelen zijn dus vooral gericht op het creëren van kaders voor jongeren om beter geïnformeerd en dus bewuster keuzes te maken voor hun gedrag online. Daarbij is naast focus op het vergroten van de kennis over gevolgen van gedrag voor slachtoffers, de samenleving als geheel en de plegers zelf, ook veel aandacht voor 'cyberburgerschap', internetethiek en kennis over intellectueel eigendom (Cybersmart; Ikeepsafe; Isafe).

*Gebruikte methoden*
De meest voorkomende methode om de doelen te bereiken, is het geven van voorlichting over de online risico's en consequenties van vormen van antisociaal online gedrag. Bij 7 van de 8 interventies is sprake van een 'sociaal ecologische' aanpak. Dit betekent dat de interventie ingrijpt op individueel-, klas-, school-, en gemeenschapsniveau. Hierbij wordt door middel van het voorlichten van ouders en docenten (aan de hand van presentaties of online materiaal) getracht een ondersteunende en controlerende omgeving te creëren (Cross, et al., 2016). Aan de jongeren wordt daarnaast klassikaal voorlichting gegeven. Naast kennisoverdracht wordt in sommige interventies aan de hand van interactief materiaal en rollenspellen vaardigheden aangeleerd en inzichten verdiept. Hierbij wordt gebruik gemaakt van uitgangspunten van sociaal leren.

*Effectiviteit*
Van de 8 interventies is er voor 5 interventies (CyberSmart, ISafe, KnowItAll, Net-Detectives en Social Networking Safety Promotion and Cyberpesten Prevention) een effectevaluatie uitgevoerd. Hieronder waren geen studies met een experimenteel design, wel was er één quasi-experimentele studie, was er één studie met een voor en nameting zonder controle groep, één studie met een controlegroep maar alleen een nameting en waren er twee studies met alleen een nameting (zie tabel 4.3). Gegeven deze designs zal het dus maar beperkt mogelijk zijn conclusies te trekken over de effectiviteit van de interventies.

Tabel 4.3 Designs van de evaluatiestudies naar interventies voor online veiligheid

| Experimenteel design | Quasi-experimenteel design | Voor/nameting zonder controle groep/ posttest gecontroleerd | Nameting zonder controle groep | Inhoudelijke evaluatie |
|---|---|---|---|---|
| | ISafe | Cybersmart | KnowItAll | iKeepSafe |
| | | Social Networking Safety promotion | Net-Detectives | ISafe |
| | | | | NetSmartz |
| | | | | WebWiseKids |

*over ISafe zijn twee evaluaties met een verschillend design gevonden.

Slechts één evaluatiestudie (ISafe) kijkt naar effecten op feitelijk gedrag van potentiële daders door de mate van onacceptabel online gedrag[11] te meten (Chibnall, et al., 2006). Hier werd geen effect van de interventie gevonden. Van de studies die effecten onderzoeken op de intermediaire uitkomsten: kennis van en inzicht in online daderschap, wordt één interventie gevonden die effectief lijkt te zijn voor het inperken van daderschap. Het gaat dan om de bewustwording dat je beter kunt afzien van 'wraaknemen op pesters' (Roberto, et al. 2014). Dit betreft dus een hele specifieke groep cyberagressieplegers (reactieve agressie naar aanleiding van pesten). Daarnaast lijkt het Cybersmart programma erin te slagen kennis en inzicht over veilig en verantwoord deelnemen aan de digitale wereld bij potentiële daders en slachtoffers te vergroten. Hierbij wordt geen onderscheid gemaakt tussen daderschapsgerichte en slachtoffergerichte doelen en de conclusies worden getrokken op basis van informatie uit focusgroepen (Beavis, et al., 2011).

Voor het terugdringen van slachtofferschap geven de evaluatiestudies meer informatie maar ook dit levert geen eenduidige conclusies op. Er worden geen effecten gevonden op feitelijk gedrag (Chibnall, Wallace, Leicht, Lunghofer, 2006) maar wel op de gedragsintentie om verdachte situaties te melden aan een volwassene (Roberto, et al., 2014) en diverse maten van risicobewustzijn en kennis[12] (Chibnall, et al., 2006; Schilder, et al, 2016).

Het uitblijven van effecten op gedrag zowel bij potentiële daders als bij slachtoffers kan mogelijk verklaard worden met behulp van een door Jones, Mitchel en Walsch (2014a) ontwikkelde KEEP-checklist (Known Elements of Effective Prevention). De KEEP-checklist is een lijst met elementen voor educatieve programma's waarvoor uit empirisch onderzoek aanwijzingen zijn gevonden dat ze effectief kunnen zijn. Zo bleek dat educatieve interventies waarin naast bewustwording van risico's ook het aanleren van vaardigheden om risico's te vermijden expliciet als programmadoel was opgenomen, effectiever zijn dan de interventies die alleen op bewustwording zijn gericht. Hoewel er bij de meeste interventies gericht op veilig

[11] Dit betrof een schaal van 9 items waaronder: 'verzenden of online posten van dingen die kwetsend of gemeen voor anderen zijn', 'kijken naar ongepaste foto's online' of 'gokken via internet'. In deze schaal zitten ook items die in meer algemene zin over risicovol gedrag gaan zoals 'het vertellen van je password aan vrienden' en 'het openen van junkmail'.

[12] Zoals het herkennen van digitale kinderlokkers, beheersing van risico's online, risico's bij het delen van informatie, virusherkenning (Chibnall, et al, 2006).

internetgebruik naast voorlichting wel de intentie was ook training te gegeven om gedragsverandering te realiseren, werd dit in de meeste gevallen beschreven als bijzaak, en staat het vaak niet expliciet vermeld in de programmadoelen. Dit komt ook duidelijk naar voren uit de inhoudelijke evaluatie van iKeepSafe, iSafe, NetSmartz, WebWiseKids, aan de hand van de KEEP-checklist (Jones, et al., 2014b). Hier wordt gesteld dat van deze 4 interventies slechts 2 interventies trainingsdoelstellingen hadden, waarvan er voor 1 training aannemelijk is gemaakt op basis van theorie dat jongeren hierdoor online veiliger gaan handelen.

*Programma integriteit*

Uit de evaluaties wordt niet duidelijk in hoeverre het creëren van de ondersteunende omgeving door het voorlichten van ouders en docenten daadwerkelijk toegepast wordt en hoe effectief dit is. Bij de interventies naar online veiligheid lijkt er dus sprake van een beperkte programma integriteit. Het betreft daarbij juist aspecten die aansluiten bij de algemene responsiviteit bij het bereiken van gedragsverandering namelijk interactief en praktisch trainen van vaardigheden en inzichten in een motiverende omgeving van goed getrainde 'coaches' (Andrews & Bonta, 1990).

## 4.2 Cyberagressie: slachtoffers, daders en omstanders

Van de tien beschreven interventies voor cyberagressie richten negen zich op cyberpesten. De tiende interventie (Restorative Justice, Halder, 2015) richt zich op stalking. De anti-cyberpest interventies zijn vrijwel allemaal ontwikkeld met als uitgangspunt traditionele (en dus offline) anti-pest interventies. Voor deze traditionele antipest interventies is uitgebreid onderzoek gedaan een zijn duidelijke aanwijzingen voor hun effectiviteit gevonden (Olweus, 2010; Holt, Raczynski, et al. 2013). Onze literatuurstudie leverde totaal veertien evaluaties op naar de effectiviteit van interventies voor het tegengaan van cyberpesten.[13] Cyberpesten wordt in de onderzochte interventies veelal gedefinieerd als een agressieve opzettelijke daad, uitgevoerd door een individu of groep met behulp van ICT (zie tabel 2, bijlage 3). De gevonden interventies richten zich allemaal op jongeren in het algemeen, en net als bij de meeste 'online veiligheid interventies' (paragraaf 4.1), richten de interventies zich op potentiële slachtoffers, daders en omstanders. Een interventie richt zich daarbij exclusief op leerlingen op de basisschool (Bully Busters), vijf interventies richten zich op de hogere klassen van het basisonderwijs en op het voortgezet onderwijs (Conred, Kiva, Meida Heroes, Restorative Justice en VISc), drie interventies richten zich alleen op leerlingen uit het voortgezet onderwijs (Friendly schools, No-Trap, Positieve Psychologische benadering) en een interventie richt zich op eerste en tweede jaar studenten aan de universiteit (TRA). Net als in de online veiligheid interventies staat veelal het voorkomen van slachtofferschap centraal. Net als de online veiligheidsinterventies maken de antipest interventies gebruik van de 'sociaal ecologische aanpak' waarin verschillende actoren (leraren, ouders en leerlingen) uit een gemeenschap worden betrokken bij het terugdringen van cyberpesten.

[13] Voor sommige interventies is meer dan 1 effectstudie uitgevoerd.

Tabel 4.4 Korte beschrijving van de cyberagressieprogramma's

| |
|---|
| Het **Bully Busters programma** is een programma tegen pesten. Met als doel kinderen sociaal acceptabele waarden aan te leren en hen te helpen begrijpen hoe ze anderen met respect moeten behandelen. De focus is zowel dader- als slachtoffergericht en doelt op de verbetering van het zelfbewustzijn. (Cuffy, 2015) |
| **ConRed** (Conocer, Construir y Convivir en la Red) is een educatief programma dat door middel van voorlichting en sociaal leren gericht op de ontwikkeling van positieve emoties, sociale en technische vaardigheden, gezonde tijdsinvestering in ICT wil zorgen voor het veilig en voorzichtig gebruik van het internet. (Del Rey, Casas, & Ortega, 2015). |
| **Friendly Schools Whole-of-School project** anti-pest programma dat is aangepast voor cyberpesten. Gericht op de proximale en distale risico- en beschermende factoren die gereguleerd of gemedieerd zouden kunnen worden op school, klas, familie en/of individuele niveaus om cyberpesten te verminderen. De interventie is gericht op de online contexten waarin studenten communiceren en de acties en reacties die ze daar en offline uitwisselen. (Cross, Shaw, Hadwen, Cardoso, Slee, Roberts, Thomas, & Barns, 2016) |
| **KiVa** is een curriculum programma gericht op positieve veranderingen in het gedrag van *peers* (omstanders, slachtoffers en daders) gericht op het verminderen van de beloning die pestkoppen krijgen en het aanleren van specifieke gedragsstrategieën voor slachtoffers om zich in bedreigende omstandigheden te verdedigen. (Salmivalli, Kärnä, & Poskiparta, 2011; Williford, Elledge, Boulton, DePaolis, Little, & Salmivalli, 2013) |
| **Media Heroes** wil cyberpestgedrag verminderen door het bevorderen van kennis en competenties (i.e. empathie, kennis over gevolgen van cyberpesten, vaardigheden en strategieën voor omstanders en slachtoffers om in te grijpen bij cyberpestsituaties). Dit gebeurt door studenten psycho-educatie te geven over definities, wettelijke rechten, online beveiligingsopties, en training van sociale vaardigheden en hen vaardigheden voor perspectief nemen bij te brengen. (Chaux, Velasque, Schultze-Krumbholz, & Scheithauer, 2016; Wolfer, Schultze-Krumbholz, Zagorscak, Jakel, Gobel, & Scheithauer, 2014; Schultze-Krumbholz, Schultz, Zagorscak, Wolfer, & Scheithauzer, 2016). |
| Het **NoTrap!** is een educatief programma dat o.a. gebruik maakt van sociaal leren waarbij voorlichting plaatsvindt, wordt door *peers* en online programma's. (Palladino, Nocentini, & Menesini, 2016; Menesini, Nocentini, & Palladino, 2012) |
| **Positief psychologische benadering** Het doel van deze aanpak is het bevorderen van positieve relaties met leeftijdsgenoten om zo relationele agressie tegen te gaan. Een hoog niveau van sociale steun kan de negatieve invloed van relationeel pesten verminderen en het psychisch welbevinden stimuleren. (Chesssor, 2008) |
| **Restorative justice** ook wel Herstelrecht benadrukt het herstellen van de schade door bemiddeling waarbij het slachtoffer, de dader en de juridische actoren en mediatoren op een niet vijandige manier het probleem proberen op te lossen. Herstelrecht richt zich op beïnvloeding van communicatieve technieken, waaronder begrip en empathie van de juridische actoren. (Navarro, Vuberto, & Larranaga, 2016; Halder 2015) |
| **Theory of Reasoned Action (TRA)-based video program** geeft voorlichting om positieve houdingen ten opzichte van het pestgedrag tegen te gaan en stimuleert de afwijzende normen ten opzichte van het pestgedrag. (Doane, Kelley, & Pearson, 2016) |
| **ViSC** is een preventief programma met een systemisch perspectief dat gebruik maakt van voorlichting en sociaal leren met als doelen: (a) voorkomen van agressief gedrag en pesten en (b) de sociale en interculturele competenties van actoren in scholen te versterken. (Gradinger, Yanagida, & Strohmeier, 2015; Gradinger, Yanagida, Strohmeier, & Spiel, 2016) |

*Programmadoelen*

Twee interventies (Theory of Reasoned Action (TRA)-based video program, ViSC Social Competence Program) benoemen het feitelijk terugdringen van cyberpesten als programmadoel (Doane, Kelley, Pearson, 2016; Gradinger, et al., 2016). Het overgrote deel van programmadoelen dat bij de interventies genoemd wordt, betreft dus ook hier intermediaire doelen, via welke de interventies uiteindelijk indirect tot een afname in cyberpesten moeten leiden. De intermediaire programmadoelen die beschreven worden zijn in te delen in de volgende categorieën:

1) Kennis en bewustzijn vergroten over de prevalentie en gevolgen van pesten.
2) Veranderen van individuele en groepsnormen in afkeurende normen ten opzichte van cyberpesten.
3) Aanleren van (sociale) vaardigheden om te reageren bij incidenten.
4) Verbeteren van emotioneel welzijn van potentiële pesters en slachtoffers.
5) Vergroten van de empathie bij (potentiële) pesters.
6) Vergroten van online vaardigheden.

Van deze programmadoelen is alleen programmadoel 5, het vergroten van empathie exclusief en direct op potentiële pesters gericht. Het gaat hierbij zowel om affectieve empathie wat inhoudt dat potentiële pesters leren om mee te voelen wat anderen voelen en cognitieve empathie waarbij het gaat om begrijpen wat anderen voelen (bijv Media Heroes, Schultze-Krumbholz, et al., 2016). Andere programmadoelen die direct op pesters zijn gericht maar die ook veranderingen bij omstanders (inclusief ouders en docenten) en/of slachtoffers beogen, zijn de programmadoelen 1, 2 en 4. Programmadoel 1, het vergroten van kennis en bewustzijn over cyberpesten en de gevolgen voor slachtoffers, spreekt voor zich en blijkt ook vooral een tussenstap te zijn naar het bereiken van andere programmadoelen zoals het vergroten van de empathie (doel 5) en het creëren van afkeurende normen (doel 2). Programmadoel 2 kent verschillende uitwerkingen. De meeste interventies met dit programmadoel richten zich op het creëren van afkeurende normen over cyberpesten op klasse niveau zodat de sociale beloning voor het pestgedrag afneemt. Daarbij wordt onderscheid gemaakt tussen injunctieve normen (wat van je verwacht wordt te doen) en descriptieve normen (wat je anderen ziet doen). Er is ook een interventie die gebruik maakt van al aanwezige afkeurende normen over cyberpesten op het niveau van de klas door de individuele normen te confronteren met deze klasse normen (Media Heroes, Chaux, et al., 2016). Interventies met programmadoel 2 veranderen de (sociale) kosten en baten van het plegen en verminderen daarmee de aantrekkelijkheid van het cyberpesten. Sommige interventies richten zich ook specifiek op de aanwezigheid van positieve sociale relaties (Friendly schools, Cross, et al. 2016). Programmadoel 4 dat gaat over het verbeteren van het emotioneel welzijn van potentiële slachtoffers *en* potentiële daders omvat ook factoren als het zelfbewustzijn en de self efficacy (positief psychologische benadering, Chessor, 2008; Kiva, Williford, et al. 2013).

Programmadoelen 3 en 6 zijn voornamelijk op slachtoffers en omstanders gericht, waarbij programmadoel 3 zich richt op het trainen van reacties door slachtoffers en omstanders en het aanreiken van handelingsalternatieven bij incidenten. Hier spelen actief burgerschap, pro-sociaal gedrag en de aanwezigheid van conflict oplossingsvaardigheden bij omstanders een belangrijke rol (No-trap, Palladino, et al. 2016; positief psychologische benadering, Chessor, 2008).

*Gebruikte methoden*

De methoden die bij de interventies worden ingezet zijn vrij eenduidig (zie Tabel 2, bijlage 3 voor detailverschillen). De meeste interventies stellen dat kennisoverdracht en het geven van duidelijke kaders over acceptabel gedrag jongeren zullen helpen een pro sociale houding aan te nemen en pro sociaal gedrag te vertonen. Richting de plegers gaat het dan vooral om kennis over de schade die het gedrag aanricht maar ook over de gevolgen voor daders (bijvoorbeeld

eventuele strafrechtelijke gevolgen). Daarnaast worden cognitieve gedragstherapeutische methoden ingezet en is er aandacht voor positieve versterking en het versterken van het moreel redeneren. Bij sommige interventies wordt er tevens gebruik gemaakt van trainingen om jongeren aan de hand van rollenspellen te laten uitvinden welke normen anderen hebben, en om te leren hoe je kunt optreden als omstander (Bully Busters Program, KiVa, Media Heroes en ViSC). Ook het trainen van sociale vaardigheden, cognitieve en affectieve empathie en onlinevaardigheden komt in verschillende interventies terug (Conred, Media Heroes).

*Effectiviteit*

Voor zeven van de tien interventies zijn effectstudies gedaan. Bij drie interventies betrof dit een of meer studies met een experimenteel design (RCT), bij vier interventies een quasi-experimenteel design (matching of gecontroleerd) en voor een interventie een casestudie. Voor drie interventies zijn alleen inhoudelijke evaluaties beschikbaar (zie tabel 4.5). Voor de zeven op effectiviteit getoetste interventies zijn totaal vijftien effectstudies gedaan[14]. Alle effectstudies zijn gebaseerd op zelfrapportages van jongeren waarbij gevraagd is naar welzijn, houding, gedrag en ervaringen met cyberpesten. Voor vijf van de zeven interventies zijn effecten op feitelijk cyberpesten en op slachtofferschap van cyberpesten bepaald, bij de andere twee interventies zijn geen effecten op slachtofferschap maar wel op cyberpesten bepaald.[15]

Tabel 4.5 Designs van de evaluatiestudies naar interventies tegen cyberagressie

| Experimenteel design | Quasi-experimenteel design | Voor/nameting zonder controle groep/ posttest gecontroleerd | Nameting zonder controle groep | Inhoudelijke evaluatie/ case studie |
|---|---|---|---|---|
| KiVa | Conred | | | Bully Busters Program |
| Media Heroes | Friendly schools | | | Restorative Justice |
| ViSC | No Trap | | | Positieve psychologische benadering |
| | TRA-video program | | | |

Alle interventies blijken tot een significante afname in cyberpesten en/of slachtofferschap van cyberpesten te leiden. Van de vijf interventies waarvan de effecten op slachtofferschap en daderschap worden gemeten zijn er bij vier interventies (Conred, Friendly schools, Kiva en No Trap) sterkere afnames in gerapporteerd slachtofferschap dan in gerapporteerd cyberpesten. De vijfde studie (VISc) vindt juist sterkere effecten op daderschap. Van deze laatste interventie

[14] Voor sommige interventies is er meer dan één effectstudie gevonden.

[15] Slechts bij twee programma's werd het terugdringen van cyberpesten als expliciet programmadoel geformuleerd, veel interventies formuleren intermediaire doelen maar daar wordt in lang niet alle effectevaluaties aandacht aan besteed.

zijn ook de langere termijn effecten bepaald en daarin blijft dit beeld overeind (Gradinger, et al. 2016). Deze bevinding sluit aan bij de programmadoelen van de VISc die veel meer dan de andere interventies exclusief zijn gericht op het terugdringen van agressief gedrag en pesten. Andere interventies richten zich tegelijk op weerbaarheid, vaardigheden en welzijn van slachtoffers.

Sommige studies geven ook inzichten in verschillen in effecten van interventies voor jeugdigen met verschillende kenmerken (subgroepanalyses). Del Rey, et al. (2012) concluderen dat het programma Conred wel effect heeft op het daderschap voor daders die zelf ook slachtoffer zijn van (cyber)pesten en niet op de daders die uitsluitend dader zijn. Deze bevinding sluit aan bij de conclusie van Roberto et al. (2014) dat het effect van de SNSPCP interventie[16] vooral tot stand komt via de intermediaire uitkomst 'intentie om geen wraak te nemen'. Deze bevindingen suggereren dat een belangrijk gedeelte van de cyberagressoren niet bereikt wordt met de interventies. Een van de twee effectstudies van de KiVa gaf aan dat de interventie alleen bij jongere leerlingen het cyberpesten vermindert (Williford, et al., 2013). De evaluaties van de interventies Media Heroes (Schultz-Krumbholz, Schultz, Zagorscak, Wolfer en Scheithauze, 2016) en ViSC (Gradigner et al., 2015) vonden dat de effecten vooral groot waren bij leerlingen die voorafgaand aan de interventie laag scoorden op beschermende factoren zoals cognitieve en affectieve empathie en hoog scoorden op cyberpesten (Schulze-Krumbhol, et al. 2016). Het effect van de interventie No Trap, lijkt sterker voor mannen dan voor vrouwen (Palladino, et al., 2012), maar in een vervolgstudie werd dit onderscheid niet meer gevonden (Palladino, et al., 2016). De ViSC heeft juist sterkere effecten op meisjes zowel als het om het pesten als om het gepest worden gaat (Gradigner et al., 2015).

