Universiteit Twente, Enschede

Masterthese

Probleemverkenning 'Cybercrime & Jeugd'

Een kwalitatief onderzoek naar de verschillende vormen van cybercriminaliteit gepleegd door jongeren tot 18 jaar, en hun achtergrondkenmerken, motieven en criminele carrières.

Auteur: K. Egberink (s1016261)
Begeleiders: P. de Vries
M. Kuttschreuter
Opleiding: Psychologie
Richting: Master Conflict, Risico & Veiligheid
Juli 2013

Inhoud

Voorwoord

In Oktober 2012 ben ik begonnen met mijn afstudeeronderzoek voor de Master Conflict, Risico & Veiligheid aan de Universiteit Twente. In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is er onderzoek gedaan naar cybercrime en jeugd. Aangezien vooral de jongere generatie een risicogroep vormt voor cybercriminaliteit, maar hier nog wel veel onduidelijkheid over is, bestaat er bij het Justitieel Jeugdbeleid van het ministerie van Veiligheid en Justitie de behoefte aan een beter inzicht in de betrokkenheid van jongeren tot 18 jaar bij cybercriminaliteit.

Dit onderzoek heeft zich dan ook zowel gericht op de verschillende vormen van cybercrime waar jongeren tot 18 jaar bij zijn betrokken als de achtergronden en motieven van jongeren die cybercriminaliteit plegen. Daarnaast wordt er ook nog gekeken of jongeren criminele carrières aan het opbouwen zijn of dat het misschien wel eenmalig is.

Hierbij wil ik de gehele onderzoeksgroep, S. Zebel, E. Giebels, P.W. de Vries, M. Kuttschreuter en L.D. Slot bedanken voor de samenwerking en begeleiding. Daarnaast nog een extra dank voor P.W. de Vries en M. Kuttschreuter, mijn begeleiders, want dankzij hun adviezen en ondersteuning is deze scriptie tot stand gekomen.

Samenvatting

Vanwege het feit dat cybercrime in een aantal jaren uitgegroeid is tot een verschijnsel waarmee iedere computergebruiker bijna dagelijks wordt geconfronteerd en waarbij jongeren een risicogroep vormen, is het belangrijk dat er meer inzicht wordt verkregen in de betrokkenheid van jongeren tot 18 jaar bij cybercriminaliteit in Nederland. Met meer inzicht kan de directie Justitieel Jeugdbeleid een beleid opstellen om de betrokkenheid van jongeren bij cybercrime te voorkomen dan wel aanpakken.

Middels analyseren van zaken in de database rechtspraak.nl (N=47)en het afnemen van interviews (N=10) bij belangrijke sleutelfiguren binnen dit onderwerp, is in deze studie getracht te achterhalen welke vormen van cybercriminaliteit veelal worden gepleegd door jongeren tot 18 jaar en of er mogelijk bepaalde achtergrondkenmerken en motieven kenmerkend zijn voor die groep. Tevens is er gekeken of er sprake is van het opbouwen van een criminele carrière of dat jongeren dit eenmalig doen.

Uit het onderzoek is gebleken dat jongeren meer betrokken zijn bij vormen van cybercriminaliteit in ruime zin, zoals sexting, kinderporno en bedreiging. Wanneer jongeren wel betrokken zijn bij cybercrime in enge zin dan betreft dit over het algemeen Ddos aanvallen en hacken. Een reden waarom jongeren minder bij cybercrime in enge zin betrokken zouden zijn is dat dit vaak een meer georganiseerde vorm van cybercriminaliteit is die ook veel geld kost. Wat betreft combinaties tussen cybercrime in enge zin en ruime zin of cybercrime in enge zin en offline criminaliteit zijn er niet gevonden. Daarentegen komen combinaties van cybercrime in ruime zin en offline criminaliteit wel voor onder jongeren. Zo kan het zijn dat wanneer een delict begint op internet dit op straat verder wordt uitgevochten of andersom.

Verder is gebleken dat er geen prototype dader kan worden vastgesteld. Zo is het lastig te achterhalen welke achtergronden nu een rol spelen bij jongeren die cybercriminaliteit plegen. Wel bleek dat als er iets over werd benoemd dit achtergrondkenmerken waren betreffende (licht) autistische trekken, emotionele en cognitieve achterstand en een laag IQ.

Eveneens vallen er geen conclusies te trekken over de criminele carrières van de jongeren die cybercrime plegen. Dit vanwege het feit dat er op rechtspraak.nl vrijwel niets over wordt benoemd, maar ook vanwege het feit dat cybercriminaliteit bij de politie vaak niet zo wordt geregistreerd, volgens geïnterviewden. Ze registreren het vaak als gewoon bedreiging en dus niet via internet.

Niettemin zijn er wel overeenkomsten in motieven, die uit rechtspraak.nl naar voren zijn

gekomen en uit de interviews. Motieven voor het plegen van cybercrime kunnen zijn: wraak, jaloezie, erbij willen horen, en macht.

Tenslotte is er uit de resultaten ook naar voren gekomen dat er nog specifieke risico's volgen uit het digitale gedrag van jongeren. Zo is er een verwevenheid tussen daders en slachtoffers. Slachtoffers kunnen ook daders worden, waardoor de maatschappelijke schade groter wordt. Daarnaast gedragen een aantal jongeren zich strafbaar zonder dat zij het weten, maar wanneer ze dan gepakt worden heeft dit een negatief effect op hun latere leven, zoals zoeken van werk. Jongeren zullen dus vroegtijdig bewust moeten worden gemaakt van hun (strafbare) gedrag op het internet. Niettemin zijn er ook jongeren die wel weten dat zij strafbaar zijn, maar zij weten dat de pakkans laag is en zullen dan ook doorgaan met hun handelingen. Daarbij ontwikkelen zij steeds meer tactieken en kunnen ook steeds meer schade gaan aanrichten. Dit kan volgens geïnterviewden voorkomen worden door niet de strafmaat te verhogen maar de pakkans te vergroten.

Abstract

Due to the fact that cybercrime in a number of years, has become a phenomenon that every computer user almost daily is confronted with and where young people are at risk, is it important that there is more insight in the involvement of young people up to 18 years in cybercrime in the Netherlands. With better understanding, the management Judicial Youth Policy draw up a strategy to prevent or tackle involvement of young people in cybercrime.

Through analysis of cases in the database rechtspraak.nl (N = 47) and interviews (N = 10) with important key figures within this topic, is obsolete in this study which forms of cyber crime are committed by young people under 18 and whether certain background characteristics and motives are characteristic of that group. There is also examined whether there is a case of a criminal career or that young people do this once.

The study found that young people are more involved in forms of cyber crime in the broad sense, like sexting, child pornography and threats. When young people are involved in cyber crime in the strict sense, this relates generally DDoS attacks and hacking. A reason why young people would be less involved in cyber crime in the strict sense is that this is often a more organized form of cybercrime and it is also costly. Beside that there are no combinations found of cybercrime in the strict sense and broad sense or cybercrime in the strict sense and offline crime. In contrast combinations of cybercrime in the broad sense and offline crimes do occur among young people. It may be that when an offense begins on the internet this is further fought out on the street or vice versa.

Furthermore the results also show that there is no prototype perpetrator. So is it difficult to determine which backgrounds of young people play a role in who commit cybercrime. It was apparent that if something was appointed on this background characteristics, it concerned (light) autistic traits, emotional and cognitive delays and a low IQ.

Also on criminal careers there can be no conclusions drawn. This is due the fact that there is virtually nothing appointed out in rechtspraak.nl, but also because of the fact that cybercrime is often not recorded as to the police, according to interviewees. For example, they often just register it as a threat, but not over the internet. Therefore it is difficult to say whether they give it up or continue if they have received a community service.

Nevertheless, there are similarities in motifs that have emerged from rechtspraak.nl and the interviews. Motives for committing cybercrime can be: revenge, jealousy, wanting to belong with a group, and power.

Finally, the results also show that there are specific risks that follow from the digital

behavior of young people. There is a close relationship between perpetrators and victims. Victims can also become perpetrators, causing to increase social damage. In addition, a number of young people behave criminal without knowing it, but when they are caught they do not realize it has negative consequences on their later life, such as job search. Therefore young people will have to be made early aware of their (criminal) behavior on the internet. Nevertheless, there are also young people who know that they behave illegal, but they know that the chances of being caught are low and they will therefore continue with their operations. In addition, they are increasingly developing tactics and also damage more and more. According tot interviewees this can be prevented by not increasing the sentence but through increasing the probability of detection.

Inleiding

Tegenwoordig vervullen ICT (Informatie en Communicatie Technologie) toepassingen een prominente rol in het dagelijks leven. Zo zijn iPads en smartphones gebruikelijke middelen geworden om op zoek te gaan naar nieuwe informatie, zich te vermaken, of te communiceren met leeftijdsgenoten. Uit cijfers van het CBS blijkt dan ook dat tussen de 75% en 84% van de jongeren tussen de 12 en 15 jaar dagelijks gebruik maakt van internet. Het internet is dus uitgegroeid tot een steeds populairder medium onder jongeren (Van Rooij & Van den Eijnden, 2007; Kowalski, Limber & Agatston, 2008). Doordat ICT een grote rol speelt in het dagelijks leven van de jongeren worden zij vaak aangeduid als de digitale generatie (De Haan, Van t'Hof & Van Est, 2006; Schols, Duimel, & De Haan, 2011). Tevens maakt het vele gebruik van ICT, door jongeren, dat deze ook in toenemende mate een rol spelen bij illegale en strafbare activiteiten. Zo kan internet bijvoorbeeld worden gebruikt om fraude te plegen, kinderporno te verspreiden of anderen te treiteren (Leukfeldt, Domenie en Stol, 2010). Hierbij kunnen jongeren zowel het slachtoffer als de pleger van het delict zijn.

Delicten waarbij ICT een rol speelt worden geschaard onder de noemer 'cybercrime'. Cybercrime, in al zijn vormen, is dagelijks in het nieuws. Meer en meer incidenten vinden plaats en het beeld tekent zich af dat cybercrime een prominente rol zal blijven spelen in onze maatschappij. Sommige mensen breken digitaal in om geld of kennis te verkrijgen, terwijl anderen digitaal in breken vanwege activistische ideeën. Weer anderen versturen sekstapes via internet om zodoende mensen af te persen of om wraak te nemen.