Naast effecten op cyberpesten en slachtofferschap zelf, toetsen twee studies ook effecten van de interventies op de tussenliggende programmadoelen. De interventie Media Heroes blijkt positief bij te dragen aan het aanleren van cognitieve en affectieve empathie, perspectief nemen en afname van algemene agressie (Media Heroes, Schultz-Krumbholz, Schultz, Zagorscak, Wolfer en Scheithauze, 2016). Er wordt in de studie echter geen verband gevonden tussen het aanleren van cognitieve en affectieve empathie en een afname in cyberpesten of in cyberslachtofferschap. Een verband dat gezien de theorie achter de interventie wel verwacht was. In de evaluatie van het op de Theory of Reasoned Action (TRA)-gebaseerde video programma (Doane et al., 2016) wordt getoetst wat het effect is op de aanwezige beschrijvende en injunctieve normen op groepsniveau. De studie vindt geen statistisch significante effecten maar de auteurs schrijven dit toe aan de kleine steekproef en concluderen op basis van de resultaten dat de interventie veelbelovend is.

*Programma integriteit*

In de bestudeerde evaluatiestudies naar cyberagressie is weinig informatie terug te vinden over de programma integriteit. Alleen bij het Bully Busters programma (Cuffy, 2015) wordt geconcludeerd dat het programma in de regel zo uitgevoerd wordt als bedoeld. Dit is op basis van rapportages door de schooldirecteuren bepaald er zijn geen zelfstandige observaties van de onderzoekers aan te pas gekomen.

[16] SNSPCP is de Social Networking Safety Promotion and Cyberbullying Prevention interventie.

## 4.3 Sexting: onthouding en bewustwording

Sexting wordt door de interventies omschreven als de gedraging waarin individuen inhoudelijk seksueel getinte foto's of video's plaatsen of verzenden met behulp van ICT (zie tabel 3, bijlage 3). De gevolgen van Sexting kunnen volgens de evaluatiestudies ernstig zijn. Zo kunnen de seksueel getinte foto's terecht komen in de verkeerde handen, waarmee jongeren vervolgens gepest of gechanteerd kunnen worden (Döring, 2014; Winegust, 2015). Bij sexting speelt er een complicerende factor mee namelijk dat vaak de persoon die de foto of video zelf in eerste instantie verzendt, de persoon is die zelf op het beeldmateriaal staat. Deze persoon wordt in de sexting wetgeving in veel landen als dader beschouwd omdat deze persoon zich immers schuldig maakt aan het maken en de verspreiding van pornografisch beeldmateriaal. Later wordt deze 'dader' slachtoffer nadat andere 'daders' het materiaal doorsturen en mogelijk misbruiken voor pesterijen, smaad of chantage. Het onderscheid tussen daders en slachtoffers is bij deze vorm van cybercrime dus vaak niet te maken (Döring, 2014; DeMitchell & Parker-Magana, 2011). Van de 13 (veelal alleen inhoudelijk) geëvalueerde sexting interventies richten 4 interventies zich alleen op de ouders en docenten. De andere 9 interventies richten zich op jongeren in het algemeen (Döring, 2014; Karian, 2013; Winegust, 2015; Wood; DeMitchel & Parker-Magana, 2001). De leeftijdsgroep waar de interventies zich op richten, ligt zoals te verwachten wat hoger dan bij online veiligheid en cyberagressie. De meeste studies zijn gericht op jongeren vanaf 13 jaar. De bovengrens varieert sterk maar ligt het vaakst rond de 24.

Tabel 4.6 Korte beschrijving van de sexting interventies.

| |
|---|
| **Respect Yourself** is een voorlichtingscampagne gemaakt aan de hand van filmpjes. Met als doel het vergroten van het bewustzijn over de risico's van sexting (Karaian, 2013) |
| **Exposed** is een voorlichtingscampagne gemaakt aan de hand van filmpjes. Met als doel het doen stoppen van sexting (Karaian, 2013) |
| **Pass it On** een educatief voorlichtingsprogramma waarin bewustwording gecreëerd wordt over de risico's van sexting en trainen van gedragsalternatieven. (Winegust, 2015) |
| ***Zero tolerance*** aanpak reageert op sexting van studenten door de student, zonder evaluatie of constitutionele overwegingen, over te dragen aan de politie. (Wood, 2010; DeMitchell, Parker-Magagna, 2011) |

*Programmadoelen*

Van alle dertien geëvalueerde sexting interventies wordt bij twaalf het doen stoppen van sexting als programmadoel benoemd. Om dit te bereiken worden ook hier tussenliggende doelen genoemd die zich richten op bewustwording en het aanleren van reactiestrategieën. Meer specifiek worden de volgende programmadoelen geformuleerd:

1) Het vergroten van het bewustzijn over de risico's van sexting.
2) Het herkennen van online seksueel geweld.
3) Waarschijnlijkheid ingrijpen omstanders vergroten (handelingsstrategieën bieden).
4) Verantwoordelijkheidsgevoelens (bij potentiële plegers) vergroten.
5) Het doen stoppen van sexting.

We zien hier dus ook de verschillende strategieën terug die in het begin van dit hoofdstuk benoemd zijn: de interventies worden ingezet om de weerbaarheid van slachtoffers te vergroten (strategie 1), het toezicht op de daders te vergroten door de kans op omstanderinterventies te vergroten (strategie 2) en door bewustwording bij de slachtoffers en daders van de gevolgen sexting (strategie 3).

De hoofdboodschap van de sexting interventies is een boodschap van gehele onthouding. Sexting wordt hier gezien als een verzameling risicovolle en ongezonde handelingen die weggezet kunnen worden als geseksualiseerd deviant gedrag en daarom in zijn geheel vermeden moeten worden. Van één interventie (het *Pass it On* project) is de boodschap niet gehele onthouding, maar juist het verantwoordelijk omgaan met zulke gedragingen. Door een verhoging van de bewustwording over de online risico's en een training in het herkennen van situaties waarin ingegrepen moet worden, beoogt de interventie de schadelijke gevolgen van sexting tegen te gaan.

*Gebruikte methoden*

De interventies gebruiken vooral voorlichting en discussie om bewustwording van de gevaren van sexting te bereiken. Slechts één interventie, *Pass It On,* traint de jongeren ook door vaardigheden voor omstandersinterventie te vergroten (Winegust, 2015).

*Effectiviteit*

De enige effectevaluatie die we hebben gevonden is van het Pass it On project (Winegust, 2015). Dit is tevens de enige interventie die niet inzet op geheelonthouding maar op het verantwoordelijk omgaan met de gedragingen. De effectevaluatie vindt dat het *Pass it On* project wel effectief lijkt te zijn voor het creëren van intenties en self-efficacy bij omstanders om op te treden als ze sexting observeren. Ook nam het victim blaming af door het programma. De interventie lijkt echter geen effect te hebben op het feitelijk herkennen van seksueel getint geweld of pesten via internet of de perceptie die er is over de aanwezigheid van dit gedrag in de schoolomgeving (Winegust, 2015).

De inhoudelijke evaluaties bij de andere interventies zijn kritisch over deze interventies waarin gehele onthouding voorop staat. Ze raden de boodschap van gehele onthouding af met als argument dat sexting door de 'informatierevolutie' een normaal onderdeel van de seksuele ontwikkeling is geworden. Döring (2014) stelt dan ook dat deze reactie op sexting gezien kan worden als een *moral panic*. Een beleid van totale onthouding waarbij sexting leidt tot strafrechtelijke gevolgen zal volgens Döring grote schade kunnen opleveren. Wat extra schadelijk is volgens evaluatieonderzoeken, is dat de interventies die uitgevoerd worden onder algemene populaties jongeren zich inhoudelijk gezien vaak alleen richten op het gedrag van de meisjes. De kritiek is dan ook dat de interventies actief deelnemen aan *female victim blaming* (Döring, 2014; Karian, 2013).

Tabel 4.7 Designs van de evaluatiestudies naar interventies tegen sexting

| Experimenteel design | Quasi-experimenteel design | Voor/nameting zonder controle groep/ posttest gecontroleerd | Nameting zonder controle groep | Inhoudelijke evaluatie |
|---|---|---|---|---|
| | | Pass it On | | Respect Yourself |
| | | | | Exposed |
| | | | | Zero Tolerance |
| | | | | A thin Line |
| | | | | Before you sext |
| | | | | Common Sense Media |
| | | | | NetSmartz |
| | | | | Respect me don't sext me |
| | | | | SaferInternetProgram |
| | | | | Sheeplive |
| | | | | ThatsNotCool |
| | | | | ThinkUKnow |

*Programma integriteit*

Zoals beschreven in de alinea over effectiviteit zijn er duidelijke beperkingen gevonden aan de programma-integriteit die ook de effectiviteit in de weg zullen staan. Behalve het daar beschreven probleem van victim blaming is ook geconstateerd dat er sterke raciale en leeftijdsselectie in het materiaal is toegepast. Het zijn vooral voorbeelden van blanke tienermeisjes. Daarmee zal de bedoelde boodschap maar een deel van de populatie aanspreken (Karaian, 2013; Döring, 2014). Dit probleem is bij de interventie 'Exposed' duidelijk minder groot dan bij de voorganger 'Respect yourself' (Karaian, 2013) en diverse in door Döring (2014) beschreven campagnes. De evaluaties geven echter niet aan of deze verbetering ook tot een versterking van het gewenste effect leidt.

## 4.4 Hacken: waarschuwen, alternatieven en effectieve normen

De gevonden interventies gericht op hacken, zijn divers in hun manier waarop ze het gedrag van hackers proberen te beïnvloeden. Daarbij zijn de hacking interventies in tegenstelling tot de interventies in de voorgaande paragrafen wel expliciet op daders gericht. Van de 4 gevonden interventies is er één die zich specifiek op jeugdige hackers richt (*re-integrative shaming,* Kao, Fu-Yang Huang, Wang, 2009*)*. De andere drie interventies richten zich op de gehele populatie hackers. Een korte inhoud van de interventies is te vinden in het onderstaande kader:

Tabel 4.8 Korte beschrijving van de hacking interventies

| |
|---|
| **'Duty to Report'**, betreft het beleid waarbij hackers verplicht zijn te melden zodra het hen gelukt is ongeautoriseerd toegang tot een systeem te krijgen. Deze reguleringswijze gaat ervan uit dat hackers geen kwaad in de zin hadden met het hacken (in Nederland heet dit responsible disclosure). (Wible, 2003) |
| **'Hack-in-contest'** (bijv. 'Bug Bounty Program' of 'Crime Diggers'), is een wedstrijd waarbij hackers uitgedaagd worden om een systeem te hacken en de eerste die dit lukt, wint. Dit kunnen ook particulier gesponsorde wedstrijden zijn. (Wible, 2003) |
| **Re-integrative Shaming.** remt de intenties om zich te misdragen door binnen de subcultuur een proces tot stand te brengen van afkeuring van het illegale gedrag. Degenen die deelnemen aan het *shaming*-proces hebben minder kans om zich te misdragen in de toekomst. Dit type van *shaming* veroordeelt het strafbare feit, niet de dader in het openbaar. (Kao, Fu-Yang Huang, Wang, 2009) |
| **Warning banners**<br>Een interventie waarbij het individu online geïnformeerd wordt dat de handeling die ze willen begaan strafbaar is en hoe groot de kans is dat ze gepakt zullen worden. (Maimon, Alper, Sobesto, Cukier, 2014) |

*Programmadoelen:*

De vier hacking interventies formuleren gezamenlijk de volgende programmadoelen:

1) Samenwerking en wederzijds vertrouwen creëren tussen hackers en wetshandhavers.
2) Verandering in de hackersethiek (naar zelfregulatie met gezagsgetrouwe normen).
3) het beïnvloeden van de voorkeuren en mogelijkheden van hackers.
4) Afschrikking creëren.
5) hackers doen stoppen met illegaal hacken.
6) Toename internet beveiliging.

De strategieën die gebruikt worden door de interventies zijn strategie 2 (dadergerichte beperking en controle) en 3 (bewustwording bij daders). Twee studies (die samen drie van de vier interventies evalueren) bediscussiëren waar de grens ligt tussen legaal en illegaal hacken en in hoeverre hacken gecriminaliseerd moet worden (Wible, 2003; Kao, Fu-Yang Huang & Wang, 2009). Deze discussie is belangrijk bij de interventie *Duty-to-report, de hack-in-contest* en de *aanpak volgens reintegrative shaming. Duty-to-report* is een manier van reguleren die er vanuit gaat dat hackers geen kwaad in de zin hadden met de ongeautoriseerde toegang tot het systeem, zolang de hacker inspanning verricht het incident te melden aan de houder van het systeem. De *hack-in-contest* als privaat gesponsorde hacker wedstrijd, zorgt door het organiseren van wedstrijden waarin op verzoek systemen worden gehackt, voor een expressieve- en voorkeur- vormende functie. Terwijl het tegelijkertijd criminaliseren van al het andere hacken zorgt voor een duidelijke signaal en afschrikkingsfunctie. Voorbeelden van hack in contests zijn *bugg bounty* of *crime diggers* (Wible, 2003).

De benadering van *reintegrative shaming* (Kao, Fu-Yang Huang en Wang, 2009) kent als uitgangspunt de observatie dat een aanpak via het strafrecht niet werkt omdat hackers door hun eigen subcultuur gesteund worden in de overtuiging dat ze niks verkeerd doen met het hacken. Na afloop van de straf zullen ze dus opnieuw gaan hacken. Door samen met de hackers veranderingen in de hackersubcultuur te creëren waarmee meer afkeurende normen tegen schadelijk hacken worden gevormd zullen deze vormen van hacken kunnen afnemen. De laatste interventie, namelijk het gebruik van *warning banners* is gericht op het effect van afschrikking (Maimon, Alper, Sobesto, & Cukier, 2014).

*Gebruikte methoden*

*Duty to Report* (of wel *responsible disclosure*), houdt in dat er regels zijn omtrent het hacken waaronder het verplicht stellen van het melden van een hack. Hierover zou duidelijke communicatie richting de hackerswereld moeten bestaan. Daarin wordt ook duidelijk gemaakt dat bij het uitblijven van zo'n melding het gedrag strafbaar is. De *hack in contest* zet in op verandering in gedrag door behoeften (uitdaging, competitie, creativiteit) te kanaliseren in legale alternatieven en tegelijk de strafdreiging van het illegaal hacken te verhogen. Daarmee wordt de kosten-baten verhouding van het illegaal-hacken negatief bijgesteld. Ook de interventie van *reintgrative shaming* zet in op deze kosten-baten structuur maar dan via afname van de sociale beloning uit de subcultuur voor het gedrag. De *warning banners* zijn een methode om de doelgroep met afschrikkende boodschappen te bereiken op het moment dat ze bezig zijn met het illegale gedrag.

*Effectiviteit*

Er is één effectstudie beschikbaar en drie inhoudelijke evaluaties (zie tabel 4.9). De effectstudie naar waarschuwingsbanners vergelijkt een experimentele groep die tijdens een hackpoging een waarschuwingsbanner te zien krijgt met informatie over de strafbaarheid van de handeling en de bijbehorende pakkans, met een controle groep die deze boodschap niet kreeg. De banners bleken er niet voor te zorgen dat hacken voorkomen wordt of dat de hackers niet nog een keer bij het systeem inbreken. Wel werd gezorgd dat ze minder lang in het systeem rondneuzen (Maimon, Alper, Sobesto, Cukier, 2014). Dit onderzoek laat zien dat er niet zondermeer van een effect van afschrikking uitgegaan kan worden. Deze studie is overigens gericht op de algemene hackerpopulatie en niet specifiek op jeugdigen.

In een inhoudelijke analyse wordt de interventie *duty-to-report* afgezet tegen een *hack-in-contest.* Conclusie is dat de hack in *contest* waarschijnlijk beter zal werken dan *duty-to-report* omdat het inzet op positieve bekrachtiging en het herstellen van de relatie tussen handhavings- en beveiligingsprofessionals en (een deel van de) hackers. Hierdoor worden de minder schadelijke vormen van hacken uitgefilterd en kan de handhaving zijn middelen inzetten op het meer destructieve hacken. Daarbij kunnen de deelnemers aan de *contests* bovendien een bijdrage leveren.

De inhoudelijke evaluatie van interventies gericht op *reintegrative shaming* neemt als startpunt het effect van een traditionele strafrechtelijke aanpak (Kao, Fu-Yang Huang en Wang, 2009). Uit informatie van 9 jeugdige hackers (o.a. uit *face-to-face* interviews) werd duidelijk dat deze jongens niet geloofden dat ze iets fout hadden gedaan en dat ze zich aan de hackers ethiek hadden gehouden. De strafrechtelijke aanpak blijkt uit te lopen op het door Braithwaite (1989) als niet effectief beschreven '*shaming*'. Na het strafrechtelijk vervolgen van deze jongeren vervielen zij weer in het strafbare gedrag. De strafrechtelijke vervolging zou hen juist verder van de maatschappij hebben afgezet en meer in de hackersubcultuur hebben geplaatst. Het alternatief van *re-integrative shaming* zou zoals beschreven juist gebruik maken van de specifieke subcultuur waarin deze jongeren zich bevinden. Daarbij wordt geprobeerd het contrast dat er bestaat tussen de normen in deze cultuur en in de samenleving daarbuiten te verkleinen. Daarom wordt verwacht dat deze interventie mogelijk effectief is. Dat de invloed

vanuit de hackersubcultuur mogelijk belangrijk is bij het voorlichten van jeugdigen werd eerder al onderstreept door het falen van een andere methoden namelijk het gebruik van de waarschuwingsberichten (Maimon, et al., 2014). Deze bevinding sluit ook aan bij de conclusies uit de what works traditie over effectieve interventies. Daar bleek dat interventies die alleen uit zijn op straffen of afschrikking en waarin geen aandacht is voor de aanpak van de criminogene factoren die direct samenhangen met het deviante gedrag (Lipsey & Cullen, 2007).

Tabel 4.9 Designs van de evaluatiestudies naar interventies tegen hacking

| Experimenteel design | Quasi-experimenteel design | Voor/nameting zonder controle groep/ posttest gecontroleerd | Nameting zonder controle groep | Inhoudelijke evaluatie |
|---|---|---|---|---|
| Warning banners | | | | Duty to Report |
| | | | | Hack-in-contest |
| | | | | Re-integrative Shaming |

*Programma integriteit*

Voor de meeste interventies wordt niet duidelijk in welke mate er sprake is van programma-integriteit. Dat heeft uiteraard ook te maken met het feit dat het veelal nog interventies in ontwikkeling zijn. Een belangrijke tekortkoming bij de uitvoering van de hack in contests is volgens de auteur dat er onvoldoende werk gemaakt wordt van het criminaliseren (strafbaar stellen en daar ook op handhaven) van al het hacking gedrag buiten de contests om. De overheid moet hiertoe volgens de auteur van de inhoudelijke evaluatie duidelijkere signalen geven (Wible, 2003).

## 4.5 Technische interventies: filters en gebruik van open source software

Net als algemene technische interventies voor de bescherming van slachtoffers (zoals virussoftware), waarover we in de introductie van dit hoofdstuk spraken, zijn internetfilters en open source software breed inzetbare technische interventies. Internetfilters en open source software kunnen echter ook ingezet worden om het gedrag van specifieke daders te beïnvloeden.

Tabel 4.10 Korte beschrijving van de technische interventies

| |
|---|
| CyberPatrol is een filter gericht op het probleem van internetmisbruik. De filter blokkeerd de toegang tot internetpagina's volgens van te voren ingestelde waarden om schadelijk gedrag tegen te gaan. Daarbij wordt er een logboek bijgehouden waardoor gedrag gemonitord kan worden. (Chou, Sinha, Zhao, 2010) |
| CyberSitters is een filter gericht op het probleem van internetmisbruik. De filter blokkeerd de toegang tot internetpagina's volgens van te voren ingestelde waarden om schadelijk gedrag tegen te gaan. Daarbij wordt er een logboek bijgehouden waardoor gedrag gemonitord kan worden. (Chou, Sinha, Zhao, 2010) |
| NetNanny is een filter gericht op het probleem van internetmisbruik. De filters blokkeren de toegang tot internetpagina's volgens van te voren ingestelde waarden om schadelijk gedrag tegen te gaan. NetNanny heeft ook een logboek functie maar die is minder uitgebreid dan die van de hiervoor beschreven programma's (Chou, Sinha, Zhao, 2010) |
| Het idee achter virtual neighbourhood watch is dat ieder individu dat in verbinding staat met internet lid is van de gemeenschap. Zij kunnen samenwerken met de rechtshandhaving om problemen te identificeren en methoden ontwikkelen om risico's te beperken, door gebruik van *open source* software waardoor elke gebruiker aanpassingen kan maken in de onderliggende broncode kwetsbaarheden aan te pakken. (Jones, 2007) |

*Programmadoelen en methoden filters*

De filters blokkeren de toegang tot internetpagina's volgens van te voren ingestelde waarden. Daarbij kan het gaan om pagina's die schadelijk gedrag mogelijk maken zoals illegaal downloaden of een mogelijk schadelijke inhoud hebben zoals pornografie. Naast het blokkeren van internetsites houden sommige internetfilters (o.a. CyberSitter en CyberPatrol) ook een logboek bij dat het mogelijk maakt de potentiële dader te monitoren en dus misbruik te constateren (Chou, Sinha, Zhao, 2010). De filters zouden volgens diverse auteurs goed ingezet kunnen worden door ouders of leerkrachten tegen bijvoorbeeld cyberagressie of sexting door jongeren (o.a. Cohan & Algmor, 2010; Paravecchia 2011-2012).

*Effectiviteit filters*

Hoewel we geen evaluatiestudies hebben gevonden over de effecten van filters op jeugdige plegers, is de algemene effectiviteit van dergelijke filters aan de hand van simulatiestudies getest. Internetfilters waarvoor we dergelijke evaluaties hebben gevonden zijn: CyperPatrol, CyberSitter en NetNanny (Chou, Sinha, Zhao, 2010). Uit een evaluatiestudie blijkt dat de filters niet goed werken (Chou, Sinha, Zhao, 2010; zie tabel 5, in bijlage 3). Er wordt geconstateerd dat CyberPatrol, CyberSitter en NetNanny slecht presteren op zowel het onterecht niet blokkeren van een pagina (onderblokkering) als het onterecht wel blokkeren (overblokkering). Naast het adequaat toegang verlenen tot websites is bij CyberPatrol en CyberSitter een specifieke filtertechniek geëvalueerd, namelijk de *text mining* techniek (NetNanny bezit deze techniek niet). In vergelijking met een controle groep van *text mining* technieken presteerde CyberPatrol en CyberSitter significant slechter (Chou, Sinha, Zhao, 2010).