Cybercrime is dus een overkoepelend begrip. Cybercrime wordt ook wel beschreven als "criminaliteit op of via het internet" (NCSC, 2012). Toch wordt er in deze beschrijving geen rekening gehouden met het misbruik dat ook van binnenuit kan plaatsvinden of betrekking kan hebben op ICT-voorzieningen die niet op het internet zijn aangesloten. Een bredere definitie omvat vormen van criminaliteit die betrekking hebben op, of gepleegd zijn met, computersystemen, inclusief telecommunicatienetwerken. De criminele activiteiten kunnen zijn gericht tegen personen, eigendommen en/of organisaties of elektronische telecommunicatienetwerken en computersystemen. In navolging van het KLPD wordt in dit onderzoek cybercrime gedefinieerd als: '*Cybercrime omvat elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.'*

In dit onderzoek wordt er tevens onderscheid gemaakt tussen cybercrime in enge zin en –ruime zin. Onder *cybercrime in enge zin* verstaan we strafbare gedragingen die niet zonder

tussenkomst of gebruik van ICT gepleegd hadden kunnen worden. Kenmerkend is dat de ICT structuur zelf en de daarin of daarmee opgeslagen gegevens het doel van de actie zijn (Hulst & Van der Neve, 2008). Om te spreken over cybercrime in enge zin moeten ICT-middelen dus het voornaamste doelwit zijn of moet de daad niet zonder het misbruiken van ICT-voorzieningen kunnen worden uitgevoerd.

Onder *cybercrime in ruime zin* worden strafbare gedragingen verstaan die met behulp van of via ICT worden uitgevoerd. ICT-middelen of digitale technieken worden hierbij als ondersteuning gebruikt voor het plegen van anderszins traditionele criminaliteit (Hulst & Van der Neve, 2008).

Wanneer er specifiek wordt gekeken naar vormen van online delinquent gedrag van jonge daders dan blijkt er uit onderzoek van Leukfeldt et al. (2010) dat meer dan de helft van de verdachten van e-fraude in de leeftijdscategorie van 12-24 jaar valt. Bij haatzaaien op internet is 60,5% van de verdachten uit deze leeftijdcategorie betrokken, bij hacken is dat 42,6% en bij het produceren en verspreiden van kinderpornografie is 23.8% van deze leeftijdscategorie betrokken. Toch komen er nog veel meer vormen van cybercriminaliteit voor in Nederland, zoals digitale afpersing, bedreiging etc. Vanwege het feit dat er nu nog veel onduidelijkheid is over de manier waarop jongeren gebruik maken van ict in het plegen van strafbare feiten en of zij zich hierbij richten op alleen cybercrime in ruime- of enge zin of een combinatie hiertussen is de volgende onderzoeksvraag opgesteld: **In welke vormen en in welke mate doen zich in Nederland combinaties voor van cybercrime in enge en ruime zin gepleegd door jeugdige daders tot 18 jaar?**

Delinquent gedrag jongeren

Tijdens de adolescentie ontwikkelen jongeren zich op verschillende gebieden. Zo kenmerkt deze levensfase zich door het verkennen en opzoeken van eigen grenzen en die van de omgeving, experimenteren met mogelijkheden en het ontwikkelen van een eigen identiteit (Van der Ploeg & Scholte, 1990). Volgens Erikson (1995) is het ontwikkelen van een relatief stabiele en consistente identiteit het belangrijkst tijdens de adolescentie.

Door de adolescentie experimenteren jongeren niet alleen offline met hun identiteit, maar ook online zijn ze volop aan het experimenteren. Dit doen ze door zich zowel te identificeren als te onderscheiden van leeftijdsgenoten (Bauwens, Pauwels, Lobet-Maris, Poullet & Walrave, 2009). Ook risicogedrag speelt een rol bij het ontwikkelen van de eigen identiteit en is tot op zekere hoogte onderdeel van een normale ontwikkeling. In dit onderzoek wordt er onder risicogedrag gedrag verstaan met een verhoogde kans op nadelige consequenties voor

de pleger en/of zijn omgeving, wat betreft de gezondheid, het economisch, psychische of sociale functioneren en dat maatschappelijk gezien afgekeurd wordt en/of wettelijk verboden is (Heijkants & Snijder, 1999).

Rond de adolescentie gaan jongeren dus ook onder andere experimenteren met criminaliteit (Kromhout & Van San, 2003). Of jongeren hun risicogedrag ook daadwerkelijk omzetten in delinquent gedrag kan afhangen van verscheidene (risico)factoren (Van der Heiden-Attema & Bol, 2000). Onder delinquent gedrag word hier wetschendingen verstaan.

Het ASE model

Het gedrag van jongeren verklaren is een complex probleem. Om te bepalen welke determinanten invloed hebben op cybercrimineel gedrag van jongeren wordt er in dit onderzoek gebruik gemaakt van het ASE model (De Vries, Dijkstra & Kuhlman, 1988). Het A(ttitude) S(ociale invloed) E(igen-effectiviteitsverwachting) model is een model om met name beredeneerd gedrag te verklaren en is gebaseerd op de twee gedragsmodellen 'Theory of reasoned action' (Fishbein & Ajzen, 1975) en de 'Theory of planned behavior' (Ajzen, 1988).

Volgens het ASE model wordt het gedrag beïnvloed door de intentie om het gedrag wel of niet uit te voeren, welke op zijn beurt weer wordt beïnvloed door de attitude ten aanzien van een bepaald gedrag, de sociale invloed die men in de omgeving waarneemt en de eigen-effectiviteitsverwachting. De determinanten attitude, sociale invloed en eigen-effectiviteitsverwachting worden weer door achtergrondkenmerken zoals, geslacht, leeftijd, opleidingsniveau, en sociaal- economische status, etc. beïnvloed (De Vries et al., 1988).

Het ASE model verschilt op twee belangrijke punten van de Theory of reasoned action en de Theory of planned behavior. Het eerste verschil is, dat in het ASE model gesproken wordt over een determinant 'sociale invloed' in plaats van over de determinant 'subjectieve norm'. Volgens het ASE model zijn er meer sociale invloeden dan subjectieve normen alleen. Het ASE model onderscheidt drie sociale invloeden, namelijk: subjectieve normen, sociale steun/sociale druk, en modelling of voorbeeldgedrag. Het tweede verschil is, dat in het ASE model geen sprake is van 'waargenomen gedragscontrole', maar van Bandura's concept van 'eigen-effectiviteitsverwachting'. Dit is vooral een verschil in naamgeving, ontstaan uit de verschillende achtergronden van het model (Brug, Schaalma, Kok, Meertens & Van der Molen, 2003).

Door het ASE model aan te passen aan onze onderzoeksomstandigheden is er een nieuw model gevormd, waarbij het ASE model gekoppeld is aan het Sociaal Ecologische Model van Bronfenbrenner (1979) om zo de determinant 'sociale invloed' verder uit te werken (zie bijlage I). Allereerst wordt de determinant 'attitude' besproken, waarna vervolgens de determinanten 'sociale invloed' (met behulp van Sociaal Ecologisch Model van Bronfenbrenner) en 'eigen-effectiviteitsverwachting' worden besproken.

De attitude is de houding die je hebt ten aanzien van de gevolgen van het gedrag. In dit geval kunnen daarbij kennis en de perceptie van jongeren ten aanzien van de pakkans, de ernst en de strafmaat een rol spelen bij het vertonen van crimineel gedrag. Nagenoeg alle Nederlandse jongeren hebben toegang tot internet en zij maken gebruik van de mogelijkheden die dit medium biedt (Kerstens & Stol, 2012). Doordat zij veel op internet zitten ontwikkelen zij meer kennis en vaardigheden, waardoor ze zich ook meer gaan bezig houden met verschillende online activiteit (Livingstone & Helsper, 2007). Door het opdoen van kennis en vaardigheden met betrekking tot internet kunnen jongeren zich beschermen tegen online risico's, maar ze kunnen ook gaan experimenteren met hun vaardigheden en daarmee een grens overgaan waarbij ze cybercriminele delicten plegen. Over de perceptie van jongeren is uit onderzoek van Bosman (2011) gebleken dat jongeren vaak wel weten dat asociaal gedrag, zoals kleineren, schelden, beledigen via internet, niet juist is maar ze willen graag bij de groep horen. Ook blijkt uit dit onderzoek dat jongeren wel weten dat er weinig toezicht is op hun activiteiten via de digitale media en dat zij de effectiviteit van de toezicht ook erg laag inschatten. Daarnaast achten zij zichzelf verantwoordelijk voor hun internetgedrag.

Eveneens wordt het gedrag van jongeren ook bepaald door de sociale invloed. Deze determinant zal verder worden uitgewerkt aan de hand van het Sociaal Ecologisch model van Bronfenbrenner (1979). De theorie van het Sociaal Ecologisch Model heeft betrekking op verschillende niveaus om gedrag van jongeren te verklaren. Deze indeling betreft: de jongere, het gezin, de vrienden en school en tenslotte het niveau van de maatschappelijke en culturele omgeving. Het Sociaal Ecologisch Model gaat er vanuit dat de omgeving invloed uitoefent op de ontwikkeling en het gedrag van een individu. De omgeving wordt hierbij ook wel de ecologische ruimte genoemd (Van der Mooren, 2006).

Daarnaast stellen Junger-Tas, Steketee en Moll (2008) dat gedrag altijd een resultaat is van voortdurende interacties tussen aanleg van een mens en de omgeving waarin hij/zij zich bevindt. Dus naast de invloed die de omgeving uitoefent op het gedrag spelen individuele factoren ook een rol. In het navolgende zullen eerst de individuele factoren (de jongere) worden beschreven en vervolgens de overige risicofactoren (gezin, vrienden en school, en

maatschappelijk en cultureel niveau).

Op het individuele niveau zijn kenmerken als geslacht, leeftijd, persoonlijkheidseigenschappen, opleidingsniveau en intelligentie aan te duiden als risicofactoren. Uit veel onderzoeken blijkt dat jongens erg verschillen van meisjes wat betreft delinquent gedrag. Zo blijkt uit het onderzoek van Junger-Tas e.a. (2008) dat jongens beduidend meer delinquent gedrag vertonen dan meisjes. Ook speelt leeftijd een rol bij het verklaren van delinquent gedrag. Zo vindt er volgens Uggen (2000) een stijging van delinquent gedrag plaats in de vroege adolescentie. In de midden en late adolescentie is er een piek, waarna er een daling volgt. Dit is gebaseerd op de 'Age-crime curve' en deze leeftijdscurve is gebaseerd op officiële cijfers van criminaliteit (Louber, Slot & Sergeant, 2001). Uit onderzoek van Van der Laan en Blom (2005) blijkt ook dat jongeren in de leeftijd van 10 tot 13 jaar significant minder delicten plegen dan jongeren in de leeftijd van 14 tot 17 jaar. Niet alleen leeftijd of geslacht kunnen een rol spelen bij het verklaren van delinquent gedrag, ook aanlegfactoren zoals persoonlijkheidseigenschappen, IQ en opleidingsniveau van de jongeren kunnen een rol spelen. Zo lijkt een impulsief temperament, hoge spanningsbehoefte en extraversie (Eysenck, 1996), samen te hangen met de kans op delinquent gedrag. Ook blijkt dat zowel jongeren die hoog opgeleid zijn als jongeren die laag opgeleid beide delinquent gedrag kunnen vertonen. Toch vindt het meeste delinquent gedrag plaats onder lager opgeleide jongeren (Wright, Entner, Caspi, Moffitt, Miech & Silva, 1999). Jongeren die lager zijn opgeleid of een lager IQ hebben, kunnen ook te weinig vaardigheden hebben of niet de juiste vaardigheden hebben aangeleerd gekregen, waardoor ze uit onvermogen delinquent gedrag gaan vertonen. Aan de andere kant kunnen jongeren die juist wel de vaardigheden hebben, deze gebruiken voor het vertonen van delinquent gedrag om zo hun doel te kunnen bereiken. Achter deze bevindingen over het ontstaan en/ of ontwikkelen van delinquent gedrag ligt het leertheoretisch kader als basis (Loeber, 1998).

Op het niveau van het gezin zijn onder andere gebrek aan toezicht en discipline, ouderlijk geweld, geen liefde/ondersteuning krijgen, lage sociale economische status en meemaken van echtscheiding of opgroeien in eenoudergezin risicofactoren voor delinquentgedrag (Van der Heiden-Attema & Bol, 2000).

Vervolgens vallen de risicofactoren slechte schoolprestaties, en risicogedrag van vrienden onder het niveau van school en vrienden en waardering van woning en buurt onder het maatschappelijke en culturele niveau (Van der Heiden- Attema & Bol, 2000). Zo is de leefbaarheid van de directe omgeving zoals het voorzieningen niveau en de kwaliteit van de woning van invloed op criminaliteit in een buurt (Loeber,1998). Matige huisvesting is volgens

Loeber (1998) een risicofactor voor een slechte sociale binding of isolement en de bindingstheorie stelt dat iemand minder snel een delict pleegt wanneer iemand bindingen heeft met de omgeving (Hirsch, 1969). De theorie van Hirschi gaat er ook vanuit dat jongeren die delinquentgedrag vertonen te weinig sociale controle hebben ervaren van onder andere hun ouders, familie, vrienden en school (Sampson & Laub, 1993). Jongeren die weinig of geen contact hebben met hun ouders of familie, hebben het idee dat ze toch niets te verliezen hebben want ze horen als het ware niet bij een sociaal netwerk. Ze worden daardoor niet aangesproken als ze delinquent gedrag vertonen. De theorie van Hirschi wordt ondersteund door onderzoek Luijpers (2000). Hier blijkt namelijk dat meer dan de helft van de onderzochte empirische onderzoeken een negatief verband aantoont tussen sociale binding en delinquent gedrag.

Naast de determinanten attitude en sociale invloed speelt eigen-effectiviteitsverwachting ook een rol bij het beïnvloeden van het gedrag. Onder dit concept wordt de verwachting verstaan tot het in staat zijn van het uitvoeren van het gedrag. Hierbij spelen eerdere ervaringen een rol. Of jongeren het gedrag wel of niet herhalen door hun eerdere ervaringen zal later worden besproken onder criminele carrière.

Achtergrondkenmerken van cybercriminaliteit

Ondanks dat er al veel achtergrondkenmerken van jongeren die traditionele criminaliteit plegen bekend zijn, is het nog niet duidelijk of deze achtergrondkenmerken ook gelden voor jongeren die cybercriminaliteit plegen. Wel is er al wat onderzoek verricht naar achtergrondkenmerken van jongeren die cybercriminaliteit plegen. Zo blijkt dat bij cybercriminaliteit de jongens oververtegenwoordigd zijn (Kerstens & Stol, 2012). Dit geldt in het bijzonder voor delicten als kinderporno. Daarentegen zijn vrouwen relatief vaker betrokken bij e-fraude zaken. Hierbij moet wel vermeld worden dat deze onderzoeken zich specifiek op een aantal online delicten hebben gericht, maar er bestaan natuurlijk een verscheidenheid aan online delicten. Zo heeft dit onderzoek geen online afpersing of bedreiging meegenomen. Hierdoor is het lastig te stellen of cybercriminaliteit over het algemeen meer plaatsvindt onder jongens.

Daarnaast blijkt dat jongeren over het algemeen slechts binnen één risicogebied werkzaam zijn, ofwel cyberpesten of online financieel-economische delicten of online seksuele activiteiten (Kerstens & Stol 2012). De daders daarentegen die wel delinquent gedrag vertonen op meerdere terreinen kenmerken zich door hun impulsieve, nieuwsgierige en

ongeremde gedrag. Deze jongeren, vooral jongens hebben een lage zelfcontrole en een minder goede band met hun ouders en school. Hier staat tegenover dat dit moeilijk te generaliseren is naar alle cybercrime delicten vanwege het feit dat dit onderzoek zich alleen maar heeft gericht op drie cybercrime delicten, namelijk cyberpesten, virtuele diefstal/veiling fraude, en sexting.

Over de rol die opleidingsniveau speelt bij cybercriminaliteit is uit onderzoek van Kerstens en Stol (2012) bekend dat cyberpesten, virtuele diefstal/veiling fraude en het plaatsen van seksueel beeldmateriaal het meeste plaatsvindt onder daders die op het voortgezet onderwijs zitten met daarbinnen een accent op het VMBO. Bij het maken van seksueel beeldmateriaal van zichzelf en/of anderen is er een onderscheid. Zo vindt het maken van seksueel beeldmateriaal van zichzelf het meest plaats onder VMBO-scholieren en het maken van beeldmateriaal van anderen onder havisten en allochtone jongeren. Van de omgevingsfactoren speelt de band met ouders een rol. Zij die seksueel beeldmateriaal maken hebben een minder goede band met hun ouders en komen vaker uit niet-traditionele gezinnen (Kerstens & Stol, 2012).

Daarnaast blijken online dader- en slachtofferschap met elkaar samen te hangen. Zo vertonen jongeren met een verhoogde kans op slachtoffer- en daderschap een overeenkomstig internetgedrag, zijn regelmatig online en hebben vaak niet in de gaten dat de online wereld een publieke wereld is, dat iedereen kan zien (Kerstens & Stol, 2012).

Vanwege het feit dat alle bovenstaande onderzoeken zich hebben gericht op specifieke vormen van cybercriminaliteit is het niet duidelijk of alle factoren ook te generaliseren zijn naar alle vormen van cybercriminaliteit. Daarnaast is er ook geen eenduidig beeld hoe jongeren tegenover cybercriminaliteit aankijken en of zij zich ook als daders zien. Hieruit volgt de volgende onderzoeksvraag: **Wat is er bekend over de achtergrondkenmerken van jongeren die cybercrime in enge en ruime zin (of combinatie daarvan) plegen?**

Motieven

Recent neurologisch onderzoek heeft aangetoond dat de hersenen van jongeren bij het nemen van beslissingen anders functioneren dan die van volwassenen (Van Leijenhorst, 2010). Jongeren zijn gevoeliger voor het vooruitzicht van een mogelijke beloning en daarom sneller geneigd om risico's te nemen. Ze zijn op zoek naar een directe behoefte bevrediging en kunnen hun eigen gedrag nog niet goed reguleren.

Ook kan de Rationele Keuze Theorie (RKT) een belangrijke rol spelen in het nemen van beslissingen. De rationele keuze benadering is één van de klassieke visies op criminaliteit en

normafwijkend gedrag (Griffiths, 1995; Huisman, 2001). Deze benadering veronderstelt dat de mens een rationeel wezen is en in vrijheid een weloverwogen keuze maakt tussen de verschillende aangeboden alternatieven om zijn doel te verwezenlijken. In deze theorie wordt de mens beschouwd als een persoon die kiest voor die optie die het meeste oplevert tegen de minste kosten. Daarbij maakt hij een rationele afweging tussen de verwachte kosten en baten van de verschillende beschikbare opties (Becker 1968; Ultee, Arts & Flap, 2003). Daarbij tellen niet alleen de kosten en baten, maar ook de kans hierop. Men weet in vele gevallen bijvoorbeeld niet wat de precieze pakkans is, maar men heeft daar wel een verwachting van. Deze verwachting, vermenigvuldigd met de kosten bij constatering van de overtreding spelen mee bij de uiteindelijke afweging. Wanneer de baten hoger zijn dan de kosten zullen de jongeren eerder delinquent gedrag vertonen.

Ondanks de kritiek op de RKT dat een individu maar een beperkte rationaliteit heeft, dat er rekening dient te worden gehouden met de omgeving bij het keuzeproces (Witteveen, 2010) en dat criminaliteit lang niet altijd het gevolg van een vrije keuze is maar mede de uitkomst van beïnvloedbare factoren, beargumenteert Becker (1986) toch dat het menselijke keuzegedrag goed te verklaren is, met behulp van deze theorie. Mensen zullen, volgens dit model wanneer ze een keuze maken de uitkomsten van alle mogelijke opties evalueren en voor de optie gaan waarvan de uitkomst hen het meeste oplevert. Verder stelt hij dat er voor criminaliteit geen ander soort verklaringsmodel nodig is, dan voor al het andere gedrag en dat ook hier een economisch model goed te gebruiken is. Maar geldt dit ook voor jongeren die cybercriminaliteit plegen? Maken zij ook rationele afwegingen in het bepalen van hun gedrag of werkt het bij hen anders?

Een tweede veelgebruikte theorie is de Routine Activiteiten Theorie (RAT). Het uitgangspunt hiervan is dat criminaliteit plaatsvindt wanneer er sprake is van een combinatie van een gemotiveerde dader, een geschikt en aantrekkelijk doelwit en de afwezigheid van (capabele) bewaking van het potentiële doelwit (Felson, 2003). Traditioneel gezien gaat de RAT uit van routine activiteiten buitenshuis, in de fysieke wereld. De vraag dient zich echter dan ook aan of, nu een steeds groter deel van het leven zich op het digitale vlak begint af te spelen, deze theorie ook toepasbaar is op online activiteiten.

Het internet creëert nieuwe gebieden waar interactie plaats vindt tussen personen, en potentiële slachtoffers dus blootgesteld kunnen worden aan daders. Dat veel mensen in Nederland deze gebieden betreden blijkt uit een peiling van het CBS (2012). Zo heeft 96% van de Nederlanders heeft toegang tot het internet en is 87% (bijna) dagelijks online. Naast de mogelijkheden die het internet biedt voor legitieme doeleinden, liggen er ook legio kansen

voor daders. Het internet biedt vele mogelijkheden om anoniem en onzichtbaar te blijven, terwijl er makkelijk en goedkoop naar geschikte doelwitten gezocht kan worden. Naast het feit dat op het internet fysieke nabijheid tot doelwitten niet nodig is, biedt het internet daders dus gunstige omstandigheden voor het zoeken naar een geschikt doelwit (Pratt, Holtfreter & Reisig, 2010; Van Wilsem, 2011).

Daarnaast kunnen daders vanuit verschillende motieven handelen. Zo blijkt uit onderzoek van Kerstens en Stol (2012) dat voor de lol, wraak, meedoen met de groep, geld verdienen en jaloezie motieven zijn voor cyberpesten en virtuele diefstal. Tevens blijkt er ook dat bij het maken van seksueel beeldmateriaal veelal de motivatie van experimenteergedrag tussen jongeren onderling een rol speelt (Kerstens & Stol, 2012). Ook blijkt uit onderzoek van Van Geffen, Gumbs, Feltzer, Van der Vlugt en Hellings (2005) dat er nog andere mogelijke motieven voor het plegen van online delicten zijn, zoals: bij een groep te willen horen, statusverhoging binnen de vriendengroep, uit verveling of juist om de kick.