*Programmadoelen en methoden open source software*

Naast het kijken naar technologieën om cybercrime of (potentiële) daders buiten te houden, moet er ook naar de mensen gekeken worden achter de technologische beveiliging, waar menselijk gedrag cybersecurity aantast. Hackers maken bijvoorbeeld vaak gebruik van *social*

*engineering*[17] om een anders gesloten netwerk binnen te komen. Dit betekent dat er bij cybersecurity ook naar de menselijke factor gekeken moet worden (Waldrop, 2016; Árpád, 2013). Het is dan ook interessant te zien dat Jones (2007) en Brown (2003) beide een vorm van *virtual neighbourhood watch* voorstellen met gebruik van open source software. Het idee achter deze *virtuele neighbourhood watch* is dat ieder individu dat in verbinding staat met internet, elk systeem dat is aangesloten, elke eigenaar en systeembeheerder, lid is van de gemeenschap. Al deze potentiële slachtoffers kunnen samenwerken met de rechtshandhaving om problemen te identificeren en methoden ontwikkelen om risico's te beperken. Door gebruik van *open source* software kan elke gebruiker toegang verkrijgen tot de onderliggende broncode en daarin aanpassingen maken om kwetsbaarheden voor cybercrime in te software in te perken (Jones, 2007; Brown, 2003). Deze interventie is een voorbeeld waarin technische en menselijke factoren die een rol spelen in cybercrime worden gecombineerd.

*Verwachte effectiviteit open source software*

De evaluatie voor deze interventie betreft een inhoudelijke evaluatie, waarbij gekeken wordt of de interventie theoretisch gezien zou kunnen werken (Jones, 2007). De conclusie is dat het instrument geschikt zou kunnen zijn voor de aanpak van cybercrime vanwege de proactieve vorm van misdaadbestrijding waarin het delen van informatie wordt aangemoedigd en gebruikers bij het vinden van beveiligingsfouten direct kunnen bijdragen aan de oplossing. Dit past bij de snelheid en de afwezige noodzaak van nabijheid die cybercrime karakteriseert (Jones, 2007). Deze interventie zou bovendien effectief zijn omdat de actieve rol van de gemeenschap een sterkere bekrachtiging van normen over online veiligheid oplevert dan top-down beveiligingsmaatregelen doen (Jones, 2007).

## 4.6 Conclusie

Uit onze systematische internationale literatuurstudie komen geen geëvalueerde interventies naar voren die zich specifiek richten op jeugdige daders van cybercrime *(onderzoeksvraag 1)*. De enige studies waarin specifiek wordt ingegaan op interventies voor jeugdige daders betreffen theoretische uiteenzettingen (*Re-intergratieve Shaming* voor jeugdige hackers en *Restorative justice* bij stalking en dus cyberagressie). Beide zijn echter geen vast omschreven interventies maar meer algemene benaderingen die in plaats van of naast het strafrecht zouden moeten functioneren. (Halder, 2015; Kao, et al., 2009)[18].

Alle andere interventies die uit de literatuurstudie naar voren kwamen, opereren in de preventieve sfeer. In de literatuurstudie werden totaal 75 interventies genoemd, waarvan er voor 39 interventies evaluatiestudies beschikbaar zijn. Deze interventies richten zich op de volgende typen cybercrime: 'cyberagressie', 'sexting', en 'hacking'[19] *(onderzoeksvraag 2a)*

[17] Dit houdt in dat gebruik gemaakt wordt van het gedrag van personen die deel uit maken van een systeem om dat systeem binnen te komen (Mouton, Leenen, & Venter, 2016). Daarbij worden verschillende manipulerende technieken gebruikt (autoriteit, verleiding, vriendschap) om informatie los te krijgen of direct toegang te krijgen tot systemen. Phishing is een bekende vorm van social engineering.

[18] Voor geen van deze 'interventies' is een effectstudie gevonden.

[19] De categorieën interventies in dit hoofdstuk onder de kopjes 'online veiligheid' en 'technische interventies' richten zich ook grotendeels op deze drie delict groepen.

daarnaast zijn er algemene interventies gericht op online veilig gedrag waarin ook aandacht is voor het voorkomen van daderschap.

De interventies richten zich vrijwel allemaal op algemene populaties jongeren of in het geval van hacken algemene populaties van hackers *(onderzoeksvraag 2b)*. Veruit de meeste interventies richten zich op daders, slachtoffers en omstanders.

Bij de meeste interventies wordt er gebruik gemaakt van theorieën over sociaal leren, actief leren en de sociaal ecologische aanpak *(onderzoeksvraag 2c).* Al worden deze theorieën slechts bij enkele interventies specifiek genoemd. Bij hacking interventies zijn vooral subculturele theorieën en neutralisatietechnieken van belang.

De gebruikte methoden richten zich veruit bij de meeste interventies op de bewustwording van de online risico's (sexting, online veiligheid, cyberagressie) bij daders, slachtoffers, en omstanders *(onderzoeksvraag 2d)*. Al ligt de focus zoals gezegd veel meer op de bewustwording van en omgang met de risico's op slachtofferschap (door voorlichting en sociaal leren) en veel minder op het tegengaan van daderschap. Opvallend is dat de meeste interventies op deze gebieden zich inhoudelijk vooral focussen op de risico's voor slachtofferschap en veel minder op het tegengaan van daderschap. Dat de focus van de meeste interventies voor de gehele populatie jongeren vooral ligt op het voorkomen van slachtofferschap betekent echter niet dat deze interventies niet waardevol zijn in het voorkomen cybercrimedaderschap onder jeugdigen. Zo kan het beperken van de toegang tot of beschikbaarheid van criminele doelen door gedrag van de potentiële slachtoffers te veranderen, gezien worden als een belangrijke strategie om cybercrime te voorkomen.

Uit de evaluaties komt maar zeer beperkt informatie naar voren over de programma-integriteit bij de interventies *(onderzoeksvraag 3)*. Wat wel duidelijk wordt is dat er vooral sprake is van voorlichting en sociaal leren (aan de hand van interactief materiaal) en veel minder van 'actief leren' (rolspellen). Uit wetenschappelijk onderzoek komt juist naar voren dat 'actief leren', het daadwerkelijk aanleren van vaardigheden, effectiever is dan alleen voorlichting (Jones, Mitchel & Walsch, 2014a).

Voor de meerderheid van de online veiligheid en cyberagressie programma's zijn effectstudies gevonden *(onderzoeksvraag 4)*. Voor cyberagressie ging dit veelal om een (quasi)-experimenteel design waarmee met enige zekerheid uitspraken over effectiviteit gedaan kunnen worden. Alle interventies naar cyberagressie bleken effectief waarbij het directe effect op daderschap vaak kleiner was dan op slachtofferschap. De interventie die vooral effecten op daderschap vond (VISc, Gradinger, et al, 2016) had programmadoelen die veel meer dan de andere interventies exclusief zijn gericht op het terugdringen van agressief gedrag en pesten.

Voor de online veiligheid interventies was het evaluatiedesign meestal zwakker (vaak geen controlegroep). Van de online veiligheid interventies werden bovendien geen effecten op feitelijk gedrag gevonden en slechts één studie vond een effect op bewustwording over daderschap (een intermediaire uitkomst). Bij sexting en hacking is voor ieder slechts één effectstudie gevonden.

Gegeven de beperkte informatie over dadergerichte interventies die uit deze literatuurstudie naar voren komt, kunnen geen uitspraken gedaan worden die een antwoord geven op *onderzoeksvraag 5* naar de wijze waarop effectieve en veelbelovende interventies zich onderscheiden van de niet-effectieve interventies. Dit geldt ook voor de uitkomsten uit de

preventieve interventies die gericht zijn op algemene populaties, deze zijn te gefragmenteerd en te weinig gericht op de terugdringing van daderschap om uitspraken te kunnen doen over effectiviteit voor het inperken van daderschap van cybercrime. Het is daarom van belang verder te zoeken in de literatuur en in de praktijk naar handvaten voor het ontwikkelen van dadergerichte interventies. De uitkomsten hiervan zullen in hoofdstuk vijf beschreven worden.

# 5. Verdiepingsstudie naar aangrijpingspunten voor interventies

Uit de literatuurstudie in hoofdstuk 4 komt naar voren dat er geen concrete evaluaties zijn uitgevoerd van interventies voor jeugdige daders van cybercrime. Om meer inzicht te krijgen in typen interventies die mogelijk effectief kunnen zijn, hebben we daarom een verdiepende literatuurstudie en expertbijeenkomsten uitgevoerd. De doelen van deze verdiepende studie zijn:

1) In kaart brengen welke typen interventies kansrijk zijn gezien de problematiek die er is;
2) Beschrijven wat er feitelijk in de praktijk gebeurt met jeugdige cyberdaders om de kans op recidive en het ontwikkelen van carrières in de cybercrime te beperken; en
3) Na te gaan welke lessen er uit deze praktijk kunnen worden getrokken.

Deze verdieping heeft een exploratief karakter en zal zich om voldoende focus te kunnen aanbrengen, richten op een selectie van typen delicten. Om een relevante keuze te kunnen maken uit verschillende vormen van criminaliteit hebben we rekening gehouden met de volgende factoren:

- Prevalentie van cyberdelict typen
- Carrière ontwikkelingen van jeugdige plegers van de cyberdelict typen
- De gevolgen van de cyberdelict typen

Voordat we verder ingaan op de selectie van factoren moet opgemerkt worden dat in veel recent onderzoek betreffende jeugdige cybercrimeplegers lang niet alleen strafbare cyberdelicten worden meegenomen maar ook diverse vormen van antisociale gedragingen. Bij Kerstens en Stol (2012), Van der Broek et al. (2013) en Zebel et al. (2013) worden onder daderschap van cybercrime zowel normafwijkende als strafbare gedragingen gevat. Van der Laan en Goudriaan (2016) nemen in de 'Monitor Jeugdcriminaliteit' alleen strafbare gedragingen mee. In onze verdiepende studie is ook aandacht voor antisociale gedragingen die (nog) niet strafbaar zijn maar wel schade opleveren, maar de focus zal liggen op de meer ernstige strafbare gedragingen.

## 5.1 Verantwoording selectie cyberdelicten[20]

*Prevalentie*

Over de prevalentie van cybercrime in Nederland kan nog niet veel gezegd worden. Er is een beperkte registratie van cybercrime in politie- en justitiestatistieken (Van der Laan & Goudriaan, 2016) en slechts enkele zelfrapportagestudies (Kerstens & Stol, 2012, Van der Broek et al., 2013, Zebel et al., 2013 en Van der Laan & Goudriaan, 2016). Uit het beschikbare onderzoek komt naar voren dat (in willekeurige volgorde): sexting, cyberpesten, financieel-economische online delicten en hacken de cyberdelicten zijn die (voor zover dat gemeten is) het meest voorkomen onder jongeren in Nederland (Kerstens en Stol, 2012; Van der Broek et al., 2013; Zebel et al., 2013; Van der Laan & Goudriaan, 2016). De percentages jongeren die plegen, variëren van minder dan 1% (virus verspreiden) tot 24% (cyberpesten).

De vergelijking met andere leeftijdsgroepen is alleen te maken op basis van registratiegegevens. Hieruit blijkt dat van alle afgedane cyberdelicten in de periode 2006-2011

[20] Hieronder is een beknopte beschrijving van de overwegingen weergegeven. In bijlage 4 is een uitgebreide weergave te vinden van de gevonden informatie over deze factoren.

ongeveer 10% (272 van de 2883 delicten) gepleegd is door een jeugdige dader (18 jaar of jonger). Van deze afgedane cyberdelicten betrof 53% kinderpornografie, 28% hacken, en 9% vernieling van digitale gegevens (Zebel et al, 2013, blz 60-61, tabel 5). Het is mogelijk dat er sprake is van een leeftijdsbias in deze registratiegegevens omdat delicten met jeugdigen mogelijk vaak anders worden afgehandeld. Bovendien betreft dit relatief oude cijfers maar recentere cijfers met een dergelijke uitsplitsing hebben we niet gevonden.

*Carrière ontwikkeling*

Naast prevalentie wordt ook het potentieel belang van interventies voor de toekomst van de pleger meegenomen in de overweging. Kortom het verloop van de criminele carrières en de negatieve consequenties voor de normale maatschappelijke carrière (opleiding, werk, relaties, etc.) zijn van belang. Uit het beperkte beschikbare empirisch materiaal blijkt dat cyberagressie een interessante groep delicten vormt voor nadere analyse vanwege het sterke verband met offline gedrag. Jeugdigen die online agressie plegen, vertonen ook in grote mate offline antisociaal gedrag (Van der Broek et al, 2013).

Hacken is bij uitstek een delict type waarin jeugdigen zich kunnen specialiseren en een carrière opbouwen, waarbij hacken zowel een doel op zich als een middel kan zijn om andere delicten te plegen (Leukfeldt, et al., 2010; Van der Wagen, Althoff & Van Swaaningen, 2016). Vooral de combinatie van 'toekomstperspectieven' in de legaliteit en de illegaliteit is bij hacken interessant. Zo bestaat het risico dat jeugdige hackers ingezet worden voor illegale praktijken van criminelen. Het komt echter ook voor dat jeugdige hackers juist, vanwege de door het hacken opgedane vaardigheden, kansen krijgen in reguliere banen (Van der Wagen, Althoff & Van Swaaningen, 2016)[19].

*De gevolgen*

Wanneer de mogelijke schade beschouwd wordt, komen: sexting, cyberagressie en hacken als relevante delicten naar voren. Sexting kan ernstige gevolgen hebben wanneer het door derden wordt ingezet als middel voor smaad, laster, cyberpesten, afpersing of bedreiging, (Kerstens & Stol, 2012; Zebel et al, 2013; Döring, 2014; DeMitchell & Parker-Magana, 2011). Cyberpesten(agressie) heeft een duidelijk verband met een verminderd psychosociaal welzijn van de slachtoffers (Albin, 2012; Dredge, Gleeson & De Piedad Gracia, 2014). Waarbij daders en slachtoffers van cyberagressie beide een groter risico lopen om criminele handelingen te verrichten (Albin, 2012). De schade van hacken kan groot zijn doordat het de deur open zet tot andere cyberdelicten, waaronder financieel economische cyberdelicten (Leukfeldt, et al, 2010; Van der Wagen, Althoff & Van Swaaningen, 2016).

Al deze factoren meegenomen, is er besloten om de cyberdelicten: cyberagressie en hacken te selecteren voor een verdiepende studie. Sexting zal niet expliciet meegenomen worden, maar zal door de relatie met cyberagressie indirect besproken worden[19].

## 5.2 Aangrijpingspunten voor interventies tegen cyberagressie

Cyberagressie wordt beschreven als een spectrum aan agressieve online gedragingen waarvan de mate van strafbaarheid varieert (France, Danesh & Jirard, 2013; Holt, Bossler & May, 2011; Aboujaoude, Savage, sarcevic, Wael & Salame, 2015; Chrisholm, 2014). Een groot deel van de cyberagressieliteratuur richt zich op cyberpesten. Daarbinnen wordt een grote variëteit aan agressieve gedragingen geschaard. Gedrag wordt als (cyber)pesten gezien als het gaat om het herhaaldelijk en bewust kwaad doen van de ontvanger gedurende een langere periode waarbij er sprake is van een werkelijke of beleefde ongelijke machtsverhouding tussen de dader en het slachtoffer (Olweus, 2010). Vormen van cyberpesten zijn roddelen, schelden, bedreigen, toesturen of online plaatsen van kwetsend beeldmateriaal, buitensluiten, beledigen, smaad, en laster (Kerstens & Stol, 2012; Noonan, 2009). Dezelfde handelingen worden als ze eenmalig voorkomen in een bepaalde relatie niet als cyberpesten maar wel als cyberagressie gezien (France, et al., 2013; Mitchell et al., 2014)[21]. Vormen van cyberagressie kunnen strafbaar worden gesteld[22]. De politie heeft geen eenduidige cijfers omtrent cyberagressie. Dit komt onder andere doordat nog vaak onduidelijk is wanneer en in welke mate cyberagressie strafrechtelijk vervolgd kan worden. Zo zijn er geen wetsartikelen specifiek voor cyberpesten of cyberagressie, maar moet er een beroep gedaan worden op algemene wetsartikelen afhankelijk van wat er precies op het internet gebeurt[12] (Kerstens & Stol, 2012; $R1_a$ politiefunctionaris). In het gesprek met de experts blijkt dan ook dat er nog weinig duidelijkheid is over waar de grens moet liggen tussen strafbaar en niet strafbaar gedrag (R1, R4 & R5, onderzoekers; Baas, De Jong & Drossaert, 2013).

> **"**Het begint natuurlijk veel kleiner, bij het softe wat pesten toch nog steeds wel heeft. Dat gaat op een gegeven moment alleen wel echt richting heel heftig. Het is natuurlijk een spectrum, […] een spectrum waarvan je zegt: is het dan strafbaar of niet? Wat heb je gedaan?...**"**
>
> R4 Onderzoeker

Het is daarom belangrijk dat er een goede samenwerking tussen scholen en politie bestaat op dit terrein. Ondanks het bestaan van landelijk beleid voor het samenwerken van scholen en politie is de problematiek nog niet goed zichtbaar en wordt de politie pas ingeschakeld wanneer het fout gaat. Recent zijn er aanpassingen in het beleid gedaan gericht op betere afspraken over preventie, repressie, signaleren en adviseren in cyberagressie zaken ($R1_a$ praktijkexpert;

---

[21] Andere termen die in de literatuur veel naar voren komen zijn cyberstalking en cyberharassment waarbij harassment soms als synoniem voor pesten wordt gezien maar door anderen ook als benaming voor eenmalig agressief gedrag (Mitchell et al., 2014). Overigens richten de studies die naar determinanten van cyberagressie kijken zich vrijwel allemaal op herhaalde cyberagressie en daarmee dus op cyberpesten.

[22] *Cyberagressie* (Kerstens & Stol, 2012; $R1_a$ politiefunctionaris)*:*

- Identiteitsfraude art 231b Sr
- Belediging art 266 en 271 Sr
- Smaad art 261 Sr
- Laster art 262 Sr
- Stalking art 285b Sr
- Bedreiging art 285 Sr
- Discriminatie art 137c en 137e Sr

beleidsdocument 'politie en schoolveiligheid visie en ambitie). Het is nog onduidelijk welke effecten die afspraken hebben.

### 5.2.1 Samenhang en verschillen met offline agressie

Veel plegers van cyberagressie blijken ook offline agressieve delicten te plegen (Van der Broek, et al. 2013). Er is echter ook een groep online-plegers die offline geen agressieve delicten vertonen (o.a. Rokven, Weijters & Van der Laan, 2017). Voor de verklaring van het gedrag van deze laatste groep plegers speelt het online *disinhibitie-effect* een rol (Kokinos, Antoniadou, Asdre & Voulgaridou, 2016; Suler, 2004). Mensen durven meer te zeggen en doen wanneer zij online zijn door de beperktere (in)formele controle, beperkter bewustzijn van strafbaarheid en het lage slachtofferbewustzijn (Suler, 2004; R1, R4 & R5 onderzoekers). Wanneer deze factoren gecombineerd worden zien we dat mensen op internet relatief gemakkelijk kunnen overgaan tot het vertonen van antisociaal en deviant gedrag dat zij in '*real life*' niet zouden vertonen (Suler, 2004; R1, R4 & R5 onderzoekers). De grootste veroorzaker voor disinhibitie is de anonimiteit die individuen hebben op internet. Dit geeft mensen de kans om hun handelen online te scheiden van hun leven offline, ze hoeven hun handelen niet te verantwoorden. Dit gecombineerd met onzichtbaarheid en asynchroniteit[23] zorgt er voor dat mensen meer durven zeggen en doen op het internet dan dat ze zouden durven in een *face-to-face* situatie (Suler, 2004). Het cyberelement zorgt er dus voor dat mensen gemakkelijker agressie vertonen en dat niet alle daders zich bewust zijn van hun acties. Dit komt ook naar voren in het onderstaande citaat.

> **"**In discussies op internet zie je juist het tegenovergestelde. Ik denk dat mensen soms een beetje het zicht verliezen dat er mensen aan de andere kant zitten. En dat moet je van jongs af aan al leren. Dat is nou juist die leeftijd waar dat ook nog kan.**"**
>
> R5 Onderzoeker

Naast een gebrek aan remmingen zorgt de online omgeving er ook voor dat de basis voor de machtsverschillen tussen daders en slachtoffer anders is. Waar bij traditionele agressie fysieke verschillen een grote rol spelen is dat nu de toegang tot en vaardigheden voor digitale technologie (Chisholm, et al., 2014).

### 5.2.2 Achtergronden van jeugdige plegers van cyberagressie

Uit de literatuur komt naar voren dat de kenmerken van plegers van cyberagressie voor een groot deel overeenkomen met kenmerken van plegers van offline agressie (Aboujaoude, et al. 2015; Mitchell, Ybarra & Finkelhor, 2007; Kokkinos et al., 2016). Zo is er bij beide typen

[23] Doordat er na een online actie vaak geen directe reactie komt en plegers ook zelf kunnen beslissen wanneer zij een reactie zien en erop reageren, blijft de directe feedback cirkel die gebruikelijk is bij offline interactie uit. Wanneer deze directe feedback wel bestaat en plegers dus moeten omgaan met de onmiddelijke reactie van het slachtoffer, komen plegers vaker tot inkeer en wordt normconform gedrag bekrachtigd (Suler, 2004).

agressieplegers vaker sprake van een minder gunstig opvoedingsklimaat (Hemphill & Heerde, 2014), slechtere relaties met de ouders (Kiriakidis & Kavoura, 2010; Mitchell, et al., 2007), middelenmisbruik, delinquente vrienden (Mitchell, et al., 2007), beperktere impulscontrole (Kokkinos, et al. 2016), gedragsproblemen, een negatieve stemming (Aboujade, et al. 2015) en minder afwijzende attitudes ten opzichte van pesten (Pabian & VandeBosch, 2014). Offline en online agressief gedrag komt daarom zoals hierboven beschreven dus ook vaak in combinatie bij dezelfde jongeren voor (o.a. Kersten & Stol, 2012; Hemphill & Heerde, 2014). Uit recent onderzoek weten we dat er bij jeugdige daders naast overeenkomsten ook verschillen zijn in daderprofielen van offline- en onlinedaders. Zo weten we dat online daders minder vaak drugs gebruiken en een hogere mate van zelfcontrole hebben dan offline daders maar dat zij wel vaker dan niet daders slachtoffer zijn van offline delicten (Rokven, Weijters & Van der Laan, 2017).