Vanwege het feit dat 70% van de jongeren over een eigen computer beschikt, waarvan de meerderheid deze ook op zijn of haar kamer heeft staan en 34% geen beperkingen krijgt opgelegd door ouders aangaande online gedrag (de Smet & Mahjoub, 2008), is het voor een jongere dus redelijk gemakkelijk om delinquent gedrag te vertonen op internet. Andere voordelen van het gebruik van internet is de anonimiteit en een lage pakkans vanwege het feit dat daders moeilijk op te sporen zijn wanneer het delict vanuit een internetcafé is gepleegd. Daar komt nog bij dat het internet snel is, en je veel mensen kan bereiken. De kosten die daar tegenoverstaan is de straf die je oploopt wanneer je juist wel gepakt wordt. Hieruit volgt de volgende onderzoeksvraag: **Wat is er bekend over de motieven van jongeren die cybercrime in enge en ruime zin (of combinatie daarvan) plegen?**

Criminele carrière

De term ‘criminele carrière’ verwijst naar de ernst en frequentie van delicten die gepleegd zijn door een dader over een bepaalde periode. Zo zijn er daders die één delict plegen en vervolgens niet meer, maar er zijn ook daders die telkens weer in herhaling vallen en een criminele carrière opbouwen.

Zoals eerder al aangegeven verkennen jongeren in de adolescentieperiode hun grenzen en experimenteren met allerlei gedrag dat maatschappelijk niet altijd is toegestaan. Veelal is de criminaliteit onder deze jongeren leeftijdsgebonden en blijft de jongere op het ‘rechte pad’ (Jansen, 1989). Ook Ferwerda (1992) stelt dat crimineel gedrag het beste te typeren is als

leeftijdsgebonden 'kickgedrag' dat voortkomt uit het experimenteergedrag dat bij de adolescentieperiode hoort. Daarentegen blijkt uit onderzoek van Van der Laan en Blom (2010) dat in 2008 42% van de jongeren vaker in aanraking komt met politie en justitie. Hieruit blijkt dus dat veel jongeren weer in herhaling vallen en mogelijk een criminele carrière gaan opbouwen en het crimineel gedrag in de adolescentie periode niet leeftijdsgebonden hoeft te zijn.

Aangezien veel onderzoek wordt verricht naar recidive van jeugdcriminaliteit in het algemeen en niet naar recidive van verschillende vormen van jeugdcriminaliteit, zoals in dit onderzoek cybercriminaliteit, is het niet duidelijk hoe de recidive is bij de verschillende vormen van jeugdcriminaliteit. Daarom is de volgende onderzoeksvraag opgesteld: **Wat is er bekend over de criminele carrières van jongeren die verschillende vormen van cybercrime plegen en in welke mate plegen zij herhaaldelijk vormen van cybercrime?**

Al met al vraagt de veranderende samenleving dat politie en justitie zich aanpassen. Wanneer er wordt gekeken naar ontwikkelingen in criminaliteit (van analoog naar digitaal) wordt er inzicht verkregen in veranderingen van eisen die aan politie en justitie wordt gesteld. In politieregistraties wordt er gezien dat cybercrime een breed maatschappelijk verschijnsel is geworden (Leukfeldt et al., 2010). Zo is hacken bijvoorbeeld niet het kunstje van whizzkids, maar van gewone mensen die elkaar dwars willen zitten of oplichten (Leukfeldt et al., 2010).

Het gebruik van technologie in het plegen van criminaliteit zorgt voor een uitdaging voor de overheid en de rechtshandhaving. Stol (2004) stelt dat 'Het primaire probleem bij de bestrijding van cybercrime is gebrek aan kennis bij politie en justitie'. Om beperkingen te ondervangen is er bij de politie een National High Tech Crime Center (NHTCC) en een Meldpunt Cybercrime opgericht. Toch vereist het nemen van verdere maatregelen nog meer kennis over de aard en omvang van deze criminaliteit. Dit ook vanwege het feit dat onderzoek zich tot nu toe over het algemeen alleen heeft gericht op een aantal vormen van cybercrime. Om zodoende een algeheel beeld te krijgen van cybercriminaliteit onder jongeren in Nederland richt dit onderzoek zich op de probleemverkenning van cybercrime en jeugd. Daarbij worden de eerder vermelde onderzoeksvragen onderzocht en tenslotte wordt er ook de volgende onderzoeksvraag beantwoord:**Zijn er op basis van alle gestelde onderzoeksvragen nog specifieke risico's die volgen uit het digitale gedrag van jongeren en hun mogelijke betrokkenheid als daders van cybercrime? Zo ja, welke?**

2. Methode

Voor dit onderzoek is er gebruik gemaakt van twee verschillende methoden. In het eerste gedeelte wordt de database rechtspraak.nl besproken, waarna in het tweede gedeelte de interviews verder worden uitgewerkt.

Voor dit onderzoek is gekozen om de database www.rechtspraak.nl te gebruiken om de onderzoeksvragen te kunnen beantwoorden, omdat deze database toegang biedt tot meer dan 230.000 uitspraken. Daarnaast moet er van het kabinet in deze database een 'representatief beeld' van rechtelijke uitspraken worden gepubliceerd. Deze uitspraken zijn gecodeerd met een 'LJN' wat staat voor 'Landelijk Jurisprudentie Nummer'; dit is een uniek nummer dat in deze databank aan rechterlijke uitspraken is toegekend. Verder is dit de officiële site van rechtbanken, gerechtshoven, CRvB, CBb, Hoge Raad en Raad voor de rechtspraak. Door uitspraken in deze database te analyseren kan men inzicht krijgen in de vormen van cybercriminaliteit die in Nederland gepleegd worden.

Tevens is er in dit onderzoek gebruik gemaakt van interviews. Door het interviewen van belangrijke sleutelfiguren binnen de cybercriminaliteit onder jongeren, is er getracht inzicht te krijgen in de vormen van cybercriminaliteit gepleegd onder jongeren en de achtergrondkenmerken/motieven/criminele carrières van jongeren met betrekking tot cybercriminaliteit.

2.1 Rechtspraak.nl

2.1.1 Onderzoekseenheden

Met behulp van de zoekmachine kan gezocht worden op LJN, zaaknummer, instantie, vindplaats of kenmerken. Eerst is er een vooronderzoek verricht om na te gaan hoe er binnen rechtspraak.nl het best gezocht kan worden voor optimaal resultaat. Hieruit zijn verschillende zoektermen naar voren gekomen die gebruikt zijn (zie Bijlage II).

Er is gekozen om breed te beginnen met zoeken om later meer specifiek naar bepaalde termen te kijken. Om breed te beginnen zijn termen als internet, cyber, computer en geautomatiseerd werk gebruikt. Later is er gezocht op specifieke strafbare feiten en wetsartikelen. Elke zoekterm is altijd gebruikt in combinatie met jeugd, minderjarige verdachte en geautomatiseerd werk. Op deze manier zijn de zaken uit de database gefilterd waar specifiek jongeren bij betrokken zijn geweest.

Om te bepalen of de gevonden zaken relevant waren voor dit onderzoek zijn enkele

inclusie- en exclusiecriteria gebruikt. Allereerst moet de dader in de leeftijd van 12 tot 18 jaar oud zijn. Deze leeftijden kunnen zowel impliciet als expliciet worden benoemd in een bepaalde zaak. Wanneer de leeftijd expliciet wordt genoemd, wordt er in de zaak een geboortedatum vermeldt van de verdachte. Als deze leeftijd impliciet wordt benoemd is er aangegeven dat de zaak is afgedaan in jeugdstrafrecht of dat de jeugdreclassering betrokken is geweest bij de zaak. Andere woorden die gebruikt kunnen worden bij het impliciet benoemen van de leeftijd zijn jeugddetentie en jeugdpsychiatrie. Wanneer de verdachte ouder is dan 18 jaar wordt deze zaak niet meegenomen in de analyse. Dit geldt ook voor oudere verdachten die berecht worden via het jeugdstrafrecht. Dit kan bijvoorbeeld het geval zijn wanneer de omstandigheden dat rechtvaardigen (artikel 77b van het wetboek van strafrecht en artikel 77c van het wetboek van strafrecht). Wanneer de verdachte ouder is dan 18 jaar op het moment van de uitspraak, maar jonger dan 18 jaar op het moment van plegen wordt deze zaak meegenomen voor verdere analyse.

Daarnaast is het van belang dat er gebruik is gemaakt van informatie communicatie technologie (ICT). Er is gebruik gemaakt van ICT als uit de beschrijving van de zaak blijkt dat het delict tot stand is gekomen door middel van het gebruik van een informatie- en communicatie technologisch middel. Wanneer dit niet duidelijk in de zaak staat vermeld wordt deze zaak niet meegenomen voor verdere analyse.

Een ander criteria waar gebruik van is gemaakt is dat er uit de beschrijving van de zaak moet blijken dat de jongere daadwerkelijk verdachte is. Wanneer in de omschrijving van de zaak duidelijk staat vermeld dat de jongere slachtoffer is in plaats van dader zal deze zaak ook niet meegenomen worden. Allereerst valt een zaak af wanneer er niet duidelijk wordt vermeld of het om cybercriminaliteit gaat. Deze criteria hebben geleid tot 47 relevante uitspraken.

2.1.2 Procedure

Er is in de periode februari tot april 2013 onderzoek gedaan in de database van rechtspraak.nl. Waarbij er met behulp van de eerder genoemde zoektermen is gezocht naar unieke uitspraken die te maken hebben met jongeren tot 18 jaar die cybercriminaliteit plegen. Zoals al eerder vernoemd zijn deze unieke uitspraken uit de database gehaald met behulp van de inclusie en exclusie criteria. Vervolgens is elke zaak tot in detail doorgelezen en zijn de genoemde kenmerken in een bestand geplaatst voor nadere vervolg analyse.
Deze analyse betreft het vergelijken van overeenkomsten en verschillen tussen unieke zaken. Op basis van de onderzoeksvragen is bepaald welke aspecten er achterhaald moesten worden om de onderzoeksvragen te kunnen beantwoorden.

Tabel 1. Kenmerken behorende bij de onderzoeksvraag

Onderzoeksvraag	**Kenmerken**
Algemeen	Gebruikte zoektermen, LJN, omschrijving van de zaak, wetsartikelen, leeftijd dader, leeftijd expliciet of impliciet benoemd, geslacht, jaartal van plegen, jaartal van uitspraak
Vormen	Combinaties enge- en ruime zin/ online en offline
Achtergrondkenmerken en Motieven	Achtergronden & Motieven
Criminele carrière	Recidive

2.1.3 Operationalisatie

De gevonden zaken zijn grondig geanalyseerd en wanneer ze voldeden aan de inclusie- en exclusie criteria zijn ze opgenomen in een bestand. Van iedere zaak die binnen de selectie viel zijn de volgende gegevens genoteerd: Gebruikte zoektermen, LJN, omschrijving van de zaak, wetsartikelen, leeftijd van de dader, leeftijd expliciet of impliciet benoemd, geslacht, jaartal van plegen, jaartal van uitspraak, cybercrime in enge en ruime zin, cybercrime enge/ruime zin expliciet of impliciet benoemd, type delict, combinaties, achtergrond, motieven en recidive.