Er zijn ook verschillen aangewezen in de literatuur, zo hebben cyberpesters een hogere sociale intelligentie dan jongeren die (alleen) offline pesten (Pabian & VandeBosch, 2014) en hebben zij meer internetvaardigheden (Vandebosch & Van Cleemput, 2009). Plegers van cyberpesten hebben bovendien lagere niveaus van algemene agressie dan traditionele pesters (Kubiszewski et al., 2014). Het pester-slachtoffer fenomeen blijkt juist weer gemakkelijker online te ontstaan dan offline (Aboujade, et al. 2015). Voor cyberstalking wordt gevonden dat het vooral om oudere vaak goed opgeleide adolescenten met een internetverslaving gaat (Chisholm, 2014).

### 5.2.3 Interventies

Uit bovenstaande beschrijving blijkt dat de criminogene problematiek bij plegers van cyberagressie voor een belangrijk deel overeenkomt met de problematiek van plegers van offline agressie. Het frequente voorkomen van gecombineerde offline/online plegers sluit aan bij die constatering. Bestaande gedrag beïnvloedende interventies zoals een agressie regulatietraining (ART), cognitieve vaardighedentraining (COVA), of behandeling van verslavingsproblematiek (leefstijltraining), zouden volgens de experts en de wetenschappelijke literatuur dan ook mogelijk effectief kunnen zijn bij cyberagressie (R6, 9, 10 praktijkexperts; Jäger, Amado, Matos & Pesoa, 2010; Camerman, 2013; France, Danesh & Jirard, 2013). Al moet daarbij wel rekening gehouden worden met het cyberelement.

> **"**Het gaat om het onderliggende gedrag, ik denk dat dat niet wezenlijk anders is als je het hebt over de cyber of het reguliere werk. Ik denk wel dat het cyber aspect veel meer meegenomen moet worden. Om zo meer zicht te krijgen op de leefwereld van mensen.**"**
>
> R6 Praktijkexpert

Wat betreft dat cyberelement opperden verschillende praktijkexperts in de discussiegroep om de mogelijkheden van *serious gaming* of *virtual reality* te onderzoeken bij het vertalen van de online situatie naar de offline werkelijkheid.

> **"**Dat je iemand, door middel van *virtual reality* cyberagressie laat ervaren. Gewoon de dader in de huid van het slachtoffer steekt door middel van *virtual reality*...**"**
>
> R10 Praktijkexpert

*Virtual reality* en *serious gaming* is een domein dat verschillende toepassingen kent, volop in ontwikkeling is, en waar veel onderzoek naar gedaan wordt. Zo wordt er nu onderzocht in hoeverre het gebruikt kan worden om persoonlijke vaardigheden, sociale vaardigheden, moreel redeneren en sociaal bewustzijn aan te leren (Pereira, Brisson, Prada, Paiva, Bellotti, Kravick, & Klamma, 2012). Onderzoek richt zich onder andere op de toepasbaarheid voor pedagogische interventies, waarbij er ook gekeken wordt naar toepassingen in het domein cyberpesten (o.a. De Troyer, van BroeckHoven & Vlieghe, 2017). Recent is bijvoorbeeld een *serious game* ontwikkeld om op te treden tegen cyberpesten door het *bystander effect* te verminderen. Een van de doelen van deze *serieous game* is om jongeren te leren inzien wanneer een bericht bedoeld is om een ander pijn te doen en om jongeren te weerhouden om de pesters te bekrachtigen (De Smet et al, 2016). Het is een *serious game* waarvan de effectiviteit onderzocht is en die positieve resultaten oplevert (De Smet, et al., 2016)[24].Naast deze specifieke dader- en omstandergerichte interventies wordt het bewustmaken van de algemene populatie jongeren ook als een belangrijke strategie gezien door de experts. Dit kan aan de hand van voorlichtings- en educatieve programma's die zich focussen op internet etiquette. Daarbij zou echter meer aandacht moeten zijn voor mogelijk daderschap (zie 4.2 online veiligheid; R1, R4 & R5 onderzoekers). Er bestaan diverse anti-agressie programma's die ook geschikt zijn of kunnen worden gemaakt voor online agressie. Daarbij moet rekening gehouden worden met het cyberelement dat ervoor zorgt dat mensen gemakkelijker agressie vertonen en dat niet alle daders zich bewust zijn van hun acties (disinhibitie). Jeugdigen zouden op een jonge leeftijd al moeten leren dat ook een ontvanger die je niet kunt zien, er wel degelijk is. Daarnaast is het van belang jongeren te leren dat doordat toon, intonatie en gezichtsuitdrukking over het algemeen afwezig zijn bij online gesprekken, een bericht anders of harder aan kan komen dan het oorspronkelijk bedoeld was (R1, R4 & R5 onderzoekers; Albin, 2012; Suler, 2004).

Een andere kanttekening bij het gebruik van bestaande programma's is dat de belevingswereld van de jongeren kan verschillen met die van de leraren. Zo kan het zijn dat de leraar juist door het cyberelement geen goed zicht heeft op het pesten of op wie de pesters zijn (Baas, 2010; Baas, De Jong & Drossaert, 2013).

> **"**In Groningen loopt een onderzoek over pesten. Twee weken geleden of zo kwam daar een bericht van, ook in het nieuws, dat leraren geen of heel slecht zicht hebben op wie nou daadwerkelijk de daders zijn, of wie de pesters zijn. Dus het is de vraag in hoeverre scholen ook echt iets kunnen, tenzij daar iets aan gedaan kan worden**"**
>
> R4 Onderzoeker

[24] Omdat het hier om een interventie gaat die uitsluitend gericht is op de omstanders hebben wij deze interventie niet opgenomen in het overzicht van geëvalueerde interventies in hoofdstuk 4.

Uit onderzoek over mogelijk interventies voor cyberpesten waarin specifiek gekeken wordt naar de mening van de jongeren zelf, komt naar voren dat jongeren stellen dat leraren en ouders vaak te weinig afweten van technologie of de ernst van cyberpesten. Om cyberpesten op een effectieve manier aan te pakken wordt er hier dan ook aangeraden om de kennis over technologie, de bestaande vormen van cyberpesten en wat zij er aan kunnen doen te vergroten bij ouders en leraren (o.a. Baas, 2010; Juvonen & Gross, 2008; Baas, De Jong & Drossaert, 2013). Een mening die gedeeld wordt in de discussiebijeenkomst (onderzoekers R1, R4 & R5).

Behalve door algemene voorlichting kunnen jeugdigen ook door een directe reactie op antisociale online gedragingen gewaarschuwd worden dat hun gedrag mogelijk kwetsend of strafbaar is. Om escaleren te voorkomen zou snel op de gedragingen gereageerd moeten worden. Volgens onderzoekers R1, R5, R4 en praktijkexperts $R1_a$ kan hierbij een rol gespeeld worden door een digitale agent. Deze agent kan niet alleen waarschuwen maar ook het gesprek daadwerkelijk aan gaan en een vertrouwensband opbouwen. Hij hoeft hiervoor geen *wizkid* te zijn ($R1_a$ praktijkexpert). Ook online zou men de jongeren aan kunnen spreken. Een *tool* die hiervoor gebruikt zou kunnen worden, is het instrument *digigeren* (Broekman, Wetzer, Wijn & Roelofs, 2014). Dit is een instrument dat momenteel ontwikkeld wordt om geautomatiseerd te reageren op antisociaal gedrag. Digigeren maakt gebruik van sociale psychologie om gedrag te beïnvloeden, te informeren, of de informatiepositie te verbeteren. Of dit een effectieve methode is wordt momenteel onderzocht (Broekman, Wetzer, Wijn, & Roelofs, 2014). Bij deze offline en online gesprekken is het belangrijk in het oog te houden dat dader- en slachtofferrollen vaak wisselen en traditionele- en cyberagressie in afwisseling bij de zelfde actoren voorkomen ($R1_a$ praktijkexpert; Kerstens & Stol, 2012). De inhoud, vorm, en afzender van een waarschuwingsbericht moeten bovendien afgestemd zijn op de motivatie en achtergrond van de pleger (R3 onderzoeker & R2, R6, R13 praktijkexperts; Broekman, Wetzer, Wijn & Roelofs, 2014).

Wat tot slot benadrukt wordt in de discussiebijeenkomst is dat dit fenomeen niet alleen een jongeren probleem is. Daarbij worden voorbeelden genoemd van zeer agressieve reacties door volwassenen waaronder online belaging van publieke figuren (onderzoekers R1, R4 en R5). Dergelijke rolmodellen zijn schadelijk voor het gedrag van de kinderen. Om cyberagressie aan te pakken moet dus niet alleen gefocust worden op het jeugdprobleem. Er zou een vorm van online *community* gecreëerd moeten worden waar door informele en formele controle alle mensen, onder wie ook jongeren, zich op een socialere manier gedragen (R1, R2, R3, R4, R5 onderzoekers, R6, 9, 10, $R1_a$, praktijkexpert en R11 beleidsexpert; Jones, 2007; Brown, 2003, Albin, 2012).

> **"**[…] bij preventief denk ik ook veel meer aan digitaal burgerschap. Dat je gewoon leert dat je je op een bepaalde manier hebt te gedragen, óók in de digitale wereld. Dat dat niet ineens totaal anders is […] dat je daar niet met mensen te maken zou hebben.**"**
>
> **R5 Onderzoeker**

## 5.3 Aangrijpingspunten voor interventies tegen Hacken

Hacken (ook wel computervredebreuk) is strafbaar gesteld in de wetsartikelen art. 138ab lid 1, 138ab lid 2, 138ab lid 3, en/of 138b. Het is een overkoepelend begrip dat de verschillende vormen van wederrechtelijk binnendringen in een computersysteem of netwerk beschrijft (o.a. Zebel et al, 2014; Ruiter & Bernaards, 2013; Holt, Bossler, May, 2012; Morris, 2011). Daarnaast is Hacken een *gateway* naar verschillende andere vormen van criminaliteit (Leukfeldt et al., 2010: Van der Wagen, Althoff & Van Swaaningen, 2016). Wat betekent dat hacken zowel een middel als een doel kan zijn[25].

Aan hacken ligt een grotere variëteit aan motieven en intenties ten grondslag. Deze motieven komen soms geïsoleerd maar vaak ook in combinatie voor (Xu, Hu, & Zhang, 2013; Van der Wagen, et al. 2016; Aiken, Davidson & Amann, 2016; Morris, 2011; Hoek van Dijke, 2016). Ook kunnen de motieven en intenties van hackers veranderen over de tijd (Árpád, 2013; Xu, Hu, & Zhang, 2013; Aiken, Davidson & Amann, 2016; Hoek van Dijke, 2016; Madarie, 2017)[26]. De belangrijkste (categorieën van) motieven die in de literatuur te vinden zijn, zijn:

- Uitdaging, bevrediging nieuwsgierigheid, zelfontplooiing
- Status onder peers vergroten
- Activistische doelen (boodschap af geven)
- Ethische doelen (slechte beveiliging blootleggen; waarschuwen voor online gevaren)
- Financieel gewin
- Macht over anderen verkrijgen (hacken om cyberagressie zoals stalking, bedreigen, afpersing mogelijk te maken)

Hacken is een handeling die strafbaar is bij wettelijke bepaling, maar anders dan bij offline criminaliteit gaan de handhavingsautoriteiten voor een deel mee in de gedachte dat er positieve functies bestaan van hacken. Zo is er in Nederland rond het beleid voor hacken een leidraad *responsible disclosure* die goedwillende, ethische hackers de mogelijkheid biedt om de ICT-beveiliging te verhogen (NCSC, 2013). Het blijkt in de praktijk echter erg lastig overeenstemming te bereiken over waar de grenzen liggen tussen ethisch en strafbaar hacken.

> **"**Dat ethisch hacken is zo'n lastige problematiek. […] want ik geloof dat het OM één van de grootste voorstanders is van goeie afspraken over ethisch hacken, maar dat wil niet zeggen dat ál het hacken ethisch is, en dat al het hacken dus goed is.**"**
>
> R4 Praktijkexpert

[25] De termen hacken en hacker hebben echter niet altijd deze negatieve connotatie. Zo wordt de term hacker ook gebruikt om een persoon te beschrijven die computerprogramma's en systemen dingen kan laten doen buiten hun oorspronkelijke ontwerp (Xu, Hu, & Zhang, 2013; Kao. Fu-Yuan Huang & Wang, 2009; Van der Wagen, et al. 2016).

[26] Traditioneel werden hackers in drie groepen ingedeeld, de *white hats,* de *grey hats* en de *black hats. De white hats* ook wel ethische hackers worden niet als crimineel beschouwd en hacken met goede intenties. De *black hats* zijn hackers die hacken met criminele intenties (Xu, Hu & Zhang, 2013; Van der Wagen, Althoff & van Swaaningen, 2016; Kao Fu-Yuan Huang & Wang, 2009; Morris, 2011). De *grey hats* zijn personen die uit bijvoorbeeld nieuwsgierigheid of ter zelfontplooiing hacken zonder hoger ethisch doel maar ook niet met de intentie iemand kwaad te doen (Xu, Hu & Zhang, 2013; Van der Wagen, Althoff & van Swaaningen, 2016; Morris, 2011).

Om maatregelen te kunnen ontwikkelen om te bevorderen dat jongeren alleen hacken met goede bedoelingen en weten waar de grenzen liggen, is het belangrijk inzicht te hebben in de wijze waarop hackers in een situatie terecht komen waarin zij besluiten te gaan hacken met kwade bedoelingen. Daartoe zullen we eerst beschrijven wat bekend is over de ontwikkeling die jeugdige hackers doorlopen. Vervolgens beschrijven we wat mogelijke maatregelen zijn om strafbaar hacken te verminderen.

### 5.3.1 Ontwikkelingen en achtergronden van jeugdige hackers

Hackers volgen de *age-crime* curve van traditionele daders, hacken wordt dan ook wel een jeugdprobleem genoemd (o.a. Yar, 2005; Xu, Hu, & Zhang, 2013; Ruiter & Bernaards; 2013; Aiken, Davidson & Amann, 2016 ). Een gangbare verklaring voor jeugdcriminaliteit is dat jongeren in hun adolescentie zich in een *maturity gap* bevinden. Een periode waarbij ze fysieke volwassenheid hebben bereikt en streven naar onafhankelijkheid en onttrekking aan controle. Jongeren hebben echter nog geen sociale volwassenheid bereikt en zijn nog op zoek naar hun eigen identiteit waarbij bevestiging gezocht wordt bij *peers* (Moffitt; 1993; Warr, 2002). Jongeren hebben in deze fase vaak nog onvoldoende cognitieve of psychosociale inzichten in normatieve vraagstukken (Eisenberg et al., 2005; Moffitt, 1993, Warr, 2002). Dit wordt ook wel aangeduid met *ethical deficit* en zorgt dat jongeren vatbaar zijn voor antisociaal en deviant gedrag (Kao. Fu-Yuan Huang & Wang, 2009; Xu, Hu & Zhang, 2013; Aiken, Davidson & Amann, 2016).

Als binnen de online dadergroep de plegers van cybercrime in brede en enge (zie H1) met elkaar vergeleken worden, kunnen verschillende daderprofielen worden onderscheiden. Zo hebben daders van cybercrime in enge zin een grotere kans dan daders van cybercrime in brede zin om veel te gamen, slachtoffer te zijn van cybercriminaliteit, offline delinquentie af te keuren, open te zijn naar ouders en minder vrienden te hebben die gedigitaliseerde criminaliteit (cybercrime in brede zin) plegen dan daders die cybercrime in brede zin plegen (Rokven, Weijters & Van der Laan, 2017).

Hackers kunnen zowel onder cybercriminaliteit in brede[27] als in enge zin vallen. Hacken betreft een groep delicten waarvoor verschillende gradaties in technische vaardigheden nodig zijn en dat een doel op zichzelf kan zijn of een middel om een bepaald doel te bereiken (Leukfeldt, et al., 2010; Rokven, Weijters & Van der Laan, 2017). Hackers zijn met andere woorden geen homogene groep, maar een heterogene groep individuen met verschillende intenties, motieven en risicoprofielen. Hieronder gaan we verder in op de rol van controle, *peers* en de *ethical deficit* binnen drie te onderscheiden stadia in het ontwikkelingstraject van hackers die door Xu, Hu en Zhang (2013) zijn onderscheiden: initiatie, groei en rijping.

#### *Initiatie*

Veel hackers beginnen niet met een crimineel motief. Het zijn vaak nieuwsgierige leerlingen die niet uitgedaagd worden door het normale lesprogramma op school, die al op jonge leeftijd

[27] Door het hacken wordt dan bijvoorbeeld toegang verkregen tot een digitale omgeving waarin diefstal kan worden gepleegd.

interesse hebben in computertechniek en beginnen te experimenteren met computers (Rokven, Weijters & Van der Laan, 2017; Hoek van Dijke, 2016; Aiken, Davidson & Amann, 2016; Xu, Hu, & Zhang, 2013; Morris, 2011; Bachmann, 2011, Ebenshade, 2002).

> "Dat ze zich inderdaad heel erg verveelden [op school] en juist heel goed daarin waren. Dus gingen ze op een gegeven moment in hun vrije tijd heel erg veel hacken en hadden het idee van: 'Ja, hier ben ik heel erg goed in'."
>
> R3 Onderzoeker

De affiniteit met computers en een betrokkenheid bij het leren hierover die jonge hackers vertonen, gaat in tegen de *General theory of crime* in (Holt, Bossler & May, 2011). Dit zou betekenen dat hackers een hoge mate van zelfcontrole hebben, het geen ondersteund wordt door de bevindingen van Rokven, Weijters en Van der Laan (2017) dat online daders een hogere zelfcontrole hebben dan offline daders. Andere onderzoeken vinden een minder hoge zelfcontrole bij hackers (Holt, Bossler, May, 2012; Bossler & Burruss, 2010). Een verklaring hiervoor kan zijn dat door de toegenomen mogelijkheden van het internet hackers de technische vaardigheden niet zelf onder de knie hoeven te krijgen, maar dat dit ook kan met behulp van sociaal leren via het internet (Hoek van Dijke, 2016; Holt & Bossler, 2011). Jongeren die de vaardigheden niet bezitten kunnen hier gemakkelijk *tools* kopen of aanleren, jongeren die de vaardigheden wel bezitten kunnen zich verder ontwikkelen (R2 praktijkexpert & R3 onderzoeker; Hoek van Dijke, 2016; Bachmann, 2011; Aiken, Davidson & Amann, 2016: Xu, Hu, & Zhang, 2013; Ebenshade, 2002).

### *Groei*

Internet is een ongereglementeerde en ongecensureerde verzameling bronnen met informatie, instructies en tools die jongeren kennis bieden om (criminele) handelingen uit te voeren (Aiken, Davidson, & Amann, 2016; Xu, Hu, & Zhang, 2013; Bachmann, 2011; Hoek van Dijke, 2016). Dit zorgt ervoor dat hun ontwikkeling als 'hacker' in een stroomversnelling terechtkomt (R2 praktijkexpert & R3 onderzoeker; Xu, Hu, & Zhang, 2013: Morris, 2011; Aiken, Davidson, & Amann, 2016). Internet stelt experimenterende jonge hackers bloot aan het risico met en het aangaan van online criminele handelingen (Aiken, Davidson, & Amann, 2016). Al experimenterend gaan jongeren steeds een stapje verder, waarbij de overgang van ethische hacken naar illegaal hacken geleidelijk en veelal ongemerkt verloopt (R2, R4 praktijkexperts, R3 onderzoeker; discussiebijeenkomst, Xu, Hu, & Zhang, 2013; Ebenshade, 2002).

> "Waren elke keer hele kleine trapjes [waarbij het ook echt het] grenzen verleggen is: deurtje gaat open, 'Oh wacht effe, ik ga kijken of het volgende deurtje ook open kan'. Voor je het weet kunnen ze een heel systeem hacken."
>
> R3 Onderzoeker

Het internet biedt jongeren de mogelijkheid om zich sneller te kunnen onttrekken aan de controle van hun ouders en formele controle in de offline maatschappij (zoals politie) (Katz, 1996; Mesch, 2012; Eisenberg et al., 2005; Xu, Hu, & Zhang, 2013; Bachmann, 2011; Aiken, Davidson, & Amann, 2016). Zo is de politie te weinig aanwezig om echt toezicht te hebben op

dit domein en weten ouders vaak niet wat de jongeren doen op het internet (Xu, Hu, & Zhang, 2013; Bachmann, 2011; Aiken, Davidson, & Amann, 2016; R2, R4, R6, R13, praktijkexperts, R3, R7, R12 onderzoekers). Terwijl jongeren niet gehinderd worden door sociale banden die binnen hun offline leefdomein aanwezig zijn, maken ze verbinding met gelijkgezinde, jeugdige hackers die ze online tegen komen (Aiken, Davidson, & Amann, 2016; R2 praktijkexpert & R3 onderzoeker; Xu, Hu, & Zhang, 2013; Morris, 2011). Het is deze *peergroup* aan wie ze hun gedrag normaliseren en met wie ze neutralisatietechnieken (Sykes, & Matza, 1957) ontwikkelen, die hun sociaal leven vormt en hun criminele gedrag faciliteert (R2 praktijkexpert & R3 onderzoeker; Aiken, Davidson, & Amann, 2016; Xu, Hu, & Zhang, 2013: Morris, 2011; Van der Wagen, et al. 2016; Turgeman-Goldschmid, 2008; Ebenshade, 2002; Kao. Fu-Yuan Huang, & Wang, 2009).