Allereerst zijn er een aantal algemene kenmerken, zoals LJN, van een zaak opgenomen in het bestand. Hiervoor is gekozen vanwege het feit dat zo duidelijk is welke zaak het betreft en zo kon worden voorkomen dat er dubbele zaken werden geanalyseerd.

Gebruikte zoektermen: Dit zijn de zoektermen waarmee er is gezocht om de bepaalde zaak aan het licht te krijgen. Deze zoektermen zijn te vinden in bijlage II.

LJN: 'Landelijk Jurisprudentie Nummer'. Dit is een uniek nummer dat in de databank aan rechterlijke uitspraken is toegekend.

Omschrijving van de zaak: Dit is de korte samenvatting die aan het begin van elke zaak wordt gegeven over het delict.

Wetsartikelen: Dit zijn de artikelen die gebruikt zijn om tot een veroordeling te komen.

Leeftijd dader: De leeftijd die de verdachte had op het moment van plegen.

Impliciet/expliciet benoemd: Wanneer de leeftijd van een verdachte ten tijde van plegen werd aangegeven met een geboortedatum is het gescoord als expliciet. Wanneer er gebruik is gemaakt van termen als jeugdrecht, jeugdreclassering, minderjarige verdachte is het gescoord

als impliciet.

Geslacht: Is het delict gepleegd door een man of door een vrouw.

Jaartal van plegen: Het jaar waarin de verdachte het delict heeft begaan

Jaartal van uitspraak: Het jaar waarin er tot een veroordeling van de verdachte is gekomen.

Vervolgens zijn er drie aspecten beoordeeld om onderzoeksvraag betreffende de vormen te kunnen beantwoorden.

Cybercriminaliteit in enge zin: Dit zijn strafbare gedragingen die niet zonder tussenkomst van ICT gepleegd kunnen worden. Kenmerkend is dat de ICT structuur zelf (en daarin of daarmee opgeslagen gegevens) het doel van de actie zijn. Hierbij valt bijvoorbeeld te denken aan het veroorzaken van een stoornis in een geautomatiseerd systeem, verspreiden van computervirussen of het ongeoorloofd binnendringen van een geautomatiseerd werk waarna gegevens worden beschadigd of vernietigd. Het betreft dus vormen van criminaliteit die zich zonder ICT niet zouden voordoen.

Wanneer er uit de omschrijving van de zaak blijkt dat de jongere het strafbare feit niet heeft kunnen doen zonder tussenkomst van ICT wordt het delict gescoord als cybercriminaliteit in enge zin.

Cybercriminaliteit in ruime zin: Onder cybercrime in ruime zin worden strafbare gedragingen verstaan die met behulp van ICT worden uitgevoerd. ICT wordt dan ter ondersteuning gebruikt bij het plegen van anderszins traditionele criminaliteit. Wanneer er uit de omschrijving van de zaak blijkt dat de jongere ICT als hulpmiddel heeft gebruikt om anderszins traditionele criminaliteit te plegen wordt ze zaak gescoord als cybercriminaliteit in ruime zin.

Combinaties: wanneer een verdachte veroordeeld wordt voor zowel cybercriminaliteit in enge zin als in ruime zin is dit gezien als een combinatie van cybercriminaliteit in enge en ruime zin. Wanneer de verdachte veroordeeld wordt voor alleen cybercriminaliteit in ruime zin of alleen cybercriminaliteit in enge zin is dit geen combinatie

Daarnaast kan er ook gesproken worden van een combinatie tussen online en offline criminaliteit. Er is sprake van een combinatie wanneer de verdachte wordt veroordeeld voor zowel een traditionele vorm van criminaliteit en een cybercriminaliteit. Een voorbeeld hiervan is dat de verdachte wordt berecht voor hacken en mishandeling van een persoon. Wanneer de verdachte veroordeeld wordt voor alleen een vorm van cybercriminaliteit, zoals bijvoorbeeld hacken en er geen sprake van een combinatie

Daarna is er gekeken of, en zo ja welke achtergronden en motieven er in de beschrijving van de zaak te vinden waren om zodoende onderzoeksvraag drie te kunnen beantwoorden.

Achtergrond: Gekeken is of er wat wordt beschreven over de persoonlijkheid van de verdachte, of er problemen zijn, zijn IQ, en of er wat wordt beschreven over de omgeving van de verdachte.
Motieven: Hierbij is gekeken naar de achterliggende reden waarom de verdachte het delict heeft gepleegd. Dit zou kunnen zijn om financiële redenen, groepsdruk of uit hobbyisme.

Om de onderzoeksvraag betreffende de criminele carrières te beantwoorden is er gekeken naar de recidive van de dader.
Recidive: Dit is de mate waarin een veroordeelde na zijn of haar straf weer terugvalt in het oude criminele gedrag. Het gaat erom of de verdachte opnieuw de fout in gaat en opnieuw een strafbaar feit pleegt.

2.2 Interviews

2.2.1 Geïnterviewden

Voor het afnemen van de interviews is er geprobeerd een landelijke dekking te krijgen door interviews af te nemen bij mensen die verschillende functies bezetten en in verschillende delen van het land werkzaam zijn. Hierbij is er, middels behulp van Google, Linkedin, en Facebook, gezocht naar mensen die specifiek met cybercrime en jeugd te maken hebben in hun werkveld.

Uiteindelijk is er een lijst vastgesteld waarop ook alternatieve personen stonden die we konden benaderen als een bepaald werkveld onvoldoende vertegenwoordigd zou worden. Vervolgens zijn de beoogde respondenten via de e-mail of telefoon benaderd met een uitnodiging (zie bijlage III) om deel te nemen aan het onderzoek. Om aan te geven of mensen wilden deelnemen aan het interview konden zij een reply op de betreffende mail sturen, waarbij zij ook desgewenst een geschikte datum konden aangeven voor afname van het interview. Vervolgens is er persoonlijk contact opgenomen voor het maken van een concrete afspraak.

In totaal zijn er 20 personen, per telefoon of middels email gevraagd of ze bereid waren om deel te nemen aan een interview. In deze uitnodiging stond nadrukkelijk vermeld dat het gaat om cybercriminaliteit in Nederland onder jongeren tot 18 jaar. Tien mensen reageerden daarop positief. Verder gaven twee personen aan dat zij wel wilden deelnemen maar vanwege drukte er geen tijd voor konden vrijmaken, en drie personen gaven aan dat zij niet genoeg inzicht hadden in het onderwerp en daarom niet wensten deel te nemen. Ook hebben er vijf personen niet gereageerd. Daarop is na drie weken een herinneringsmail verzonden, waar ook

geen respons op is ontvangen. Uiteindelijk zijn er tien interviews afgenomen met personen met diverse achtergronden, functies en werkvelden (zie voor een overzicht Tabel 3). Twee interviews vonden op verzoek van de benaderde persoon plaats in aanwezigheid van een of meerdere collega's.

Tabel 3. Overzicht van de respondenten

Functie	**Organisatie**
Hoogleraren en onderzoekers	Universiteit Twente
Senior onderzoeker en onderzoekers	NHL Hogeschool Leeuwarden
Bemiddelaar en beleidsmedewerker	Stichting Slachtoffer in Beeld
Bemiddelaar en beleidsmedewerker	Stichting Slachtoffer in Beeld
Digitaal wijkagent	Politie Limburg-Zuid
Analist Team High Tech Crime	Team High Tech Crime, Nationale politie
Projectleider Jeugd & Cybercrime. Projectmanager expertgroep Digikids	Politie & Stichting Mijn Kind Online
Vervangend implementatieleider en intern trainer & Raadsonderzoeker	Raad voor de Kinderbescherming
Directeur en Medeoprichter	IT Security bedrijf
Sr. Advisor Security and Cybercrime	Rabobank Nederland

2.2.2 Procedure

Voorafgaand aan het interview werd bij de introductie de geïnterviewde een informed consent formulier voorgelegd (zie bijlage IV) waarin vermeld stond wat het doel van het onderzoek is en door wie het onderzoek wordt afgenomen. Daarnaast vroegen we expliciet om toestemming om het gesprek op te nemen, zodat er later de mogelijkheid zou bestaan om specifieke stukken terug te luisteren of bepaalde reacties gedetailleerd uit te werken. Daarbij werd aangegeven dat de opnames alleen bestemd zijn voor het onderzoek en niet beschikbaar zullen zijn voor anderen. Verder werd de geïnterviewde verteld dat alle informatie strikt vertrouwelijk zal worden behandeld en in geanonimiseerde vorm zal worden verwerkt. Tijdens het interview werden er vragen gesteld door één interviewer en werd er genotuleerd

door één of soms twee ander(en).

Op basis van de geformuleerde onderzoeksvragen is er een semigestructureerd interviewprotocol uitgewerkt (zie bijlage V; vgl. Giebels & Noelanders, 2004). Dit betekent dat het interview na een introductie werd opgedeeld in twee delen. In het eerste gedeelte kreeg de geïnterviewde de gelegenheid om in eigen woorden te vertellen op welke manier hij/zij te maken heeft met cybercrime in Nederland gepleegd door jongeren tot 18 jaar, en wat hun ervaringen daarmee zijn. In het tweede gedeelte werd aan de hand van een zevental thema's- gebaseerd op de 7 onderzoeksvragen- verder doorgesproken. Deze thema's betroffen:

1) Vormen

Bij het thema vormen wordt er ingegaan op het onderscheid tussen enge en ruime zin van cybercriminaliteit. Er wordt hier inzicht verkregen in verschillende vormen en combinaties van cybercriminaliteit die zich in Nederland voordoen.

2) Achtergrondkenmerken en motieven

Hierna wordt er in het thema achtergrondkenmerken & motieven inzicht verkregen in de achtergrondkenmerken en motieven van jongeren tot 18 jaar die cybercriminaliteit plegen en of dit verschillend is van jongeren die offline criminaliteit plegen. Bij dit thema als bij de thema's *criminele carrières, ontstaanswijze, werk- & pleegwijze* is er ook een lijst opgesteld voor de interviewer van mogelijke onderwerpen die als factoren/voorspellers voor het betreffende thema kunnen gelden. Deze factoren/voorspellers zijn uit de literatuur naar voren gekomen en werden gebruikt als terugkoppeling van wat geïnterviewde heeft verteld en extra controle voor de interviewer. Wanneer een geïnterviewde dus een bepaald onderwerp niet heeft aangestipt kan de interviewer hierop inspelen en vragen of dat een mogelijk achtergrondkenmerk kan zijn.

3) Criminele carrières

In het thema criminele carrières wordt de herhaling van criminele daden en daarmee opzetten van een criminele carrière onderzocht. Ook hierbij is onderscheid gemaakt tussen online en offline criminaliteit en welke factoren mogelijk van invloed kunnen zijn op het in herhaling vallen van jongeren.