Jeugdige hackers zijn zich door de sociale waardering en neutralisatietechnieken die ze krijgen van hun *peers,* meestal ook maar beperkt bewust van het slachtoffer of de strafbaarheid van hun handelen (R2, R4, R6, R13 praktijkexperts, R3, R7, R12 onderzoekers; Kao. Fu-Yuan Huang, & Wang, 2009; Xu, Hu, & Zhang, 2013; Aiken, Davidson, & Amann, 2016; Morris, 2011). Hackers ontkennen in veel gevallen niet wat ze gedaan hebben, maar zien zichzelf als een 'positieve andere'. Veel van het hackgedrag wordt door hackers zelf dan ook niet als illegaal gezien. Zo blijken Nederlandse hackers, hacken alleen als illegaal te bestempelen als het doel financieel gewin is (Van der Wagen, et al. 2016). Verder ontkennen ze veelal slachtoffer of schade en geven aan te hacken voor een hoger doel, zoals online security of zelfontplooiing (R2, R6, R13, R4, praktijkexperts, R3, R12 onderzoekers; Van der Wagen, Althoff, & van Swaaningen, 2016; Turgeman-Goldschmid, 2008; Morris, 2011).

### *Rijping*

Volgens de experts uit de discussiebijeenkomst zal het overgrote deel van de jonge hackers na de fase van groei vanzelf stoppen met illegaal hacken en overstappen naar legaal hacken (R2, R4, R6, R13, praktijkexperts, R3, 12 onderzoekers, Hoek van Dijke, 2016; Morris, 2011). Dit is in overeenstemming met het levensloopmodel van Loeber (LeBlanc, & Loeber, 1998). De keuze om door te gaan met hacken komt volgens de wetenschappelijke literatuur vooral voort uit een verandering in motieven en de aanwezige normen en waarden (Morris, 2011; Vanderwagen, Althoff, van Swaaningen, 2016; Bachmann, 2011). De groep hackers die na hun adolescentie doorgaat met illegaal hacken onderscheidt zich volgens de experts door hun gedragsproblemen (R2, R4, R6, R13, praktijkexperts, R3, R12, onderzoekers) sommige experts benoemen zelfs zeer specifieke stoornissen.

> "Bijna al onze verdachten hebben, ja, gedragsproblemen, of zitten wel ergens het autistisch spectrum"
>
> R4 Praktijkexpert

Wanneer er over hacken als jeugdprobleem wordt gesproken met twee verschillende types, kan er een verband gelegd worden met de tweedeling van Moffitt (1993). De eerste groep bevat de *adolescent-limited* deviante jongeren. De jongeren die vanaf de adolescentie antisociaal gedrag vertonen, waarbij hun deviante gedrag vooral voortkomt uit de '*ethical deficit'* en hun contact met deviante *peers*. Deze groep stopt met vertonen van deviant gedrag

zodra zij uit hun adolescentie periode komen. Iets wat volgens de experts en wetenschappelijke literatuur over het algemeen gebeurt bij hackers (R2, R4, R6, R13, praktijkexperts, R3, 12 onderzoekers, Hoek van Dijke, 2016; Morris, 2011). De tweede groep zijn de *life-course persistent* deviante jongeren die al vroeg begonnen zijn met het vertonen van antisociaal gedrag, veroorzaakt door andere risicofactoren zoals veel gamen (op jonge leeftijd), en veel online zijn, (Rokven, et al. 2017). Dit hangt mogelijk weer samen met aangeboren karaktereigenschappen, of gebrek aan ouderlijk toezicht. Zij stoppen niet met het vertonen van deviant gedrag.

De resultaten van Moffitt (1993) over offline criminaliteit zijn waarschijnlijk niet één op één te vertalen zijn naar cybercriminaliteit door het cyberelement dat bij dit soort criminaliteit komt kijken. Zo zijn factoren die bij hacken een grote rol spelen bij het plegen van antisociaal en deviant gedrag: te weinig online controle, beperkt bewustzijn van strafbaarheid en laag slachtofferbewustzijn (zie ook Suler, 2004). Daarbij speelt het eerder besproken *disinhibition-effect* een belangrijke rol (Suler, 2004; Aiken, Davidson, & Amann, 2016). Als gevolg zien we dat mensen op internet gemakkelijk kunnen overgaan tot het vertonen van antisociaal en deviant gedrag dat zij in '*real life*' niet zouden vertonen (Suler, 2004; Kerstens, & Stol, 2012; Zebel et al., 2013). Crimineel hacken is daar een belangrijke uitingsvorm van.

### 5.3.2 Interventies

De ontwikkeling en achtergronden van jeugdige hackers zijn weergegeven in de drie stadia van Xu, Hu en Zhang (2013): initiatie, groei en rijping. Op elk van deze stadia kunnen interventies worden uitgevoerd. Het lijkt hierbij van belang rekening te houden met een onderscheid in de hierboven onderscheiden typen hackcarrières[28]. Preventieliteratuur, zowel vanuit de situationele als vanuit de dadergerichte preventie, heeft immers overtuigend laten zien dat een aanpak alleen effectief kan zijn als hij gericht is op het specifieke probleem (Clarke, 2009; Lipsey & Cullen, 2007).

#### *Initiatie*

Zoals beschreven lijken startende hackers zich vaak niet bewust van de mogelijke consequenties van hun handelingen. Zij realiseren zich niet dat het strafbaar is, dat zij verstrikt kunnen raken in criminele netwerken en zijn zich weinig bewust van de schade die zij toebrengen. Er wordt verwacht dat versterking van het bewustzijn van de gevolgen het gedrag van de jongeren zou kunnen veranderen (R2, praktijkexpert, R3, R12, Onderzoekers; Esbenshade, 2002; Aiken, Davidson, & Amann, 2016). Jonge potentiële hackers zouden zich bewust moeten zijn van het effect van hun handelen op hun slachtoffers, maar ook dat hun handelen strafbare gevolgen kan hebben en dat ze met het hacken gemakkelijk in aanraking kunnen komen met gevaarlijke criminelen. Dit bewustzijn zou op verschillende manieren vergroot kunnen worden. In de eerste plaats door voorlichting aan de hand van educatieve programma's (Árpád, 2013). De focus van de educatieve programma's zou minder dan nu gebruikelijk is op het mogelijke slachtofferschap moeten liggen en meer op de mogelijke

[28] Al moet nog verder onderzocht worden in hoeverre de tweedeling van Moffitt (1993) terug te vinden is in de hackergemeenschap.

daderschap (zie hoofdstuk 4 'online veiligheid' en R6, R13 praktijkexperts, R3 onderzoeker; Aiken, Davidson, & Amann, 2016). Naast educatieve programma's zou het om bewustwording en gedragsverandering te creëren volgens de experts ook nuttig zijn om een digitale agent (een soort wijkagent maar dan op cybergebied), in school te hebben (R6, R13, praktijkexperts, R3 onderzoeker; Aiken, Davidson, & Amann, 2016). Op die manier hebben jongeren direct toegang tot informatie over 'wat mag en niet mag'.

> **"**Ze hebben gewoon een vraag. Als jij gewoon in je uniform rondloopt in een school, gaan ze jou gewoon uiteindelijk die vragen stellen. En dat is wat we willen: gedragsbeïnvloeding.**"**
>
> R13 Praktijkexpert

Tot slot is er veel discussie over de rol van de ouders. Het gebrek aan ouderlijk toezicht verhoogt namelijk de kans dat de kinderen online daders worden (Rokven, Weijters, & Van der Laan, 2017; Kao. Fu-Yuan Huang, & Wang, 2009; Aiken, Davidson, & Amann, 2016; Hoek van Dijke, 2016) en dat gebrek aan toezicht komt veelvuldig voor. Het wordt niet goed duidelijk uit de literatuur hoe ouders hierop kunnen worden getraind en of en op welke manier zulk toezicht effectief kan zijn. Wel wordt duidelijk dat als er voorlichting wordt ingezet het van belang is dat de nadruk ligt op (de gevolgen van) daderschap (R2, R4, R6, R13, praktijkexperts, R3, R12 onderzoekers; Kao. Fu-Yuan Huang, & Wang, 2009; Aiken, Davidson, & Amann, 2016). Er is echter veel literatuur die aangeeft dat de invloed van ouders op adolescenten beperkt is en die van vrienden veel sterker (Moffitt, 1993; Warr, 2001). Recent onderzoek naar jeugdige cybercriminelen, geeft dan ook aan dat er meer verwacht kan worden van *peers* die als positieve rolmodellen fungeren en jongeren kunnen behouden van het plegen van cybercrime (Aiken, Davidson, & Amann, 2016).

### *Groei*

Tijdens het stadium 'groei' is voorlichting om bewustwording te creëren nog steeds belangrijk. Aangezien er in deze groeifase sprake kan zijn van concrete gedragingen, zal de bewustwording zich ook op die concrete handelingen kunnen richten. Daartoe voert de politie nu 'foei gesprekken' met jongeren op school of bij de jongeren thuis met de ouders er bij, ook wel *walk and talk* genoemd (R13 & R6 praktijkexperts). Over de effectiviteit van deze gesprekken is nog weinig bekend, maar de experts geven aan dat er tijdens de confrontatie zelf een schrikreactie wordt waargenomen, van zowel ouders als jongeren (R13 & R6 praktijkexperts). Opeens worden de jongeren er op gewezen dat hun online handelen, offline consequenties heeft.

> "Je kunt ervoor kiezen om een wijkagent even een gesprek te laten voeren en dan zie je een enorme schrikreactie. De ouders hebben vaak echt geen benul en het gaat vaak nog om jongere kinderen."
>
> R13 Praktijkexpert

Naast het bewustmaken dat online handelingen offline gevolgen kunnen hebben, is het belangrijk dat jongeren ook op het internet gecontroleerd worden. Dit gebeurt nu zeer beperkt en het is nog niet goed duidelijk hoe dit vormgegeven zou moeten worden (Xu, Hu, & Zhang, 2013; Bachmann, 2011; Aiken, Davidson, & Amann, 2016; R2, R4, R6, R13, praktijkexperts, R3,

R7, R12, onderzoekers). Veel jongeren in deze levensfase zijn niet instaat zichzelf te reguleren en hebben daarom juist controle op hun online gedrag nodig om niet te vervallen in antisociaal en deviant gedrag (Eisenberg et al., 2005). Met deze controle zou een duidelijkere grens moeten worden aangegeven tussen acceptabel en onacceptabel gedrag (R2, R4, R6, R13, praktijkexperts, R3, R7, R12 onderzoekers; Kao. Fu-Yuan Huang, & Wang, 2009; Xu, Hu, & Zhang, 2013; Aiken, Davidson, & Amann, 2016). Volgens Respondent 3 (onderzoeker) geven de jongeren in interviews aan dat controle geholpen zou hebben en zien we aan het aantal volgers van politievloggers dat jongeren een wens naar sturing hebben. Er is echter geen onderzoek bekend naar de effecten van dergelijke onlinecontrole op het gedrag, dus het is niet duidelijk of het werkelijk effectief is. Verschillende experts geven niettemin aan dat de zichtbare aanwezigheid van de politie op het internet moet worden vergroot (R2, R4, R6, R13, praktijkexperts, R3, R12 onderzoekers).

> "Ik heb jongeren geprobeerd te vragen: 'Wat zou dan helpen? Wat heeft dan geholpen als jij daar geweest was?' Toen zeiden ze: 'Die advertenties die ik nu zie over 'wij zoeken mensen voor de cyberpolitie'. Dat soort advertenties dat werkt wel van 'oh'. Zij hadden ook graag gewild, net als op het station, dat je in de gaten gehouden wordt. Alleen maar puur die zichtbaarheid van de politie, ook dus de zichtbaarheid op: ze komen de klas in, dat doet dan toch wat met ze, ongeacht dat ze dan zoiets hebben van: 'Mij kun je niet pakken, want je kunt het niet zien', toch werden ze daar wel een beetje zenuwachtig van. En datzelfde zeiden ze van: "Ja, als ik het online terug zou zien, dan zou ik daar ook meer bewust van zijn".
>
> R3 Onderzoeker

Online controle is belangrijk, echter zou er goed gekeken moeten worden wie de jongeren op hun gedrag aanspreekt. Ook hier zou het direct aanspreken van jongeren online (digigeren) kunnen voorkomen dat jongeren strafbare handelingen uitvoeren (Broekman, Wetzer, Wijn, & Roelofs, 2014). Maar opnieuw is bij dit digigeren van groot belang dat duidelijk is wat de motivatie van de pleger is en hoe de inhoud, woorden en afzender van een waarschuwingsbericht daarop aansluiten. Hier kunnen opnieuw peers een belangrijke rol spelen. Bevestiging van en hechting aan andere *peers* is immers belangrijk in deze groep (Warr, 2002). Bij de *adolescent-limited* deviante jongeren is het dus mogelijk nuttig de informatie door *peers* te laten verwoorden. In onderstaand citaat wordt door een ethisch hacker verwezen naar een voorbeeld van zo'n 'peerreview'.

> "Jongere gasten die nu op Twitter roepen: "Ik ga volgende week een dump releasen van de ambassade van Rusland". Die spreken we: "Joh, let op: niet alleen de politieorganen, maar ook andere inlichtingsdiensten – en daar zitten niet de meest vriendelijke tussen – en ook gewoon criminelen, die denken van: 'Hé, dat is handig, die jongen heeft potentieel […]"
>
> R2 Praktijkexpert

Bij dit stadium is het echter wel belangrijk om snel te handelen. Zoals blijkt uit de ontwikkeling van jeugdige hackers werkt contact met andere hackers in de 'groei fase' als een

stroomversnelling (R2, praktijkexpert, R3, R12 onderzoekers; Kao. Fu-Yuan Huang, & Wang, 2009; Xu, Hu, & Zhang, 2013; Morris, 2011; Bachmann, 2011; Yar, 2005).

> **"**Je moet ze heel snel aanspreken. Dan moet je dat ook kunnen doen vanuit een autoriteit. Kijk, als ik een jongen aanspreek, dan hoef ik niet uit te leggen wie ik ben, maar dat is voor andere partijen lastig en dan heb ik maar een heel korte tijdspanne, hooguit een halfuur de tijd om dan mijn verhaal aan hem over te brengen, niet op een manier als belerend, van 'opa vertelt even hoe het moet'. Als ik bijvoorbeeld, het gesprek stop, maar een uur later komt 'ie weer terug, dan kan het drie, vier uur 's nachts zijn, en ik reageer niet binnen tien minuten, dan ben ik 'm eigenlijk al kwijt.**"**
>
> R2 Praktijkexpert

Controle en bewustmaking van jongeren online hoeft dus niet alleen vanuit de politie te komen. Die online controle zou zelfs effectiever kunnen zijn als deze vormgegeven zou worden aan de hand van *community policing*, waarbij er een samenwerkingsverband bestaat tussen de gebruikers van het internet, serviceproviders, scholen, ouders, enz. en de politie (Jones, 2007; Brown, 2003; Aiken, Davidson, & Amann, 2016). Een belangrijk punt is echter wel het identificeren van jongeren die risico lopen om online crimineel gedrag te vertonen. Een mogelijke manier om jongeren vroegtijdig te identificeren, is door het ontwikkelen van een *Technology Quotiënt (T.Q.)*. Aan jeugdigen die hoog scoren op de T.Q. kunnen vervolgens in het onderwijs alternatieve ontwikkelingspaden aangeboden worden (Aiken, Davidson, & Amann, 2016; $R1_a$ praktijkexpert). Het Lectoraat Cybersafety voert momenteel onderzoek uit naar een interventie voor zulke scholieren met computer affiniteit. Het is een interventie die gebruikt maakt van het idee van *community policing* ($R2_a$ onderzoeker). In dit project worden jongeren met computer affiniteit betrokken bij politiewerk, waarbij jongeren de politie helpen door te signaleren en adviseren. Dit biedt jongeren niet alleen de kans om de samenleving te helpen, maar ook om legaal bezig te zijn met hacken. Dit onderzoek loopt nog dus het is onduidelijk welke effecten ervan uitgaan. Tot slot is het van belang te benoemen dat de *life-course persistent* deviante jongeren minder baat zullen hebben bij de hierboven beschreven interventies omdat in deze groep zoals eerder benoemd andere risicofactoren een rol spelen[29].

### *Rijping*

Bij de hackers die overgaan tot ernstiger crimineel gedrag en die in de strafrechtelijk keten terechtkomen, lopen de rechtshandhavers tegen verschillende problemen aan (R4, R6, R9, R10, R13, praktijkexperts). Zo is het lastig voor de reclassering een advies uit te brengen, vooral omdat door het 'cyber' element moeilijk het slachtofferbelang en het recidive risico in te schatten zijn. Het is volgens de reclasseringsmedewerkers in de discussiebijeenkomst dan ook van belang dat reclasseringsmedewerkers getraind worden en dat nagegaan wordt of de risico's en criminogene problematiek die spelen bij cyberdelicten voldoende in beeld gebracht kunnen worden met de huidige diagnose instrumenten op basis waarvan onder andere OM en

[29] Overigens wordt door experts de aanname uitgesproken dat (vergelijkbaar met de situatie bij offline criminaliteit) het merendeel van de jonge hackers waarschijnlijk vallen onder de *adolescent-limited* deviante jongeren (R2 ethisch hacker, R3 onderzoeker & R6, 13 politiefunctionarissen; Aiken, Davidson, & Amann, 2016).

rechter geadviseerd worden (R9, R10, praktijkexperts). Het volgende punt waar de reclassering tegen aanloopt, is dat er nog weinig kennis beschikbaar is over hoe er bij illegale hackers een gedragsverandering gestimuleerd kan worden (R9, R10 praktijkexperts, R3, R12 onderzoekers).

Teamleiders van de jeugdreclassering[30] geven aan tot nu toe slechts enkele casussen te kennen waarin deze problematiek speelt. Toch is er behoefte zijn aan landelijk beleid over deze problematiek omdat zij horen en voorzien dat deze problematiek steeds groter wordt onder de jeugd. Deze teamleiders kennen geen specifieke interventies voor dit type daders.

Beleidsmedewerkers van HALT geven aan dat er geen exacte cijfers beschikbaar zijn over aantallen daders van cyberdelicten maar dat zij meer te maken krijgen met daders van gedigitaliseerde criminaliteit (cybercrime in brede zin) dan van cybercrime in enge zin. Deze daders passen volgens de respondent goed in de gangbare aanpak van HALT maar meer training van de medewerkers in de materie zou wel een punt van aandacht zijn. De theorieën waarmee de HALT interventies onderbouwd worden, zijn inderdaad deels overeenkomstig met theorieën die beschreven werden bij de effectieve interventies in hoofdstuk 4 (i.e. sociale leertheorie, reintegrative shaming, theorie over morele ontwikkeling) daarnaast is de labelling theorie belangrijk bij HALT, een theorie waarin uiteengezet wordt hoe stigmatisering door bestraffing uiteindelijk tot meer strafbaar gedrag leidt (Goffman, 1959; Matza, 1969). Gezien de eerder besproken onduidelijkheid en beperkte kennis van jongeren over de grenzen tussen strafbaar en niet strafbaar anti-sociaal gedrag online, lijkt het bij cybercrime extra van belang interventies zo in te richten dat ze niet juist leiden tot versterking of ontwikkeling van een criminele identiteit waar die nog niet of niet sterk aanwezig is. Ook andere principes van de HALT straffen sluiten aan bij potentieel effectieve factoren die eerder zijn benoemd zoals het creëren van een groter besef van de aangerichte schade bij slachtoffers (door excuses aan te bieden), het betrekken van ouders, het bespreken van gedragsalternatieven en het inperken van negatieve *peer pressure*. Echter zowel over interventies gericht op de effectiviteit van ouderbetrokkenheid als over het inperken van negatieve *peer pressure* zijn eerder in deze studie twijfels uitgesproken of zij mogelijk zijn en zo ja of zij daadwerkelijk impact zullen hebben op online gedrag van jongeren.

De mogelijkheid om cybercrime te voorkomen door daders de toegang tot ICT te onthouden, blijken zeer beperkt. Doordat technologieën ver zijn doorgedrongen in ons dagelijkse leven en we in een afhankelijkheidsrelatie terecht zijn gekomen met ICT zouden dergelijke maatregelen snel disproportioneel zijn (R4, R6, R13, praktijkexperts, Janssen, 2015; Facer & Furlong, 2001). Bovendien is algehele onthouding van ICT moeilijk te handhaven omdat er op veel manieren toegang tot het internet te krijgen is. Toch zijn er wel degelijk technologische interventies die te handhaven zijn, denk aan *big data mining*, *biofeedback*, of *wifi-blocking* door een armband etc. Van deze mogelijke interventies is echter nog niet bekend wat de effectiviteit is (R2, R6, R9, R10, R13 praktijkexperts, R11 beleidsexpert).

> **"**Het is uitvoerbaar, maar dan moet je dus wel 1) je personeel gaan herscholen, want daar schort het echt wel aan, en 2) het gaat geld kosten. Het gaat de maatschappij geld kosten.**"**
>
> R13 Praktijkexpert

[30] informatie via e-mail wisseling van twee teamleiders uit verschillende regio's.