4) Ontstaanswijze*

Daarna wordt er bij het thema ontstaanswijze ingegaan op hoe jongeren betrokken raken bij cybercriminaliteit en factoren die mogelijk bijdragen tot het ontstaan van cybercriminele daden onder jongeren tot 18 jaar.

5) Werk- en pleegwijze*

Verder wordt er bij het thema werk- en pleegwijze ingegaan op of jongeren een bepaalde

werk- of pleegwijze hebben en of zij ook verschillen van jongeren die online criminaliteit plegen. Daarnaast wordt er ook in dit thema weer ingegaan op of er verschillen/overeenkomsten zijn tussen werk- en pleegwijze van cybercrime in enge en ruime zin.

6) Perceptie verdachten cybercriminaliteit*

Vervolgens wordt er in dit thema ingegaan op de perceptie van jonge daders. Daarbij wordt er van de geïnterviewden verwacht wanneer zij ervaringen en/of kennis hebben over de perceptie van jonge daders deze met ons te delen. Wat in dit thema centraal staat is: hoe kijken jonge daders tegen cybercriminaliteit aan en welke invloed heeft dit op de mate van plegen van cybercriminaliteit. Ook hierbij wordt er gevraagd of er onderscheid is in perceptie van daders die online of offline criminaliteit plegen en of er een verschil is bij jongeren die cybercrime in enge zin plegen in vergelijking met hen die cybercrime in ruime zin plegen.

7) Aanpak en Consequenties*

Vanwege het feit dat Politie en Justitie een belangrijke rol spelen binnen het onderwerp cybercriminaliteit in Nederland wordt het interview afgesloten met het thema Aanpak & Consequenties. Hier worden er vragen gesteld met betrekking tot het handelen van Politie & Justitie en de gevolgen van cybercriminaliteit.

Voor deze volgorde van thema's is gekozen, omdat we het interview vanuit een zo breed mogelijk perspectief wilden starten en om bijvoorbeeld eerst oorzaken en dan pas consequenties en aanpak te bespreken.

Bij de afsluiting van het interview werd er gevraagd of er nog zaken niet aan bod zijn gekomen en werd er ruimte gegeven om dat te bespreken. Als allerlaatste werd nog gevraagd of er op een later tijdstip contact op mag worden genomen met de geïnterviewde voor mogelijk verdere vragen of onduidelijkheden.

2.2.3 Analyse

De interviews zijn uitgewerkt op basis van wat er genotuleerd is tijdens het interview en de opname die is gemaakt. Hiervan is er een samenvatting van het interview gemaakt en zijn uitspraken ingedeeld onder bepaalde thema's waarover de betreffende persoon informatie geeft. Ter vergroting van de betrouwbaarheid is er voor gekozen om samenvatting te laten controleren door medeonderzoekers.

* De onderzoeksvragen behorend bij deze thema's worden besproken in de masterscriptie van L.D. Slot (medeonderzoeker).

3. Resultaten

Het hoofdstuk resultaten wordt in twee delen besproken aan de hand van de verschillende onderzoeksmethoden. Vervolgens wordt er in het derde gedeelte een geïntegreerd overzicht gegeven van de resultaten die uit de verschillende onderzoeksmethoden naar voren zijn gekomen.

3.1 Rechtspraak.nl

3.1.1 Algemeen

De verschillende zoektermen hebben verscheidene resultaten opgeleverd die te vinden zijn in bijlage V Zoekopdrachten. De zoekmachine heeft in totaal 2456 hits opgeleverd waarvan 47 bruikbare zaken. Computer en minderjarige, internet en minderjarige, kinderporno en minderjarige, computer en jeugd, internet en jeugd leverden de meeste hits op. Wel bleek dat naarmate er verder werd gezocht met verschillende zoektermen er steeds veel dezelfde zaken werden gevonden. Naast de vele dubbele zaken die werden gevonden zijn er veel redenen waarom de vele hits zo weinig bruikbare hits opleverde.

Een nadeel van de database rechtspraak.nl is dat er niet specifiek kan worden gezocht. Wanneer er op computer en minderjarige wordt gezocht worden alle zaken weergegeven waar het woordje ‘computer’ of ‘minderjarige’ of beide in de inhoudsindicatie worden genoemd. De voornaamste reden waarom zaken zijn afgevallen was omdat de daders geen minderjarigen waren. Andere redenen waren dat het om een minderjarig slachtoffer ging in plaats van een minderjarige dader. Daarnaast zijn zaken afgevallen doordat er bijvoorbeeld een overval is gepleegd op een computerwinkel, een computer is gestolen, de computer als straf is afgenomen of dat de zaak veel aandacht heeft gekregen via internet. Voor het totaal aantal hits en ook de bruikbare hits zie bijlage VI.

Ook is er gekeken naar het geslacht van de dader en zijn leeftijd. Hieruit bleek dat er bij 24 zaken expliciet benoemd is dat de dader een jongen is. De leeftijd wordt in 27 zaken expliciet benoemd en ligt tussen de 14 en 18 jaar. Wanneer de leeftijd niet expliciet wordt genoemd dan staat er vaak minderjarige dader of dat hij/zij gestraft is middels het jeugdrecht. Over het algemeen zit er één a twee jaar tussen het plegen van het delict en de afhandeling van de zaak. Zo zijn de geanalyseerde zaken veelal gepleegd tussen 2004 en 2012 en zijn de zaken afgedaan tussen 2005 en 2013. Bij negen zaken is er bekend dat het delict zich over een langer termijn heeft afgespeeld en het delict zich vaker heeft voorgedaan.

3.1.2 Combinaties cybercriminaliteit

Uit de 47 bruikbare zaken blijkt dat het in 39 gevallen gaat om cybercriminaliteit in ruime zin en in 16 gevallen om cybercriminaliteit in enge zin (zie tabel 5). Er zijn verschillende zaken waarbij de verdachte voor verschillende vergrijpen is veroordeeld. Verder kan er dus geconcludeerd worden dat cybercriminaliteit in ruime zin vaker voorkomt onder jongeren dan cybercriminaliteit in enge zin.

In de meest voorkomende gevallen gaat het om kinderporno of het verspreiden van pornografisch materiaal. Deze vorm van cybercriminaliteit is in dertien zaken teruggevonden op rechtspraak.nl. Vervolgens gaan respectievelijk tien en negen zaken over bedreiging en mishandeling. Bij bedreigingen betreft het dat het wordt gepleegd via Twitter, Facebook, GSM en/of chat. Hierbij wordt het slachtoffer bedreigd met de dood, of dat er seksueel materiaal zal worden verspreid. De zaken die mishandeling tot gevolg hebben wordt ICT gebruikt om het in gang te zetten. Zo roept de verdachte vrienden op om het slachtoffer te mishandelen of is het slachtoffer via ICT middelen, zoals Facebook gevonden. De verdachte spreekt een plaats en een tijd af waarop zij het slachtoffer te pakken nemen. Verder gaat het in vijf zaken over sexting. Dit houdt in dat er seksueel beeldmateriaal die door jezelf of anderen is opgenomen wordt verspreid via internet. Ook is er één zaak gevonden van mensenhandel die via ICT is opgezet.

Daarnaast gaan 16 zaken over cybercriminaliteit in enge zin. In vier gevallen is de verdachte veroordeeld voor het hacken van een computersysteem. Van Ddos aanvallen zijn zes zaken bekend, van phishing één en virtueel amulet drie. In de zaken betreft het virtueel amulet gaat het over dat een slachtoffer bedreigd en mishandeld is om zijn wachtwoord van een virtueel spel af te geven aan de verdachte(n). Vervolgens heeft deze verdachte virtuele goederen gestolen van het slachtoffer. Tenslotte zijn er twee zaken gevonden waarbij jongeren betrokken zijn bij afpersing via internet.

Tabel 5. Aantal gepleegde delicten

Delict	**Aantal geregistreerde vormen**
RUIME ZIN	39
Kinderporno, verspreiden van pornografisch materiaal	13
Bedreiging	10
Mishandeling	9
Sexting	7
Mensenhandel	1

ENGE ZIN	16
Ddos aanval	6
Hacken	4
Virtueel amulet	3
Afpersing	2
Phishing	1

In totaal hebben 20 zaken te maken met seksueel getinte delicten. Hierbij kan sprake zijn van bedreiging via internet tot het plaatsen van seksueel getinte foto's, en in het bezit zijn van kinderpornografie, maar ook het opnemen van gedwongen seksuele handelingen aan slachtoffer door de dader. In zes gevallen waarbij de dader in het bezit is van kinderpornografie of het verspreidt/maakt is er ook sprake van feitelijke verkrachting/aanranding/misbruik offline (zoals LJN BW8360; Hier heeft een jongen zijn zusje verkracht en tevens seksueel getinte opnames gemaakt van een ander meisje).

In zaken waarin sprake is van cybercrime in enge zin is er vooral sprake van Ddos aanvallen op bedrijven en overheid en deze zijn niet in combinatie met cybercriminaliteit in ruime zin of offline criminaliteit gepleegd. Er is alleen bij de drie gevonden zaken betreffende het virtueel amulet een combinatie gevonden met offline criminaliteit. Maar hier kunnen geen conclusies over getrokken worden, want deze drie zaken betreffen dezelfde gebeurtenis. Verder is er bij de cybercrime in enge zin die is gevonden op rechtspraak.nl geen sprake van combinaties met cybercrime in ruime zin (zie tabel 6).

Bij cybercrime in ruime zin ligt dit zoals hierboven al eerder vermeld anders. Van de 39 zaken die te maken hebben met cybercriminaliteit in ruime zin is er in 19 gevallen sprake van een combinatie met offline criminaliteit (zie tabel 6). Zoals eerder al genoemd worden er vaak via internet afspraken gemaakt met slachtoffers en vervolgens worden zij bedreigd, afgeperst of mishandeld. Daarnaast kan het ook andersom zijn dat er eerst een offline delict plaatsvindt zoals bij zaaknummer LJN BP8994. Hier worden er meisjes in het openbaar mishandeld en beroofd, dit wordt door de mededaders opgenomen en vervolgens op internet geplaatst.

Tabel 6. Combinatie delicten

	Offline	Enge zin
Enge zin	4	
Ruime zin	19	-
Totaal	23	

3.1.3 Achtergrondkenmerken en Motieven

Over de achtergrondkenmerken valt met rechtspraak.nl niet veel te concluderen. Dit heeft te maken met het feit dat in veel gevallen er niets over de achtergrond van de dader(s) worden vermeld. Wanneer dit wel vermeld wordt blijkt dat uit het feit dat dit wordt meegenomen in de bepaling van de strafmaat.

Van de gevonden 47 zaken die te maken hebben met cybercriminaliteit wordt er bij 14 zaken gesproken over achtergrondkenmerken van daders. In deze gevallen staat er bij zes zaken vermeld dat er sprake is van gedragsproblematiek, in de zin dat de dader mogelijk ADHD of een autistisch spectrum stoornis heeft. Ook wordt er in een vijf gevallen benoemd dat er bij de dader sprake is van een cognitieve en/of emotionele ontwikkelingsachterstand, waarbij er ook sprake is van een laag geestesvermogen en zwakke begaafdheid.