Naast technologische interventies kan er ook gedacht worden aan *re-intergratieve shaming*. Volgens Kao, Fu-Yang Huang en Wang (2009) moet er rekening gehouden worden met de specifieke subcultuur waarin deze jongeren zich bevinden (zie hoofdstuk 4 'hacken: waarschuwen, alternatieven en effectieve normen'). Uit de wetenschappelijke literatuur (Aiken, Davidson, & Amann, 2016) en de expertgroep (R2 praktijkexpert) kwam naar voren dat hier inderdaad mogelijkheden voor interventies liggen. Daar werd gesteld dat het ook bij deze groep hackers nuttig kan zijn om *peer-reviews* te houden. Mede hackers, als *peers*, zouden een grote invloed kunnen uit oefenen op deze jongeren (zie opnieuw het onderzoek van Aiken, Davidson, & Amann, 2016). Ethische hackers kunnen in het geval van hacken ingezet worden als positieve rolmodellen, een samenwerking met ethisch hackers die de groep van binnen uit kennen zou bovendien ook bij kunnen dragen aan de ontwikkeling van strategieën door de reclassering (R2 praktijkexpert & R3, 12 onderzoekers; Aiken, Davidson, & Amann, 2016; Kao. Fu-Yuan Huang, & Wang, 2009). Er is echter nog geen onderzoek waarin de effectiviteit van zulke interventies wordt onderzocht. Bij dit type peergerichte interventies bestaat bovendien het gevaar dat ook illegaal gedrag overgedragen wordt (vgl. uitgangspunten What works, Andrews & Bonta, 1990). Het is daarom van belang deze gevaren van te voren goed in te schatten en vervolgens te monitoren in welke mate hiervan sprake is.

# 6. Conclusie en discussie

Dit rapport bevat een inventarisatie van wetenschappelijke evaluatiestudies naar bestaande interventies voor het inperken van daderschap van gedigitaliseerde criminaliteit en cybercriminaliteit door jongeren. De onderzoeksvragen zoals geformuleerd in de inleiding richten zich op de beschrijving van die interventies (onderzoeksvragen 1 en 2), de programma integriteit van de beschreven interventies (onderzoeksvraag 3), de effectiviteit van de beschreven interventies (onderzoeksvraag 4) en de kenmerken van veelbelovende en effectieve interventies (onderzoeksvraag 5).

Van alle in de systematische literatuurstudie gevonden interventies waarvan een inhoudelijke evaluatie of effectevaluatie beschikbaar was (totaal 39) was er maar 1 specifiek op jeugdige daders gericht, het overgrote gedeelte van de interventies is gericht op algemene populaties jongeren en heeft een preventief karakter. Bovendien richten veel interventies zich tegelijkertijd op potentiële daders, slachtoffers en omstanders. Naast geëvalueerde interventies gericht op jeugdige daders, hebben we in dit rapport ook de preventieve interventies geanalyseerd en vervolgens voor twee categorieën cyberdelicten (hacking en cyberagressie) een verdiepende studie gedaan waaruit kenmerken naar voren komen waarmee toekomstig te ontwikkelen interventies rekening zouden moeten houden om effectief te kunnen zijn. Deze analyse sluit aan bij onderzoeksvraag 5 waarin het gaat om kenmerken van veelbelovende of effectieve programma's. De conclusies die uit de verdiepende studie naar voren komen, zullen echter hun waarde nog moeten bewijzen in de effect-evaluaties van feitelijke interventies waarin de inzichten zijn ingezet.

## 6.1 Beschrijving van de interventies

De eerste twee onderzoeksvragen richten zich op de beschrijving van de in de literatuurstudie gevonden interventies. Hierover werden de volgende vragen geformuleerd:

1. Welke interventies kunnen in de internationale literatuur worden onderscheiden die zich richten op daderschap van gedigitaliseerde criminaliteit en cybercrime onder jongeren?
2. In welke categorieën zijn deze interventies in te delen voor de volgende kenmerken:
    a. Het type cybercrime waarop de interventie zich richt.
    b. De populatie waarop de interventie zich richt.
    c. De achterliggende theorie op basis waarvan effectiviteit verwacht kan worden.
    d. De gebruikte methoden in de interventie.
    e. De betrokken uitvoerders.

Zoals in de introductie van de conclusie beschreven, is er informatie gevonden over totaal 39 interventies, voor de overgrote meerderheid interventies met een preventief karakter gericht op algemene populaties jongeren. Veelal was de directe beïnvloeding van dadergedrag (bij potentiële daders) maar een onderdeel van de interventie en waren daarnaast beïnvloeding van houding en gedrag van slachtoffers en omstanders belangrijke programmadoelen. Naast interventies die zich op veilig en acceptabel online gedrag en online beveiliging in het algemeen richten, werden (deels) dadergerichte interventies gevonden voor drie specifieke typen cybercrime:

1) Cyberagressie
2) Sexting
3) Hacking

*Populaties (onderzoeksvraag 2b)*

De interventies voor het vergroten van *online veilig gedrag* en voor het terugdringen van *cyberagressie* zijn gericht op jeugdigen van verschillende leeftijden. De meeste interventies richten zich op de hogere klassen van het basisonderwijs en op het voortgezet onderwijs. De exacte leeftijdsgroep waarover de evaluatiestudies rapporteren, is echter steeds verschillend.[31] De interventies hebben een preventief karakter en richten zich op de groep als geheel waarbij alle leerlingen blootgesteld worden aan dezelfde informatie, discussie en trainingsmomenten. Er wordt daarbij dus geen onderscheid gemaakt tussen potentiële daders, slachtoffers of omstanders. Voor pestgedrag is een dergelijke brede aanpak van belang omdat hierbij het hele systeem (waarbinnen de verschillende typen normen aanwezig zijn) een rol speelt. Voor andere vormen van cyberagressie (stalking, bedreiging, etc.) is het individuele aspect waarschijnlijk veel groter en zou (naar verwachting van de What Works beginselen) meer maatwerk nodig zijn om effectiviteit te sorteren.

De *sexting* interventies richten zich op jongeren vanaf 13 tot ongeveer 24 jaar, enkele interventies noemen geen bovengrens in leeftijd. Ook bij deze interventies worden (potentiële) daders, slachtoffers en omstanders gelijktijdig aangesproken. Hoewel dit niet in de programmabeschrijvingen als zodanig benoemd wordt, is bij ongeveer de helft van de interventies het educatiemateriaal en de boodschap die de interventies uitdragen sterk gericht op de (tiener)meisjes die het beeldmateriaal (van zichzelf) in eerste instantie posten en versturen. De personen (jongens en meisjes) die vervolgens misbruik maken van dit materiaal worden door deze interventies niet of nauwelijks aangesproken.

De *hacking* interventies zijn wel specifiek gericht op feitelijke daderpopulaties die in reactie op hun hackgedrag worden aangesproken. Van de vier gevonden interventies is er echter maar een gericht op jeugdige daders. Dit is de reintegrative shaming interventie die beoogt hackersubculturen aan te spreken.

*Theorieën (onderzoeksvraag 2c)*

De theorieën die genoemd worden bij de *online veiligheid* interventies zijn de sociale leertheorie, de theorie van gepland gedrag en het 'extended parallel proces model' (EPPM). Dit laatste model is vrijwel volledig gericht op het voorkomen van slachtofferschap en richt zich niet op (potentiële) daders.

De meeste *cyberagressie* interventies zijn gebaseerd op effectief bevonden schoolgerichte antipest programma's voor off-line pesten. De in de interventies genoemde theorieën zijn voornamelijk systemische theorieën, zoals de theorie over sociaal leren, normatief sociaal gedrag, de theorie van gepland gedrag, de theorie van beredeneerd gedrag, en de positief psychologische benadering. De groepsnormen (descriptief en injunctief) en

[31] Deze en andere verschillen tussen de interventie en evaluatiestudies maakt een zinvolle vergelijking van de effecten die de interventies hebben niet mogelijk.

invloed van die normen op het gedrag van individuen spelen daarbij een grote rol. Wanneer de sociale opbrengsten van de cyberagressie voor de daders omlaag gaan omdat de groep het gedrag afkeurt, zal de kans op agressie kleiner zijn. Op daderniveau speelt, hoewel niet altijd als zodanig benoemd, een belangrijk aspect uit het herstelrecht een rol, namelijk het vergroten van de empathie voor het slachtoffer wat volgens deze benadering tot een afname in de cyberagressie zou moeten leiden.

De *sexting* interventies zijn weinig theoretisch onderbouwd en lijken vooral gebruik te maken van afschrikkingsgerichte theorieën. Een enkele interventie maakt gebruik van feministische theorieën. Bovendien is bij enkele interventies een systemische benadering zichtbaar waarin omstanders een rol krijgen in het signaleren en ingrijpen bij (dreigende) schadelijke vormen van sexting.

Bij de *hacking* interventies worden verschillende theoretische uitgangspunten genoemd. Dit zijn: a) de 'preference shaping theory': door het aanbieden van aantrekkelijke alternatieven voor het illegale hackgedrag, verandert de beloningsstructuur van het illegale hacken in negatieve zin (rationele keuze benadering); b) Reintegrative shaming (Braithwaite, 1989) waarin ervan wordt uitgegaan dat de intenties om zicht te misdragen afnemen door het creëren van een 'shaming' proces waarin het strafbare feit afgewezen wordt en niet de dader; en c) de afschrikkingstheorie die ervan uitgaat dat de angst voor sancties het individu afremt in het plegen van illegale activiteiten.

*Methoden (Onderzoeksvraag 2d)*

De meeste interventies voor *online veiligheid, cyberagressie en sexting* gebruiken methoden gericht op kennisoverdracht en het geven van duidelijke kaders over acceptabel gedrag. Richting de plegers gaat het dan vooral om kennis over de aangerichte schade en over eventuele strafrechtelijke gevolgen. Daarnaast worden cognitieve gedragstherapeutische methoden ingezet en is er aandacht voor positieve versterking en het versterken van het moreel redeneren. Er worden rollenspellen ingezet om de normen van anderen te onderzoeken, en om handelingsopties te trainen voor omstanders. Ook training van sociale vaardigheden, cognitieve en affectieve empathie en onlinevaardigheden komt in verschillende interventies terug.

Bij de hacking interventies zijn de methoden minder duidelijk omschreven. Er wordt gebruik gemaakt van pscyho-educatie bij het bewustmaken van de risico's en schade door het hackgedrag. Verder is, hoewel niet expliciet beschreven een systemische aanpak noodzakelijk bij de reintegrative shaming interventie.

*Betrokken uitvoerders (Onderzoeksvraag 2e)*

Omdat een groot deel van de interventies gericht is op algemene populaties jongeren zijn de scholen in de meeste gevallen de plek waar de interventies plaatsvinden. In veel gevallen is er sprake van lespakketten waar de scholen zelfstandig mee werken in sommige programma's worden ook leerkrachten en ouders getraind door externe (veelal private) instanties die de programma's ontwikkelen en of beheren. Er zijn enkele van zulke algemene interventies geëvalueerd die volgens de programmabeschrijving ook beschikbaar zijn voor gedragsverandering binnen het strafrecht (i.e. iKeepSafe, NetSmartz en WebWiseKids). Er zijn

echter geen studies gevonden waarin de toepassing van deze interventies binnen het strafrecht werd onderzocht. Andere actoren die in de interventies genoemd worden zijn de politie en (voor de hack in contests) bedrijven.

## 6.2 Programma integriteit

De derde onderzoeksvraag richt zich op de programma integriteit en is als volgt geformuleerd:

3. Wat is er bekend over de programma integriteit bij de uitvoering van de interventies?

Uit de evaluaties komt maar zeer beperkt naar voren wat de programma-integriteit was bij de interventies. Wat wel duidelijk wordt, is dat er vooral sprake is van voorlichting en sociaal leren (aan de hand van interactief materiaal). Actieve lesmethoden waardoor jeugdigen daadwerkelijk vaardigheden kunnen trainen, lijken veelal nog onvoldoende centraal te staan in de programma's en worden daar waar ze wel beschreven zijn in de praktijk maar zeer beperkt uitgevoerd. Uit wetenschappelijk onderzoek komt echter naar voren dat 'actief leren', het daadwerkelijk aanleren van vaardigheden, effectiever is dan alleen voorlichting (Jones, Mitchel, & Walsch, 2014a). Ook zijn er aanwijzingen dat geplande trainingen en voorlichting aan ouders en leerkrachten maar zeer beperkt worden uitgevoerd. Daarmee zijn zowel de vertaling van de achterliggende werkzame mechanismen naar de programmabeschrijving als de programma integriteit bij veel interventies nog beperkt. Effecten van de programma's zouden mogelijk groter zijn als dit beter wordt uitgewerkt.

## 6.3 Effectiviteit van de beschreven interventies.

De vierde onderzoeksvraag richt zich op de effectiviteit van de interventies:

4. Wat is er bekend over de effectiviteit van de interventies voor het voorkomen van gedigitaliseerde en cybercriminaliteit onder jongeren en op welke wijze is dat onderzocht?

De evaluatiestudies die in de systematische zoektocht zijn gevonden, betroffen zowel effectevaluaties als inhoudelijke evaluaties[32]. In totaal waren er voor 13 interventies effectstudies beschikbaar. Deze gingen vooral over online-veiligheid en cyberagressie[33]. Van de effectstudies had maar een klein deel (totaal 4 studies) een experimenteel design, dit waren interventies voor cyberagressie en hacking. Daarnaast waren er 5 studies met een quasi-experimenteel design, hier was wel sprake van een voor- en nameting bij een experimentele en controle groep maar waren de groepen niet op basis van toeval samengesteld. De laatste 4 'effectstudies' hadden en nog lager experimenteel niveau, daarbij was bijvoorbeeld geen controlegroep of geen voormeting aanwezig.

Vooral de interventies gericht op cyberagressie blijken in zekere mate effectief hoewel de effecten op cyberslachtofferschap veelal groter zijn dan op daderschap. Bij de cyberagressie

[32] Uit dit laatste type evaluaties kunnen alleen conclusies worden getrokken of een interventie *naar verwachting* effectief is. Hiertoe wordt bekeken op welke mechanismen de interventies ingrijpen en of de methoden waarmee dat wordt gedaan naar verwachting effectief zijn.

[33] Daarnaast was er 1 effectstudie voor een sexting interventie en 1 voor een hacking interventie.

programma's waren naast programmadoelen over het feitelijk terugdringen van daderschap ook veel tussenliggende programmadoelen geformuleerd zoals 'het vergroten van kennis en bewustzijn over de prevalentie en gevolgen van pesten'. Deze tussenliggende programmadoelen bleken vaak in zeker mate gehaald te worden, de kennis en bewustzijn veranderde dus in positieve zin, maar deze veranderingen gaven niet zoals verwacht een verklaring voor de eveneens gevonden afnames in cyberpesten of cyberslachtofferschap. Kortom de kennis en het bewustzijn over de gevolgen nam toe en het pestgedrag nam af, maar de afname in het pestgedrag bleek niet het gevolg te zijn van de toename in kennis en bewustzijn. Daardoor bleef het achterliggend mechanisme dat leidde tot een afname in het pestgedrag onduidelijk.

Deze cyberpestprogramma's zijn vaak afgeleid van bestaande antipest of anti-agressie interventies en houden rekening met verschillende aspecten waarvan bekend is dat ze de effectiviteit van interventies vergroten. Wat betreft de daders zijn dit de inzet op dynamische criminogene factoren (op individueel en omgevingsniveau[34]) en het afstemmen van de interventie op de responsiviteit van de doelgroep. In deze interventies is er dan ook meer dan bij de interventies voor online veiligheid of sexting sprake van het daadwerkelijk trainen van vaardigheden[35] en het aanleren van alternatief gedrag[36].

Voor de online veiligheidsinterventies kan de conclusie getrokken worden dat er weinig tot geen effecten zijn op het voorkomen van daderschap van criminaliteit. Hoewel het bewustzijn over schade en risico's van het gedrag enigszins lijkt te worden bereikt, is niet aangetoond dat dit zich omzet in minder antisociaal of crimineel gedrag online. Mogelijk is een beperkte programma-integriteit van de programma's, vooral het ontbreken van feitelijke training en het uitblijven van de ondersteunende omgeving (door gebrek aan effectieve training van ouders en docenten) hier mede oorzaak van.

De effectstudie voor de sexting interventie (Pass it on) toont geen effect van de interventie op de houding ten opzichte van sexting. De hacking interventie waarvoor een effectevaluatie gevonden is (warning banners) bleek ook niet effectief. Deze interventie is gebaseerd op het principe van afschrikking maar dat blijkt in deze vorm dus niet als zodanig te werken. Op basis van inhoudelijke evaluaties zijn er positieve verwachtingen van de toepassingen van reintegrative shaming (bij hacken) maar er zijn nog geen concrete toepassingen hiervan beschreven.

Vrijwel alle geëvalueerde programma's zijn ontwikkeld voor en worden toegepast op een brede doelgroep, en de interventies lijken dan ook geen rekening te houden met specifieke criminogene factoren van mogelijke daders. Hierbij kan het bijvoorbeeld gaan om specifieke gedragsproblemen, een problematisch opvoedklimaat, of verslavingsproblematiek. Voor de cybercrime plegers met meer complexe of ernstige problematiek zullen de bestaande interventies dus naar verwachting weinig effect hebben.

[34] Zoals groepsdruk, gebrek aan toezicht en gebrek aan empathie voor het slachtoffer onder andere veroorzaakt door het disinhibitie-effect.

[35] Zoals perspectief nemen, sociale en cognitieve vaardigheden en het vergroten van de empathie.

[36] Binnen de educatieve interventies voor online veiligheid blijken ook juist die interventies, waarin naast bewustwording van risico's ook het aanleren van vaardigheden om risico's te vermijden expliciet als programmadoel was opgenomen, effectiever te zijn dan de interventies die alleen op bewustwording zijn gericht.

## 6.4 Aangrijpingspunten voor effectieve interventies

De laatste onderzoeksvraag richt zich op aangrijpingspunten voor het ontwikkelen van toekomstige interventies:

5. Op welke wijze onderscheiden de effectieve en veelbelovende interventies zich van de niet effectieve interventies voor de kenmerken uit de tweede onderzoeksvraag?

Deze vraag is in dit onderzoek beantwoord voor twee typen cyberdelicten namelijk cyberagressie en hacking.

*Cyberagressie*

Bij de aanpak van cyberagressie lijkt in sterke mate gebruik gemaakt te kunnen worden van bestaande interventies gericht op agressief en antisociaal gedrag. Uit de literatuur blijkt namelijk dat jeugdige plegers van cyberagressie sterk lijken op jeugdige plegers van offline agressie. Bestaande interventies bij de ketenpartners en zorgverleners kunnen dus in enigszins aangepaste vorm ingezet worden voor plegers van cyberagressie.

Dat de bestaande interventies wel aanpassingen nodig hebben, heeft te maken met het feit dat er ook verschillen zijn aangewezen tussen online en offline plegers van agressie. Zo hebben cyberagressieplegers een hogere sociale intelligentie, meer internetvaardigheden en lagere algemene niveaus van agressie. Daderschap in cyberagressie hangt bovendien vaker samen met slachtofferschap van agressie (zowel offline als online) dan daderschap van offline agressie. Deze conclusies zijn echter vooral gebaseerd op onderzoek uit andere landen en het is de vraag of daderkenmerken van cyberagressieplegers in Nederland op dezelfde wijze afwijken van cyber agressieplegers in de bestudeerde landen (zoals de US en Australië). Meer onderzoek is hier noodzakelijk.

Het belangrijkste aspect waarmee verder rekening gehouden moet worden bij de aanpassing van interventies is het online disinhibitie-effect. Door de anonimiteit van zowel dader als slachtoffer is de beleving van de consequenties van het gedrag bij de daders van online agressie fundamenteel anders dan bij offline agressie. Op dat gebied kunnen de recente ontwikkelingen in virtual reality en serious gaming mogelijk een rol spelen. Met deze technieken lijkt het beter mogelijk jongeren de consequenties van hun gedrag te laten beleven. De effecten van deze technieken zijn echter ook nog maar beperkt getest en zullen ook op maat moeten worden aangepast voor verschillende typen daders, delicten en situaties.

Ook andere aspecten van online disinhibitie zoals de beperktere informele controle en beperkter bewustzijn van de strafbaarheid kunnen gezien worden als aangrijpingspunten voor interventies. Bij de effectieve interventies voor online agressie zijn echter geen aspecten gevonden die zich daar specifiek op richten. Wel worden bij effectieve interventies voor het terugdringen van online agressie in algemene (veelal school) populaties programmadoelen onderscheiden die zich richten op het veranderen van groepsnormen en daarmee het verlagen van de sociale opbrengsten en het verhogen van het bewustzijn over de schade die wordt aangericht.

Om de belevingswereld van de daders te kunnen volgen en te begrijpen onder welke condities het gedrag tot stand komt is het ook hier weer van belang dat ketenpartners en

hulpverlening voldoende kennis opbouwen op cybergebied. Bij het aanpassen van de interventies is het ook hier raadzaam de doelgroep te betrekken.

*Hacking*

Uit de literatuur en expertinformatie over hacking komt als centraal punt naar voren dat interventies tegen crimineel hacken gericht moeten zijn op het voorkomen dat jongeren vanuit de meer 'goedaardige' vormen van hacken (waar ethische motieven of het zoeken naar uitdagingen aan ten grondslag liggen) overgaan naar de zwaardere vormen van illegaal hacken waarbij financieel gewin of macht belangrijke motieven zijn. Daartoe is het van belang dat jongeren in een vroeg stadium bewust worden gemaakt van de schade van hun gedrag en vooral van de consequenties die het gedrag voor de eigen toekomst kan hebben. Omdat de *peergroup* in de hackerscultuur een belangrijk rol speelt, kan de inzet hiervan van belangrijk nut zijn bij het daadwerkelijk bereiken van deze jeugdigen. Zij weten dat snel handelen en in contact blijven me de jeugdige hackers van essentieel belang is en hebben de vaardigheden, middelen en ingangen dat ook te doen. Het is hier echter belangrijk na te denken over eventuele schadelijke effecten, deze werden eerder gezien bij strafrechtelijke interventies voor offline delicten. Bij het tijdig aanspreken van jonge hackers kan in de toekomst wellicht ook gebruik gemaakt worden van geautomatiseerd aanspreken van plegers van antisociaal of illegaal gedrag (digigeren).

Andere vormen van interventies die naar voren zijn gekomen in het onderzoek zijn het versterken van de rol van de ouders in controle en begeleiding van jongeren bij het voorkomen van een criminele hacker carrière. Hoewel het belang van de rol van ouders vaak genoemd wordt in onderzoek en door experts, is uit dit onderzoek niet duidelijk geworden hoe ouders getraind zouden moeten worden en of het wel reëel is te verwachten van ouders dat zij effectief toezicht houden.

Wanneer we naar de rol van de traditionele ketenpartners kijken dan zien we dat hier de capaciteit en in veel gevallen ook de kennis en instrumenten ontbreken om adequaat in te grijpen. Zo is het cyberelement nog niet doorgevoerd in de diagnose instrumenten op basis waarvan adviezen aan OM en rechter worden verstrekt en behandel of begeleidingsplannen worden gemaakt. Veel ketenpartners hebben bovendien maar beperkt zicht op het slachtofferaspect van cyberdelicten en daarmee ook op de feitelijke ernst van het delict. Voor een adequate begeleiding van cybercriminelen door de verschillende keten- en zorgpartners is training gericht op cyberproblematiek van belang. Samenwerking met ethische hackers die veel kennis over de hackercultuur en de ontwikkeling van hacker carrières hebben kan hieraan mogelijk bijdragen.

Verder zijn er diverse technische interventies in ontwikkeling die kunnen helpen bij de handhaving van gedrag na veroordeling. Voorbeelden zijn biofeedback, of wifi-blocking door een armband. Ook van deze interventies is de effectiviteit nog niet bekend maar deze zullen net als geldt voor technische interventies bij offline criminaliteit (denk aan de enkelband) alleen tot blijvende effecten kunnen leiden als ze in combinatie met gedrag veranderende maatregelen worden ingezet die gericht zijn op de aanwezige criminogene factoren.

## 6.5 Discussie

De belangrijkste conclusie uit dit onderzoek is dat er op dit moment nog geen op effectiviteit getoetste interventies beschikbaar zijn voor jeugdige daders van cyberdelicten. Omdat we hier spreken over een relatief nieuw terrein waarop delicten plaatsvinden, is dit niet verrassend. Om de juiste interventies te kiezen en ontwikkelen is het volgens zowel de situationele preventieliteratuur als de dadergerichte 'what works' literatuur belangrijk dat uitgebreid rekening wordt gehouden met de specifieke problematiek die er speelt (bij daders, slachtoffers en met betrekking tot de situatie). Er is dus veel informatie over de problematiek nodig om de juiste interventies te kiezen en ontwikkelen. Studies naar de achtergronden en dynamiek van cybercrime zijn daarom erg belangrijk bij de ontwikkeling van interventies.

Over deze achtergronden is recent meer duidelijk geworden in verschillende studies naar de populatie cyberdaders (zoals beschreven in hoofdstuk 5 van dit onderzoek). Hoewel er uit die studies belangrijke conclusies komen, blijven er ook veel vragen onbeantwoord. Zo blijkt er een grote mate van overeenkomst tussen daders van offline agressie en van online agressie maar is er ook een groep die zich juist onderscheidt door alleen online agressief gedrag te plegen. Het is nog niet goed duidelijk welke elementen ervoor zorgen dat deze groep wel online tot het anti-sociale gedrag komt dat ze offline niet lijken te vertonen. Die kennis is wel van belang voor passende interventies. Het is bijvoorbeeld de vraag of deze jongeren op dezelfde manier reageren op de algemene programma's die nu veel worden ingezet als preventie van cyberagressie (voortkomend uit de traditionele antipest porgramma's).

Ook de variatie in kenmerken van hackers die zich in de verschillende ontwikkelingsfasen bevinden, is een belangrijke bevinding in de literatuur die handvatten geeft voor passende interventies. Tegelijk is er nog maar beperkt in beeld welke risicofactoren bij hackers maken dat zij in de rijpingsfase terechtkomen. Daardoor is ook onduidelijk in welke mate de vergelijking met bestaande levensloopmodellen voor offline criminele carrières en de daar beschreven risicofactoren op gaat. Tevens lijkt de groep hackers die wel van het begin af aan gericht is op financieel gewin of het verwerven van macht over anderen mogelijk nog maar beperkt in beeld. Omdat er steeds gemakkelijker toegang te verkrijgen is tot informatie over en instrumenten voor hacken, neemt deze groep mogelijk toe in omvang en kan de door dit type hackers aangerichte schade ook toenemen.

Daarnaast is het, ook gezien de variatie in kenmerken van daders, belangrijk stil te staan bij de beperkingen in de studies waarin de daderprofielen worden onderzocht. Deze studies hebben namelijk te maken met incomplete registraties als het gaat om het cyberelement in strafrechtelijke systemen en beperkingen in het bereiken van de relevante populaties en de meting van de verschillende (zich snel ontwikkelende) vormen van criminaliteit online bij het uitvoeren van slachtoffer enquêtes. Deze beperkingen zagen wij ook weerspiegeld in de expertmeetings en interviews waar verschillende ketenpartners aangaven deze groep daders nog maar nauwelijks in beeld te hebben. Als het dus gaat om feitelijke strafrechtelijke reacties op daders van cybercrime, is het van belang te investeren in de mate waarin cybercrimedelicten als zodanig herkend worden en bovendien geregistreerd in de strafrechtelijke systemen. Als deze signalering en registratie beter verloopt, kunnen er betere lessen uit de huidige praktijk geleerd worden dan nu.

Een andere beperking van de huidige studies is dat bij de bespreking van achtergrondkenmerken van daders vaak een grote groep daders van verschillende delicten (in type en ernst) samen wordt genomen. Gezien de nadruk in de interventie literatuur op maatwerk bij de (strafrechtelijke) aanpak van criminaliteit is het van belang dat studies in de toekomst meer inzoomen op specifieke vormen of patronen van cybercrime en juist de variatie in problematiek binnen de dadergroepen en in situaties waarin de criminaliteit plaatsvindt in beeld brengen. Evenals de daarmee samenhangende factoren. Vanuit die informatie kunnen vervolgens gerichtere diagnostiek en passende interventies ontwikkeld worden.

In het rapport beschreven we drie preventiestrategieën (voor eerste delicten en recidive van daders) die terug te vinden waren in de beschreven interventies, namelijk: 1) het beperken van toegang of beschikbaarheid van doelen; 2) het opleggen van beperkingen of controle op daders; en 3) het vergroten van de bewustwording bij daders over de gevolgen van het handelen. Het grootste deel van de bestaande interventies voor cyberagressie en stalking richten zich vooral op slachtoffers en omstanders en daarmee op de eerste strategie. Een interessant onderdeel van deze interventies zijn de elementen gericht op het verlagen van de (sociale)opbrengst door het creëren van afkeurende groepsnormen ten opzichte van zowel cyberagressie als illegaal hacken. Daarnaast is er een redelijk aandeel interventies waarin de nadruk ligt op de derde strategie en die inzet op het bewustmaken van daders van de schade die zijn met hun gedrag voor anderen en zichzelf kunnen aanrichten.

De effectieve interventies die de systematische literatuurstudie naar voren bracht, bewegen zich allen in de preventieve sfeer en op het grensgebied tussen niet strafbaar anti-sociaal gedrag en strafbare gedragingen (voornamelijk pesten). Ze zijn gericht op een brede populatie en er is weinig sprake van maatwerk. Dat de programma's toch effectief zijn heeft mogelijk te maken met het feit dat de problematiek waaruit het gedrag voortkomt in deze preventieve fase meer op groepsniveau dan op individueel niveau ligt (zie ook de theorieën achter de antipest programma's). Voor strafrechtelijke reacties op cyberagressie zou het maatwerk op individueel niveau dus wel van belang zijn. Daar lijkt het gebruik maken van bestaande interventies voor gedragsverandering bij daders een goede optie. Daarbij zijn echter wel aanpassingen noodzakelijk waardoor rekening gehouden wordt met belangrijke aspecten die een rol spelen bij cybercrime (i.e. afwijkende daderkenmerken ten opzichte van offline agressie en online disinhibitie). Juist over die kenmerken is zoals hierboven beschreven nog veel onbekend.

Interventies die reageren op hacking moeten volgens de experts in staat zijn tot snel reageren. Alle concreet ontwikkelde (en deels getoetste) interventies hebben een preventief karakter en richten zich op algemene populaties jongeren of (in het geval van hacken) op algemene en heterogene daderpopulaties. De interventies in ontwikkeling die het meest direct op het pleeggedrag inspelen zijn technische interventies zoals digigeren, serious gaming, big data mining, biofeedback, of wifi-blocking. De precieze inhoud die hoort bij een effectieve reactie kan echter nog nauwelijks bepaald worden op basis van bestaand onderzoek. In de preventieve sfeer is het bieden van legale alternatieven die de hackers uitdaging bieden mogelijk een optie, maar ook van dergelijke interventies is weinig bekend over de feitelijke effectiviteit en reikwijdte. Tevens is het zoals hierboven beschreven de vraag of hiermee niet slechts bepaalde groepen hackers bereikt kunnen worden.

We concluderen daarom dat het voor het ontwikkelen van (strafrechtelijke) reacties op daderschap van cybercrime, van belang is beter zicht te krijgen op de mate waarin cybercrimedelicten als zodanig herkend worden en geregistreerd worden in de strafrechtelijke systemen. Vervolgens zou moeten worden uitgezocht hoe nu in de strafrechtpraktijk wordt gereageerd op cybercrime-delicten en of die aanpak inspeelt op de criminogene factoren en responsiviteit van de daders. Naar aanleiding daarvan kan besloten worden: a) welke specifieke interventies eventueel moeten worden aangepast of nieuwe ontwikkeld; b) hoe met het cybercrime aspect moet worden omgegaan in de signalerings- en diagnosefase bij de politie, reclassering en zorgverleners; en c) op welke manier professionals in de keten moeten worden getraind. Pas daarna volgt de fase waarin concrete interventies op hun (mogelijke) effectiviteit kunnen worden onderzocht voor de specifieke doelgroep.

# Summary


## Introduction and research questions

Together with a strong increase in the use of the internet in the past decades, levels of cybercrime also increased strongly. Young people are strongly represented on the internet and research shows they are relatively often offenders of cybercrime. There is, however, limited systematic knowledge available on possible interventions reducing offending risks. This study aims to increase this knowledge in order to facilitate the development of preventive measures against cybercrime offending among young people. Therefore, we study the design, (intended) mechanisms, and effects of cybercrime interventions for young people.

The research questions are:

1. Which interventions can be found in the international literature, aimed at reducing cybercrime offending among young people?
2. In what categories can we organise those interventions with respect to:
   a. The type of cybercrime it treats.
   b. The population it selects.
   c. The underlying theory that explains why it is expected to be effective.
   d. The methods used.
   e. The stakeholders who are involved.
3. What do we know about the program integrity of the interventions?
4. What do we know about the effectivity of the interventions in reducing digitalised crime and cybercrime among youngsters and what study designs were used?
5. How do effective and promising interventions differ from not effective interventions, with respect to characteristics summed up in the second research question?

## Research methods

The research was done in two phases. In *phase 1* we analysed evaluation research of programs for (potential) young offenders of cybercrime as described in the scientific literature. In *phase 2* an in-depth study was held for two types of cybercrime, i.e. cyber aggression and hacking. In this phase we looked beyond the evaluated interventions and searched for insights, experiences, and suggestions in literature and from experts in the field that might be relevant in the development and selection of future interventions.

To find evaluated interventions for (potential) young offenders of cybercrime an extended systematic literature search has been done. This search focused both on sources that specifically concern evaluated interventions for young cybercrime offenders (reduction of re-offending) and evaluated interventions that aim to prevent cybercrime offending in general populations (prevention of cybercrime in general). For the in-depth study on cyber aggression and hacking interventions (phase 2) we used sources from the systematic literature search that did not qualify for phase 1, but that gave background information on offender groups or offending behaviour. Several additional reviews and sources about cyber offender populations have been included too. Next to the literature we also consulted experts (from the field and in research) during expert meetings, interviews and in e-mail conversations. With this

consultation of experts we aimed to collect *up to date* information on recent and innovative interventions as well as reflection on the results from our literature study.

# Results

## Systematic literature review of evaluated programs

Our quest for program evaluations produced studies for 39 different programs. This appeared to be almost exclusively programs designed for general populations. These programs focus on offending prevention for possible offenders instead of re-offending reduction among proven offenders. Moreover, the large majority of preventive programs focussed on the whole system, so these programs also try to change behaviour of (possible) victims and bystanders and not just behaviour of (possible) offenders. Two studies focus on interventions specifically designed for actual offenders, namely the use of *reintegrative shaming* for hackers and of *restorative justice* for *stalking*. Both interventions however were rather approximations than actual and detailed programs. The program evaluations therefore, were content evaluations and could not draw any definite conclusions on actual effects. Below, we discuss the characteristics of the programs found to answer research questions 2 until 4. This section will end in the conclusions that an in-depth study is necessary for the answer on research question 5.

*Type of cybercrime*

The programs from the systematic search focus on the following types of cybercrime:

- cyberagression (10)
- sexting (13)
- hacking (4)

Moreover, eight programs on online safety in general were found in which the offender role was treated explicitly (i.e. creating consciousness about what illegal behaviour is and what consequences this behaviour might have). Finally, we selected evaluations on four technical interventions that are specifically focussed on (potential) offenders. The cyber aggression programs focus mainly on cyberbullying and in one case on stalking. This means that for many types of cyber aggression no programs were found. Moreover, no programs were found for the prevention of financially economical offending in cyberspace.

*Populations selected*

The programs for online safety and cyber aggression, focus in most cases on children and youngsters from primary school and the first stages of secondary school. Sexting programs are aimed at youngsters at secondary schools. The hacking and technical interventions do not mention specific age groups. Most programs select the entire population and not only offenders.

*Theories*

Just for a small part of the programs, theories were described that explain why the program is expected to work. Theories that were most often described are social learning theories, the theory of normative social behaviour, and the theory of planned behaviour. The cyber aggression programs are based in particular on or are remakes of established anti-bullying

programs. These programs especially use system focussed theories in which group norms (descriptive and injunctive) and the impact of such norms on the behaviour of individuals has a central position. For this type of cyber aggression, decreasing the social benefits for offenders, by creating disapproving norms at the group level, will decrease offending risks. The theoretical basis of the *sexting* programs is very limited, the only theoretical notion that is described is deterrence. The hacking programs describe a combination of assumptions derived from the rational choice approach, *reintegrative shaming* and deterrence.

*Methods*

(Psycho)-education and cognitive behavioural methods (including positive enforcement and increased moral reasoning) are methods used frequently in the programs that were evaluated. Role-playing is a tool in those programs to facilitate possible offenders to learn about the norms of others and to train reaction strategies. In several programs training is also used to increase social skills and cognitive and affective empathy. The psycho-education tries to increase knowledge about victim consequences and possible sanctions for the offender. This final strategy is also used in hacking programs however the specific methods used in hacking interventions are poorly described.

*Stakeholders involved*

A sound consequence of the fact that most programs aim at general populations of youngsters is that execution of the programs takes place mainly at schools. Sometimes, lessons are given by teachers themselves, sometimes by external trainers from (privat) companies who often also developed the programs. For some programs it is described that they are, also available in the correctional field but no evaluation studies were found for such use. For one possible effective hacking intervention (the *hack-in-contests*) companies are important parties in the execution of the program.

*Program integrity*

Limited information is available about whether programs turn out the way they should according to the program description. One clear omission in many programs, both in the program descriptions and in practice, is the lack of a central role for activating modules in which the training of skills and interactive learning should take place. As a consequence, both in the translations of known working mechanisms to program descriptions and in the program integrity itself are not sufficiently elaborated. Effects of the programs might become stronger if these elements are better integrated in the programs.

*Effectivity*

Effect studies were available for one third of the programs (13 of 39). These are mainly online safety and cyber aggression programs. For the rest of the programs theoretical evaluations were available that discussed the possible effectivity of the programs by analysing the

descriptions of the programs. Of the 13 effect studies only 4 (3 on cyber aggression and 1 on hacking) had a fully experimental design, another 5 studies had a quasi-experimental design[37]. The cyber aggression programs decrease cybercrime offending to some extent. No effects were found for the programs on online safety, sexting-, and hacking.

*Differences between effective or promising programs and non-effective programs*
Only one type of programs: anti-cyberbullying programs, were found to be effective in the reduction of offending risks. These programs include several success factors for effectivity, like a focus on dynamic criminogenic needs (i.e. group pressure, lack of supervision, and lack of empathy for victims, partly as a result of the online disinhibition-effect), and the [afstemming] of the program at the responsivity of the population at aim (in this case a system approach with clear attention for groupnorms is important). Programs, solely using education or deterrence appear to be not effective.

For many programs no effect studies are available so few firm conclusions can be drawn about the effectivity of the programs studied. Based on content analyses, we have positive expectations about hacking interventions bases on *reintegrative shaming*.

## In-depth study potential interventions

The in depth study in the second phase of our research concerns cyber aggression and hacking and facilitates a somewhat more elaborate answer on research question 5 and as a result insights for effective interventions. Although the answer on this question differs between the two types of cybercrime, a great need for more knowledge and training is present among professionals in dealing with both types of crime. Besides knowledge about the behaviour and circumstances of cyber offenders, professionals should be trained in using technological interventions for supervising and treating young cyber offenders. In the development of interventions, train-the-trainer program should therefore not be forgotten.

*Cyberagression*
The literature shows that young offenders of cyber aggression mainly resemble offline aggression offenders. Existing behavioural programs used by correctional and forensic care institutions (i.e. Aggression regulation treatment or cognitive skills programs) might be effective in reducing the risk of reoffending in cyber aggression. An important difference, however, is that general levels of aggression for offenders of cyber aggression are lower than for offline aggressive offenders. Moreover offenders of cyber aggression are more often victims of online and offline aggression, so motives for offending might be different. Finally, differences were found in characteristics affecting responsivity for interventions like social intelligence.

Another important effect that should be concerned is that of online disinhibition. Because of the anonymity of both offender and victim, the experience of the consequences of the behaviour for offenders might be fundamentally different compared to offline aggression. Possibly, recent developments in *virtual reality* and *serious gaming* can contribute to interventions in which youngster better become aware of the consequences of their behaviour.

[37] Those quasi-experimental design studies have a pre- and post- intervention measurement and compare intervention and control groups. However those groups are not formed by chance as in a real experiment.

Those techniques should however first be tested more elaborately and next be adjusted for different types of offenders, crimes and situations.

*Hacking*

According to both the literature and experts, hacking interventions should not focus on the suppression of hacking behaviour in general, but on preventing that youngsters turn from the more 'bening' types of hakcing to more detrimental types in which financial gains or power are important motives. Hacking interventions aimed at creating consciousness among hackers about the damage they create and the consequences there actions may have for their own future are expected to be the most effective. Offering legal alternatives (hack in contests) in which youngster can find the challenges and sensations might help in preventing illegal and harmful hacking. Among young hackers it is important that reactions on illegal actions are prompt and that controlling actors stay in contact with the offender. Both expert and the literature point at the *peergroup* as an important factor of influence and suggest to give the peergroup an important role in the interventions. There is however, very limited information available about the possibilities and risks of such a role for the peergroup. Automized reactions on hacking behaviour as used in interventions like 'digigeren', may become useful in the future to improve possibilities for prompt reactions on young hackers. Format and content of the message brought with such an intervention appears to be crucial for effectivity. Until now, no effect studies were found supporting effectivity of such automatic warnings.

Finally, various technological interventions are being developed at the moment that might be helpful in supervising offender behaviour after sentencing (i.e. biofeedback, or wifi-blocking in a bracelet). Again, no evaluations of the effectivity of the interventions could be found. Comparable with such interventions for offline crime (like electronic monitoring) we can expect that they will only be effective on the long term if combined with interventions treating the criminogenic needs of offender.

## Conclusions

The most important conclusion of this study is that in scientific literature no descriptions were found of effective interventions being a correctional reaction on actual offending behaviour of young cybercrime offenders. A couple of studies describe methods that can be used in reaction on actual offending (*reintegrative shaming* and *restorative justice*), but most programs are aimed at the prevention of offending in general populations of youngsters. Of all preventive programs, just the anti-cyberbullying programs showed to be effective in the prevention of offending. These programs mainly use system-focussed methods in which building disapproving group norms against cyber aggression and the training of bystanders and victims play an important rol. Besides, the programs focus on improving (potential) offenders' consciousness of the consequences of their behaviour.

Recent studies improved our knowledge on backgrounds and dynamics of cybercrime (see chapter 5). These insights suggest that offline aggressive offender programs can probably be used for cyberaggression offenders too. However, adaptations wil be necessary for considering cybercrime specific factors in the behavior (i.e. different offender characteristics compared to offline aggression and online disinhibition). Interventions that respond to hacking should be capable to give prompt reactions. The specific content that effective reactions should

have, is however still unclear. In the preventive sphere, offering legal alternatives that challenge hackers may be a possible effectieve strategy, but again little is known about effectivity and scope of such interventions.

An important comment is that both in the population of cyberagression offenders and of hackers a wide variation in offender characteristics exists. Moreover, both populations appear to have subgroups we know only little about. For aggression we know that offline and online aggression often comes together in the same persons. However there is a group online aggressive offenders who only offend online. It is still unclear which criminogenic needs this group has. The same is the case for hackers who have financial gains or power as the core motivation for offending from the start of their hacking career on. Those offenders are not hacking with the samen motivations as the often described *eager* and *sensation seeking* secundary school student who attains step by step into a criminal hacker.

The final conclusion of the study therefore is that for the development of (correctional) reactions toward offenders of cybercrime, it is important to further improve the knowledge about the group. As a part of this job it would be relevant to study how well cybercrime offenders are recognized and registrated in the correctional system at the moment. Next, we should describe in more detail how the correctional system reacts on these cybercrime offenders and to what extent this reaction answers to the criminogenic needs and responsivity of the offender. As a result of this exercise, it can be decided which specific interventions can be used or should be developed, how to deal with the cyberelement in signaling an diagnosing by police and (youth)probation services, and (forensic) care, and how professionals should be trained.

# Literatuurlijst


Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health*, *57*(1), 10-18.