Wat betreft motieven wordt er in het merendeel van de zaken niets genoemd. Wanneer het wel wordt benoemd zijn het motieven als: sterke behoefte om macht en controle uit te oefenen, superioriteitgevoelens, jaloezie, aanzien, erbij willen horen, seksueel beter voelen en gevoel van macht.

Op basis van deze gegevens uit Rechtspraak.nl vallen er dus geen conclusies te trekken over de achtergrondkenmerken en motieven van de jongeren die cybercrime plegen.

3.1.4 Criminele carrière

Over de criminele carrières van de jongeren met betrekking tot cybercriminaliteit valt niets te concluderen met behulp van rechtspraak.nl. In acht gevallen wordt er gesproken over een destijds gedetineerde verdachte of niet. Zo is in vier zaken de dader al wel eerder veroordeeld en in de andere vier gevallen is de verdachte nog niet eerder in aanraking geweest met justitie. Ook wordt er in maar vijf zaken beschreven of er sprake is van een recidiverisico, deze varieert van gemiddeld laag tot dat het niet uitgesloten kan worden of hij/zij recidiveert.

3.1.5 Specifieke risico's van digitaal gedrag

Met behulp van rechtspraak.nl kan er niets worden gezegd over specifieke risico's die volgen uit het digitale gedrag van jongeren. Dit thema en bijbehorende onderzoeksvraag zal worden beantwoord met behulp van de interviews.

3.2 Interviews

3.2.1 Algemeen

De tien interviews hebben over het algemeen overeenkomstige resultaten opgeleverd. Zo blijkt dat cybercrime een grote rol speelt in onze maatschappij en jongeren hier veel bij betrokken zijn. Volgens geïnterviewden komt dit door het feit dat een groot deel van het leven van de jongeren zich op internet, via social media, afspeelt. Jongeren zijn daarom ook niet alleen betrokken bij cybercrime als daders maar ook als slachtoffers.

Verder bleek dat naarmate er werd doorgevraagd aan de geïnterviewden zij de neiging hadden om te praten vanuit ideeën en niet vanuit hun kennis en ervaringen. Om hen toch te laten praten over hun ervaringen werd er ook gevraagd naar voorbeelden uit de praktijk. Tevens werd er ter vergroting van de betrouwbaarheid een aantal vragen, met een andere formulering, herhaald. De verdere onderzoeksresultaten worden in de onderstaande paragrafen besproken.

3.2.2 Combinaties cybercriminaliteit

Uit de interviews kwam duidelijk naar voren dat het sociale leven van jongeren zich grotendeels op het web afspeelt. De geïnterviewden gaven daarbij voorbeelden van zowel cybercriminaliteit in enge als in ruime zin. Vormen van criminaliteit die veel werden genoemd waren: cyberpesten, sexting, laster, smaad, bedreiging, aanmaken van haatprofielen en belediging. Bij dit laatste valt op dat middelen als Twitter, Facebook en Whatsapp vaak zorgen voor een escalerend effect, waarschijnlijk omdat meer anonimiteit en afstand zorgt voor extremere uitspraken die aan de andere kant voor een veel breder publiek beschikbaar zijn. Berichten via Twitter worden dan bijvoorbeeld eenvoudig aanleiding voor een mishandeling. Ook pestgedrag via deze middelen wordt hierdoor steeds prominenter.

Onder sexting wordt het versturen van seksueel getinte berichten, pikante foto's of video's via je telefoon of internet verstaan. Dit wordt gedaan zonder toestemming van het slachtoffer en wordt meestal gedaan om te pesten en te treiteren of omdat de relatie is verbroken.

Tevens kwam er uit alle interviews naar voren dat jongeren zich minder bezig lijken houden met cybercriminaliteit in enge zin dan in ruime zin, omdat cybercriminaliteit in enge zin meer georganiseerde vormen van cybercriminaliteit betreft. Hier heb je connecties voor nodig, het is duur en ingewikkeld en het wordt hierdoor niet/weinig door jongeren gepleegd.

Vormen van cybercriminaliteit in enge zin die wel in verband worden gebracht met jongeren zijn volgens geïnterviewden uit de ICT- en opsporingssector: hacken, het plaatsen van een botnet en phishing. Volgens een geïnterviewde uit de ICT sector spelen jongeren vooral een rol in het zijn van 'katvangers' op schoolpleinen. *'Zo lenen zij bijvoorbeeld een pinpas van een ander om vervolgens geld te stelen dat gedaan wordt door iemand die de digitale wereld snapt. Dit is een nieuwe vorm van criminaliteit onder de jeugd die onder de oppervlakte zit en je alleen ziet als je er ook in zit. Er is geen fysieke afdruk van die criminaliteit.'*

Of jongeren een dergelijke vorm van cybercriminaliteit plegen heeft te maken met de vervaging van normen en waarden, stelt een geïnterviewde uit de onderzoek- en politiesector. '*Online ga je al snel een grens over.*' Verder is het lastig om inzicht te krijgen in sommige vormen van cybercriminaliteit in ruime zin, zoals bijvoorbeeld grooming. Men heeft de indruk dat dit veel gebeurt maar als slachtoffers niet in het spel trappen dan wordt het voor de politie niet zichtbaar. Bij zeven geïnterviewden bestaat de indruk dat het probleem groter is dan het nu lijkt.

Volgens een geïnterviewde die veel met jongeren werkt in het na-traject bestaan er eigenlijk twee verschillende vormen van cybercriminaliteit in ruime zin. Allereerst gaat het om bijvoorbeeld het verspreiden van pornografische of intieme beelden. Het delict is elektronisch en de computerhandeling is ook direct aanleiding tot aangifte. *Bijvoorbeeld: 'Een jongen heeft naaktfoto's van zijn ex op internet gezet vanwege woede dat het uit is.'* Daarnaast betreft het bijvoorbeeld escalatie van online conflicten die daarna offline worden voortgezet. *Bijvoorbeeld:'Twee meisjes hebben ruzie via Facebook over het feit dat de één zou hebben geroddeld over de ander en vervolgens gaat de ruzie in het openbaar verder en wordt het ene meisje mishandeld.'*

Naast deze vorm van verwevenheid tussen online en offline conflicten wordt er nog een tweede vorm van verwevenheid genoemd. Dit betreft het gegeven dat daders van online conflicten ook vaak ervaring hebben met offline criminaliteit. Het gaat dan bijvoorbeeld om oplichtingpraktijken Er worden verder geen combinaties van cybercrime in ruime en enge zin genoemd.

Daarnaast gaven acht geïnterviewden als kanttekening aan dat inzicht in de precieze

verschijningsvormen lastig te achterhalen is omdat het rapporteren van politie en justitie tijdens aangiftes vaak niet volledig is, bv als er bedreiging is plaatsgevonden via internet, wordt dit alleen gerapporteerd als bedreiging. Ook stelden zij dat mensen vaak geneigd zijn om geen aangifte te doen en dat er bij veel vormen van (cyber)criminaliteit de dader nooit in beeld komt.

3.2.3 Achtergrondkenmerken en Motieven

Allereerst moet er geconcludeerd worden dat het moeilijk is een prototype dader vast te stellen. Cybercriminaliteit wordt steeds toegankelijker, iedereen heeft internet, en daarmee is het dus moeilijk te stellen of er een bepaald type dader is met betrekking tot cybercriminaliteit. Een geïnterviewde uit de ICT sector stelt dat *'Veel daders van cybercriminaliteit uit mooie gezinnen komen, maar er is een kloof tussen ouder en kind.'*

Daarnaast komt er bij alle geïnterviewden naar voren dat het vaak wat introvertere, en stillere jongeren zijn. Waarbij de geïnterviewde uit de onderzoekssector ook stellen dat je in het algemeen kunt zeggen dat jongeren vaker in de problemen komen naarmate ze ouder worden. Dit kan mogelijk komen doordat naarmate ze ouder worden ze vaker in aanraking komen met zaken op internet. Ook komt er uit alle interviews naar voren dat daders van cybercriminaliteit mogelijk licht autistische trekken vertonen of emotioneel onderontwikkeld zijn. '*Met het stellen van dergelijke achtergrondkenmerken van daders moet men voorzichtig zijn, want het vertonen van autistisch spectrum stoornis staat ook in verband met slachtofferschap'* vertelt een geïnterviewde uit de onderzoek- en politiesector. Tevens zijn slachtofferschap en daderschap met elkaar verweven vanwege het feit dat het vaak voorkomt dat de dader vroeger zelf ook slachtoffer is geweest. Zo bleek uit eerder onderzoek, van de geïnterviewden uit de onderzoekssector, dat tweederde van de daders ook slachtoffers waren.

Verder zijn opleidingsniveau en gebruikers intensiteit van belang bij het plegen van cybercriminaliteit. Mensen die cybercriminaliteit in ruime zin plegen hebben vaak een lager opleidingsniveau dan zij die cybercriminaliteit in enge zin plegen. Verder is de gebruikers intensiteit en computer kennis bij jongeren die cybercriminaliteit in enge zin plegen ook hoger. Daarentegen hoeft, volgens een geïnterviewde die in de opsporingssector werkt, het kennisniveau van jongeren die cybercriminaliteit in enge zin plegen niet altijd heel hoog te zijn, bv Anonymus Groep. Tevens is het een vooroordeel om te stellen dat het altijd 'einzelgängers' zijn die cybercriminaliteit in enge zin plegen. Zo komen er volgens geïnterviewden uit de ICT-, opsporing- en justitiële sector ook jongeren naar voren die wel

vrienden hebben, maar dit is dan wel een kleine groepje vrienden.

Eveneens komt er uit zeven interviews naar voren dat er wel een onderscheid is met welke vorm van cybercrime jongens zich bezighouden en met welke meisjes. Zo houden jongens zich vooral bezig met cybercriminaliteit in enge zin, omdat zij volgens een geïnterviewde uit de opsporingssector veel behoefte hebben aan techniek. Meisjes daarentegen houden zich meer bezig cybercriminaliteit in ruime zin waarbij emoties zoals woede en verdriet een rol spelen. Dit omdat meiden zich niet verdiepen in hoe en waarom maar willen vooral socialiseren, en communiceren met elkaar. Wanneer er wel meisjes betrokken zijn bij cybercriminaliteit in enge zin hebben zij de rol om vertrouwen van slachtoffers te wekken en hebben zij verder geen uitvoerende rol in het proces, stelt een geïnterviewde uit de ICT sector. Vervolgens bestaat er onder zeven geïnterviewden de gedachte dat pestgedrag meer voorkomt bij meiden en jongens daarentegen meer strafbare feiten plegen op techniek zoals hacken.