Aiken, M., Davidson, j., & Amann, D. (2016, oktober). *Youth pathways into cybercrime*. Europol: European cybercrime Centre/ UCD Geary institute for public policy / Middlesex University.

Albin, K. A. (2012). Bullies in a wired world: The impact of cyberspace victimization on adolescent mental health and the need for cyberbullying legislation in Ohio. *JL & Health*, *25*, 155.

Andrews, D., Bonta, J., & Hoge, R. (1990). Classification for effecctive rehabilitation: Rediscovering psychology. *Criminal Justice and Behavior, 17*(1), 19-52.

Andrews, D. & Dowden, C. (2005). Managing correctional treatment for reduced recidivism: A meta-analytic review of program integrity. *Legal and Criminological Psychology, 10*(2), 173-187.

Árpád, I. (2013). A greater involvement of education in fight against cybercrime. *Procedia-Social and Behavioral Sciences*, *83*, 371-377.

Baas, N. (2010). *Want soms zijn kinderen gewoon de experts: Een participatief onderzoek naar het perspectief van 11-en 12-jarigen op het verschijnsel cyberpesten en naar manieren om het verschijnsel terug te dringen* (Master's thesis, University of Twente).

Baas, N., De Jong, M.D.T. & Drossaert, H.C. (2013). Children's perspectives on cyberbullying: Insights based on participatory research. *Cyberpsychology, behavior and social networking 16*(4). 248-254

Bachmann (2011) Deciphering the Hacker Underground: First Quantitative Insights. *Corporate hacking and technology-driven crime: Social dynamics and implications*, 105-126

Barlow, J.P (1996). A declaration of the independence of cyberspace. Opgehaald van https://www.eff.org/cyberspace-independence

Braithwaite (1989). Crime, shame and reintegration. Melbourne. Cambridge University Press.

Bossler, A. M., & Burruss, G. W. (2011). The general theory of crime and computer hacking: Low self-control hackers. *Corporate hacking and technology-driven crime: Social dynamics and implications*, 38-67.

Brenner, S. W. (2004). Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology, 9*(13), 1-52.

Broekman, C., Wetzer, I., Wijn, R., & Roelofs, M. (2014). *Experimentenopzet: Digigeren tegen doodsbedreigingen.* TNO-Rapport.

Brown (2003) *Community Policing on the Internet*. SANS Institute.

Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011, October). Crowdroid: behavior-based malware detection system for android. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, 15-26.

Camerman, M (2013). *De aanpak van cyberpesten bij jongeren door de (lokale en federale) politie.* Masterproef, faculteit politieke en sociale wetenschappen Universiteit Antwerpen.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social &*

*Legal Studies, 10*(2), 229-242

Clarke, R. (2009). Situational crime prevention: Theoretical background an current practice. In M. Krohn, A. Lizotte, & G. Hall, *Handbook on crime in deviance* (pp. 259-276). NewYork: Springer.

Centraal Bureau voor de Statistiek (2014, 05 27). Opgehaald van CBS: https://www.cbs.nl/nl-nl/nieuws/2014/22/jongeren-vooral-online-met-smartphone

Centraal Bureau voor de Statistiek (2016a) *Veiligheidsmonitor 2015*. Den Haag, CBS.

Centraal Bureau voor de Statistiek (2016b) *Jaarrapport 2016 landelijke jeugdmonitor*. Den Haag, CBS.

Chisholm, J. F. (2014). Review of the status of cyberbullying and cyberbullying prevention. *Journal of information systems education*, *25*(1), 77-87.

DeMitchell, T.A. & Parker-Magagna, M. (2011). Student victims or student criminals? The bookends of sexting in a cyber world. *Cardozo Public Law, Policy & Ethics Journal, 10*(1), 1-41.

De Cuyper & Weijters (2016). *Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationae Veiligheidsindex.* Den Haag: WODC. Opgeroepen op Juli 25, 2016, van https://www.wodc.nl/onderzoeksdatabase/2623b-cybercrime-in-de-nationale-veiligheidsindex-2015.aspx?cp=44&cs=6800

De Troyer, O., Van Broeckhoven, F., & Vlieghe, J. (2017). Linking serious game narratives with pedagogical theories and pedagogical design strategies. *Journal of Computing in Higher Education*, 1-25.

DeSmet, A., Van Cleemput, K., Bastiaensens, S., Poels, K., Vandebosch, H., Malliet, S., & De Bourdeaudhuij, I. (2016). Bridging behavior science and gaming theory: using the intervention mapping protocol to design a serious game against cyberbullying. *Computers in Human Behavior*, *56*, 337-351.

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1).

Dredge, R., Gleeson, J. F., & de la Piedad Garcia, X. (2014). Risk factors associated with impact severity of cyberbullying victimization: a qualitative study of adolescent online social networking. *Cyberpsychology, behavior, and social networking*, *17*(5), 287-291.

Eisenberg, N., Cumberland, A., Guthrie, I. K., Murphy, B. C., & Shepard, S. A. (2005). Age Changes in Prosocial Responding and Moral Reasoning in Adolescence and Early Adulthood. *Journal of Research on Adolescence : The Official Journal of the Society for Research on Adolescence*, 15(3), 235–260. http://doi.org/10.1111/j.1532-7795.2005.00095.x

Esbenshade, P. W. (2002). Hacking: Juveniles and Undeterred Recreational Cybercrime. *J. Juv. L.*, *23*, 52.

Evers, J. (2015). *Kwalitatief interviewen: kunst én kunde*. Amsterdam: BoomLemma

Fischer, T.F.C. (2015) Erkende gedragsinterventies voor volwassen justitiabelen in Nederland. *Panopticon*, 2015, 3 pp. 158-172.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal Computer Virol, 2*, 13-20.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies,*

*10*(2), 243–249.
Facer, K, & Furlong R. (2001). Beyond the myth of the 'cyberkid': Young people at the margins of the information revolution. *Journal of Youth Studies, 4*(4), 451-469.
Fahey, E. (2014). The EU's cubercrime and cyber-security rule-making: Mapping the internal and external dimensions of EU security. *Forthcoming European Journal of Risk Regulation, 1*, 1-20.
Fischer, F., & Zwirs, B. (2013). Erkende Gedragsinterventies. In A. Menger, E. Krechtig, & J. Bosker, *Werken in gedwongen kader, Methodiek voor het forensisch sociaal werk.*
France, K., Danesh, A., & Jirard, S. (2013). Informing aggression–prevention efforts by comparing perpetrators of brief vs. extended cyber aggression. *Computers in Human Behavior*, *29*(6), 2143-2149.
Hemphill, S. A., & Heerde, J. A. (2014). Adolescent predictors of young adult cyberbullying perpetration and victimization among Australian youth. *Journal of Adolescent Health*, *55*(4), 580-587.
Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1–24.
Hoek van Dijke, N. (2016). Onderzoeksrapportage: Jongeren over cybercrime en gedigitaliseerde criminaliteit. *Ministerie van Veiligheid en Justitie*
Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.
Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *Amikan Journal Criminal Justice, 37*, 378–395.
Jäger, T., Amado, J., Matos, A., & Pessoa, T. (2010). Analysis of Experts' and Trainers' Views on Cyberbullying. *Australian Journal of Guidance and Counselling, 20*(2), 169-181. doi:10.1375/ajgc.20.2.169
Jansen, J., Junger, M., Montoya, L., Hartel, P., Stol, W. P., & Jansen, J. (2013). Offenders in a digitized society. *by WP Stol and J. Jansen. Safety & Security Studies. The Hague, The Netherlands: Eleven International Publishing*, 45-59.
Janssen, J. (2015). De stekker eruit? Over de relatie tussen cybercrime en geweld in afhankelijkheidsrelaties. *Proces*, *5*(94), 318-328.
Jones, B.R. (2007). Virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law and Criminology, 97*(2), 601-630.
Juvonen, J., & Gross, E. F. (2008). Extending the school grounds?—Bullying experiences in cyberspace. *Journal of School health*, *78*(9), 496-505.
Katz, J. (1996, July). The rights of kids in the digital age. Opgehaald van http://www.wired.com/1996/07/kids-2/
Kao, D.-Y., Fu-Yuan Huang, F., & Wang, S.-J. (2009). Persistence and desistance: Examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law & Security Review, 25*, 464-476.
Kerstens, J. & Stol, W. Ph. (2012). Jeugd en cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren. Den Haag: Boom Lemma Uitgevers.
Kiriakidis, S. P., & Kavoura, A. (2010). Cyberbullying: A review of the literature on harassment through the internet and other electronic means. *Family & community health*, *33*(2),

82-93.

Kokkinos, C. M., Antoniadou, N., Asdre, A., & Voulgaridou, K. (2016). Parenting and internet behavior predictors of cyber-bullying and cyber-victimization among preadolescents. *Deviant Behavior*, *37*(4), 439-455.

Korvorst, M., & Sleijpen, G. (2014). Jongeren vooral online met smartphone. *Webmagazine*. Opgeroepen op Augustus 25, 2016, van https://www.cbs.nl/nl-nl/nieuws/2014/22/jongeren-vooral-online-met-smartphone.

Kubiszewski, V., Fontaine, R., Potard, C., & Auzoult, L. (2015). Does cyberbullying overlap with school bullying when taking modality of involvement into account? *Computers in human behavior*, *43*, 49-57.

LeBlanc, M., & Loeber, R. (1998). Developmental criminology updated. In *M. Tonry (Ed.), Crime and Justice, volume 23* (pp. 115-198). Chicago: University of Chicago Press.

Leukfeldt, E. R., Domenie, M. M. L., & Stol, W. Ph. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische Uitgevers.

Leukfeldt, R., Kentgens, A., Prins, E., & Stol, W. (2015). *Allerdaags politiewerk in een gedigitaliseerde wereld. Handreiking voor de intake van delicten met een digitale component.* Lecotoraat Cybersafety.

Leukfeldt, R. & Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 36(3)*, p.263-280.

Lipsey, M. & Cullen, F. (2007). The effectiveness of correctional rehabilitation: A review of systematic reviews. *Annual Review of Law andd Social Science, 3*, 297-320.

Louk, M., Lim, H., & Lee, H. (2014). An analysis of security system for intrusion in smartphone environment. *The Scientific World Journal*

Lowenkamp, C., Latesssa, E., & Holsinger, A. (2006). The risk principle in action: What have we learnd from 13,676 offenders and 97 correctional programs. *Crime & Delinquency, 52*(1), 77-93.

Madarie, R. (2017). Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International Journal of Cyber Criminology. Vol. 11(1):* 78–97. DOI: 10.5281/zenodo.495773.

Matza, D. (1969). *On Becoming Deviant*. Englewood Cliffs, NJ: Prentice Hall.

Mesch, G.S (2012). Technology and youth. New directons for youth development, *135*, 97-105.

Mitchell, K. J., Ybarra, M. L., Jones, L. M., & Espelage, D. (2016). What features make online harassment incidents upsetting to youth? *Journal of school violence*, *15*(3), 279-301.

Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online Victimization in understanding depression, delinquency, and substance use. *Child maltreatment,* 12(4), 314-324.

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

Morris, R.G., (2011). Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. *Corporate hacking and technology-driven crime: Social dynamics and implications*, 1-17.

Mouton, F., Leenen, L., & Venter, H.S., (2016). Social Engineering Attack Examples, Templates and Scenarios. Preprint submitted to Computers & Security, March 29 2016.

Nationale Politie (zonder datum) *Politie en schoolveiligheid. Visie en Ambitie*. Beleidsdocument.

NCSC (2013).Leidraad om te komen tot een praktijk van Responsible Disclosure. Opgehaald op: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

Noonan, B. (2010). Crafting Legislation to Prevent Cyberbullying: The Use of Education, Reporting, and Threshold Requirements. *J. Contemp. Health L. & Pol'y*, *27*, 330.

Oberoi, S. (2014). *Androsat: Security analysis tool for android applications* (Doctoral dissertation, Concordia University).

Olweus, D., & Limber, S. P. (2010). Bullying in school: evaluation and dissemination of the Olweus Bullying Prevention Program. *American Journal of Orthopsychiatry*, *80*(1), 124.

Pabian, S., & Vandebosch, H. (2014). Using the theory of planned behaviour to understand cyberbullying: The importance of beliefs for developing interventions. *European Journal of developmental psychology*, *11*(4), 463-477.

Pereira, G., Brisson, A., Prada, R., Paiva, A., Bellotti, F., Kravcik, M., & Klamma, R. (2012). Serious games for personal and social learning & ethics: status and trends. *Procedia Computer Science*, *15*, 53-65.

Pontell, H. N., & Rosoff, S. M. (2009). White-collar delinquency. *Crime Law Soc Change, 51*, 147–162.

Rokven, J., Weijters., G., & Van der Laan, A.M (2017). *Jeugddelinquentie in de virtuele wereld: Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?* Ministerie van Veiligheid en Justitie: WODC.

Ruiter, S. & Benaards, F (2013). Verschillend ecrackers van andere criminelen? Een vergelijking op basis van Nederlandse verdachtenregistraties. *Tijdschrift voor Criminologie 4*(55). 342-359

Schermer, B. W. & Lodder, A. R. (2014). Internet Governance: An Introduction. Hoofdstuk 1 in: *The Handbook on ICT Law.* (Recht en Computer), Deventer: Kluwer, 1-23.

Schilder, J.D., Brusselaers, M.B.J., & Bogaerts, S. (2016). The effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. *Journal of Youth and Adolescence, 45*, 286-300.

Scholten, Nelen, de Wit en Kroes (2016). *Sociale veiligheid in en rond scholen.* Praktikon b.v.

Skinner, W. F. & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Crime and Delinquency 34*, 495-518.

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies, 10*(2), 251–256.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321-326.

Sykes, G. M. & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Turgeman-Goldschmidt, O. (2008), Meanings that hackers assign to their being a hacker.*International Journal of Cyber Criminology*, 2(2), 382-396.

Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders*. Boom Juridische uitgevers.

Vandebosch, H. & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New media & society*, *11*(8), 1349-1371.

Van der Broek, T. C., Weijters, G., & Van der Laan, A. M. (2014). *Factsheet: Antisociaal gedrag van jongeren online.* Ministerie van Veiligheid en Justitie: WODC.

Van der Laan & Goudriaan. (2016). Jeugdcriminaliteit in de periode tussen 1997-2015. *Monitor Jeugdcriminaliteit.* WODC/CBS. Cahier 2016-1

Van der Wagen, Althoff, Van Swaaningen (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift voor Cultuur en Criminaliteit, 1*(6), 27-41

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

Warr, M. (2002). *Companions in Crime. The social aspects of criminal conduct.* New York: Cambridge University Press.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64-74

Yar, M. (2005). The novelty of 'cybercrime': an assessment in light of routine activity theory. *European Journal of Criminology, 2*, 407-427.

Yar, M. (2012). Sociological and criminological theories in the information era. In W. Stol, & R. Leukfeldt, *Cyber-Safety: An Introduction* (pp. 45-56). Utrecht: Eleven Interantional Publishing.

Zebel, S., De Vries, P., Griebels, E., Kuttschreuter, M., & Stol, W. (2013). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning .* Enschede: WODC/Universiteit Twente.

## Literatuurlijst: Bronnen interventies


Beavis, C., Deagon, J., Merten, A., Muspratt, S., Pendergast, D., Reynolds, J., . . . Waqailiti, L. (2011). *The ACMA cybersmart outreach program evaluation*. Griffith Institute for Educational Research for the Australian Communications and Media Authority.

Chaux, E., Velásquez, A.M., Schultze-Krumbholz, A., & Scheithauer, H. (2016).Effects of the cyberbullying prevention program Media Heroes (*Medienhelden*) on traditional bullying. *Aggressive Behavior, 42*, 157-165.

Chessor, D. (2008). Developing student wellbeing and resilience using a group process. *Educational & Child Psychology, 25*(2), 82-90.

Chibnall, S., Wallace, M., Leicht, C., & Lunghofer, L. (2006). *I-SAFE evaluation*. Virginia: Caliber, an ICF Consulting Company.

Chou, C.-H., Sinha, A.P., & Zhao, H. (2010). Commercial Internet filters: Perils and opportunities. *Decision Support Systems, 48,* 521-530.

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., Barnes, A. (2016). Longitudinal impact of the Cyber Friendly School Program on adolescents' cyberbullying behavior. *Aggressive Behavior, 42*, 166-180.

Cuffy, S.A. (2015). *Principals' perceptions of the Bully Busters Program in combating cyberbullying in elementary schools* (doctoral dissertation). Walden University, Minneapolis.

Davidson, J., Martellozzo, E., & Lorenz, M. (2009). *Evaluation of CEOP ThinkUKnow internet safety programme and exploration of young people's internet safety knowledge* (Report No. 2). Londen: Kingston University.

Del Rey, R., Casas, J.A., & Ortega, R. (2012). El programa ConRed, una práctica basada en la evidencia: The ConRed program evidence-based practice. *Revista Científica de Educomunications, 39,* 129-138.

Del Rey, R., Casas, J.A., & Ortega, R. (2016). Impact of the ConRed Program on different cyberbullying roles. *Aggressive Behavior, 42*, 123-135.

De Mitchell, T.A. & Parker-Magagna, M. (2011). Student victims or student criminals? The bookends of sexting in a cyber world. *Cardozo Public Law, Policy & Ethics Journal, 10*(1), 1-41.

Doane, A.N., Kelley, M.L., & Pearson, M.R. (2016). Reducing cyberbullying: A theory of Reasoned Action-Based Video Prevention Program for college students. *Aggressive Behavior, 42*, 126-146.

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1).

Gradinger, P., Yanagida, T., Strohmeier, D., & Spiel, C. (2015). Prevention of cyberbullying and cyber victimization: Evaluation of the ViSC Social Competence Program. *Journal of School Violence, 14*(1), 87-110.

Gradinger, P., Yanagida, T., Strohmeier, D., & Spiel, C. (2016). Effectiveness and sustainability of the ViSC Social Competence Program to prevent cyberbullying and cyber-victimization: Class and individual level moderators. *Aggressive Behavior, 42*, 181-193.

Halder, D. (2015). Cyber stalking victimization of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives. *Temida*, 103-130.

Jones, B.R. (2007). Virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law and Criminology, 97*(2), 601-630.

Jones, L.M., Mitchell, K.J., & Walsh, W.A. (2012) *Evaluation of internet child safety materials used by ICAC task forces in school and community settings.* NJI Evaluation rapport. Durham: Crimes Against Children Research Center.

Jones, L.M., Mitchell, K.J., & Walsh, W.A. (2014a). *A content analysis of youth internet safety programs: Are effective prevention strategies being used?* Durham: Crimes Against Children Research Center.

Jones, L.M., Mitchell, K.J., & Walsh, W.A. (2014b). *A Systematic Review of Effective Youth Prevention Education*. Crimes against children research centre.

Kao, D.-Y., Fu-Yuan Huang, F., & Wang, S.-J. (2009). Persistence and desistance: Examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law & Security Review, 25*, 464-476.

Karaian, L. (2013). Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. *Theoretical Criminology, 0*(0), 1-18.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2013). Restrictive deterrent effects of a warning banner in an attacked computer system. *American Society of Criminology, 52*(1), 33-59.

Menesini, E., Nocentini, A., & Palladino, B.E. (2012). Empowering students against bullying and cyberbullying: Evaluation of an Italian peer-led model. International Journal of Conflict and Violence, 6(2), 314-321.

Navarro, R., Ruiz-Oliva, R., Larrañaga, E., & Yubero, S. (2015). The impact of cyberbullying and social bullying on optimism, global and school-related happiness and life satisfaction among 10-12-year-old schoolchildren. *Applied Research Quality Life, 10*, 15-36.

Palladino, B.E., Nocentini, A., & Menesini, E. (2016). Evidence-based intervention against bullying and cyberbullying: Evaluation of the NoTrap! Program in two independent trials. *Aggressive Behavior, 42*, 194-206.

Roberto, A.J., Eden, J., Savage, M.W., Ramos-Salazar, L., & Deiss, D.M. (2014). Outcome evaluation results of school-based cybersafety promotion and cyberbullying prevention intervention for middle school students. *Health Communication, 29*(10), 1029-1042.

Salmivalli, C., Kärmä, A., & Poskiparta, E. (2011). Counteracting bullying in Finland: The KiVa program and its effects on different forms on being bullied. *International Journal of Behavioral Development, 35*(5), 405-411.

Schultze-Krumbholz, A., Schultze, M., Zagorscak, P., Wölfer, R., & Scheithauer, H. (2016). Feeling cybervictims' pain – The effect of empathy training on cyberbullying. *Aggressive Behavior, 42*, 147-156.

Wible, B. (2003). A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. *The Yale Law Journal, 112*(1577), 1577-1623.

Williford, A., Elledge, C., Boulton, A.J., DePaolis, K.J., Little, T.D., & Salmivalli, C. (2013). Effects of the KiVa Antibullying Program on cyberbullying and cybervictimization frequency among Finnish youth. *Journal of Clinical Child & Adolescent Psychology, 42*(6), 820-833.

Winegust, A.K. (2015). *Pass it On: An evaluation of sexualized violence prevention program for middle school and high school students* (doctoral dissertation). University of Toronto, Toronto.

Wishart, J., Andrews, J., & Ching Yee, W. (2005). *Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005.* Bristol: Childnet International.

Wishart, J.D., Oades, C.E., & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education, 48*, 460-473.

Wölfer, R., Schultze-Krumbholz, A., Zagorscak, P., Jäkel, A., Göbel, K., & Scheithauer, H. (2013). Prevention 2.0: Targeting cyberbullying @ school. *Society for Prevention Research, 15*, 879-887.

Wood, R.H. (2010). The first amendment implications of sexting at public schools: A quandary for administrators who intercept visual love notes. *Journal of Law and Policy*, 18(2), 701-737.

## Bijlagen

Vanwege de omvang zijn de bijlagen opgenomen in een apart document. Dit document bevat de volgende bijlagen:

Bijlage 1 Samenstelling van de begeleidingscommissie
Bijlage 2 Zoektochten
Bijlage 3 Tabellen met interventies
Bijlage 4 Achtergrondinformatie selectie delicten verdiepingsstudie