Volgens geïnterviewden is er tevens een onderscheid aan te geven tussen volwassen en jonge daders die cybercriminaliteit plegen. Zo relativeren volwassenen meer. Bij jongeren daarentegen speelt puberaal gedrag een voornamelijk rol in het plegen van een delict. Hier komt nog bij dat er een groot verschil is in intensiteit waarop volwassenen en jongeren online zijn. Zo zijn jongeren meer online dan volwassenen, stellen geïnterviewden uit de onderzoekssector.

Bij het vergelijken tussen jongeren die offline criminaliteit plegen en zij die dat online doen is er een verschil in type jongere stellen geïnterviewden uit de opsporingssector. ‘Voor offline criminaliteit moet je wat stoerder en agressiever zijn.’ Geïnterviewden uit de onderzoekssector en justitiële sector daarentegen stellen dat: ‘*Het feit dat het internet er is verplaatst alleen de criminaliteit, maar maakt de dader niet anders.’ ‘Internet verlaagt alleen de drempel en maakt het makkelijker om het te doen.’* Daarnaast wordt er gesteld dat zij die offline delicten plegen ook misdaden via internet plegen maar andersom gebeurt dit niet snel vanwege de hoge drempel.

Met betrekking tot de motivatie van daders van cybercriminaliteit wordt er door negen geïnterviewden weer gegeven dat zij het doen om stoer te zijn, vrienden te maken, respect verkrijgen, en niet om het financieel gewin. Daarentegen geeft een geïnterviewde uit de ICT sector wel weer dat financieel gewin bij een aantal jongeren wel een rol speelt. Zij worden ‘katvangers’ genoemd en lenen een pinpas van iemand waarna vervolgens een ander met ICT kennis geld van de rekening haalt. Andere motivatie is experimenteren met seksuele behoefte, prestatiedrang, en/of je willen bewijzen. Ook plegen ze cybermisdaden uit verveling of baldadigheid. Deze drijfveren wijken af van de offline drijfveren doordat de grens online

lager ligt. Jongeren zijn zich minder bewust van wat ze doen en doordat ze denken dat ze anoniem zijn handelen ze ook eerder. Daarnaast zien ze ook niet direct het resultaat, de impact, en dit is offline wel het geval.

3.2.4 Criminele carrière

De indruk onder alle participanten bestaat dat de meeste verdachte schrikken wanneer ze gepakt worden en dat ze ook weinig kwaad in de zin hadden. Een voorbeeld van een geïnterviewde uit de opsporingssector is dat iemand die gepakt is voor cybercriminaliteit in enge zin vervolgens een carrière begint als cybercrime expert. Daarbij stelt hij ook dat door een hacker op te pakken zijn/haar status wel stijgt, maar de kans wordt dan niet groter dat men recidiveert.

De groep waar wel een soort carrière bij gezien kan worden spelen zaken als een laag IQ, sociale achterstanden, middelengebruik en psychopathologie een rol. Als deze factoren samenkomen kan je een soort carrière terug zien. Tevens vallen jongeren die trots zijn op hun daad en er geen spijt van hebben vaak weer in herhaling. Om herhaling van criminele daden tegen te gaan speelt de omgeving een belangrijke rol. Er wordt gezegd door een geïnterviewde die veel met jongeren werkt in het na-traject dat jongeren niet in herhaling vallen wanneer de omgeving de jongere ondersteunt/controleert en er een positieve groepsdruk wordt uitgeoefend op de betreffende persoon.

Een geïnterviewde uit de opsporingssector stelt dat *'Bijna iedere pedofiel is een recidivist, en valt vrijwel altijd terug in zijn patroon en dat zie je ook online.' 'Zo waren er minderjarige jongens die seksueel actief waren met andere minderjarigen en die veroordeeld en behandeld zijn en vervolgens weer terug keren in de maatschappij waar ze weer een account aanmaakten om weer een zelfde seksuele activiteit uit te voeren*.' Daarentegen heeft hij bij dreigtweets nog nooit een veroordeling gezien en kan daardoor ook niet stellen of er sprake is van recidive. Verder concludeert hij dat recidive niets te maken heeft met de strafmaat.

Om te voorkomen dat jongeren toch weer in herhaling vallen zijn alle geïnterviewden het er over eens dat de strafmaat verhogen geen effect heeft, maar juist het vergroten van de pakkans zal effect hebben. Dan weten jongeren dat er consequenties zijn voor hun daden. Toch is het nog beter om voorlichting te geven. '*Als er een sexting geval plaatsvindt op een school zullen de gevolgen van deze gedraging moeten worden vertoond'*, stelt een geïnterviewde uit de opsporingssector.

Al met al blijft het moeilijk om te zeggen of jongeren in herhaling vallen, want

cybercriminaliteit wordt bij de politie vaak niet als zodanig geregistreerd, maar gewoon als bedreiging en dus niet via internet. Daardoor is het ook moeilijk te zeggen of ze ermee stoppen als ze een taakstraf hebben gekregen of doorgaan.

3.2.*5 Specifieke risico's van digitaal gedrag*

Uit de interviews komt naar voren dat er zeker specifieke risico's volgen uit het digitale gedrag van jongeren. Zo stelt een geïnterviewde uit de onderzoekssector, dat er een relatie is tussen slachtofferschap en daderschap. *'Hiertoe kunnen slachtoffers dus ook daders worden, maar ook andersom.*' Verder komt er uit alle interviews naar voren dat ondanks dat jongeren weten dat hacken strafbaar is en de pakkans laag is, ze zich toch weinig van de consequenties realiseren. Zowel de consequenties voor zichzelf als de schade aan anderen worden niet gerealiseerd door de jongeren die cybercriminaliteit in enge zin plegen. *'Ze hebben niet door dat wanneer ze gepakt worden dit ook effect heeft op hun latere carrière'*, stelt een geïnterviewde uit de ICT sector. Ook zijn jongeren die cybercriminaliteit in enge zin plegen er niet op uit om schade te veroorzaken, maar om misstanden aan het licht te brengen. Tevens zit er bij jongeren die cybercriminaliteit in enge zin plegen weinig slachtoffergevoel zegt de geïnterviewde uit de ICT sector. *'Het voelt niet voor ze dat ze slachtoffers maken, want ze krijgen niet direct feedback dat een ander er pijn van heeft. Wanneer jongeren geld van rekeningen doorsluizen naar andere rekeningen zien zij niet dat het slachtoffer geld is verloren. Vaak krijgen slachtoffers dit geld terug van banken waardoor het slachtoffergevoel helemaal verdwenen is.'* Het risico bestaat er dat jongeren zich meer bekommeren om het verhogen van hun status en dus een dergelijke tactiek gaan ontwikkelen waardoor de delicten die gepleegd worden een steeds grotere impact hebben op de maatschappij.

Wanneer jongeren cybercriminaliteit in ruime zin plegen wordt de grens tussen strafbaar en niet strafbaar erg vervaagd. De jongeren zijn zich bij deze vorm van cybercriminaliteit helemaal niet bewust van de strafbare feiten. Geïnterviewde uit de opsporingssector stelt dat *'Veel jongeren passen een struisvogeltechniek toe. Ze denken niet na maar doen gewoon.'* Volgens een geïnterviewde uit de justitiële sector zijn jongeren die cybercriminaliteit in ruime zin plegen zich er niet bewust van dat ze strafbaar bezig zijn doordat ze het uitvoeren in een opwelling. *'Op internet zeg je heel snel iets en je overziet daarvan de gevolgen niet.'* Wanneer jongeren wel worden gepakt voor hun daden schrikken ze vooral en dit werkt weer corrigerend voor de persoon zelf maar ook voor zijn/haar omgeving.

Daarentegen zijn er volgens een geïnterviewde uit de onderzoek- en politiesector ook jongeren die cybercriminaliteit in ruime zin plegen en zich wel bewust zijn van het feit dat ze

strafbaar zijn, en zij ontwikkelen dan ook een tactiek zodat ze minder snel gepakt worden. Ook stelt zij dat *'Jongeren zich niet laten leiden in gedrag wat wel of niet mag van ouders of de wet. Het hoort erbij dat jongeren de grens opzoeken, zij zijn zich aan het ontwikkelen. Deze jongeren zitten in de puberteit en die staat vaak centraal aan het uitproberen en grenzen verleggen.'* Eveneens realiseren jongeren die cybercrime in ruime zin plegen zich niet de impact die het heeft op slachtoffers.
'Iets wat op internet staat zal er altijd op blijven staan en komt er niet zomaar vanaf'.
'Iedereen kan het zien en lezen dus de impact is enorm.'

3.3 Geïntegreerde resultaten

In dit gedeelte zullen de resultaten van rechtspraak.nl en de resultaten die uit de interviews naar voren zijn gekomen met elkaar worden verbonden.

3.3.1 Combinaties cybercriminaliteit

In welke vormen en in welke mate doen zich in Nederland combinaties voor van cybercriminaliteit in enge en ruime zin gepleegd door jeugdige daders tot 18 jaar?

Met betrekking tot de verschillende vormen van cybercriminaliteit onder jongeren in Nederland blijkt zowel uit rechtspraak.nl als de interviews dat jongeren zich meer bezighouden met vormen van cybercriminaliteit in ruime zin dan in enge zin. Daarbij werd er in de interviews nog wel benoemd dat als jongeren zich bezig hielden met cybercrime in enge zin, dit dan vaak Ddos aanvallen (plaatsen van een botnet), hacken of phishing betreft. Dit zelfde gegeven blijkt ook uit rechtspraak.nl. Daarentegen blijkt uit rechtspraak.nl ook dat jongeren veelal betrokken zijn bij kinderporno, maar dit gegeven wordt niet benoemd tijdens interviews. Wel zeggen geïnterviewden dat jongeren zich dikwijls bezig houden met sexting. Hieronder kunnen zij misschien ook gedeeltelijk kinderporno verstaan, want dit behelst ook het maken van seksueel getinte beelden van kinderen. Alleen het verschil tussen deze twee strafbare feiten is dat bij kinderporno het slachtoffer altijd jonger is dan 18 jaar en dit hoeft bij sexting niet zo te zijn. Daarnaast komt sexting voort uit een relatie tussen twee personen en wanneer deze dan wordt verbroken volgt er het versturen van gemaakte beelden naar anderen.

Wat betreft de combinaties tussen cybercrime in enge zin en ruime zin blijkt zowel uit

rechtspraak.nl als de interviews dat dit niet voor komt. De combinatie cybercrime in ruime zin en offline criminaliteit blijkt daarentegen wel vaker voor te komen. Zo heeft internet een escalerend effect stelt een geïnterviewde; *'Het begint op internet en eindigt in een vechtpartij.'* Toch wordt er in de interviews niet gesproken over een combinatie tussen het verspreiden van kinderporno of seksueel beeldmateriaal en offline delicten zoals verkrachting/aanranding, afpersing etc., maar dit blijkt wel uit rechtspraak.nl.

Voor het gegeven dat er op rechtspraak.nl niet meer dan 47 zaken werden gevonden, waarin jongeren betrokken zijn als verdachten van cybercrime delicten, hebben de geïnterviewden de verklaring dat inzicht in de precieze verschijningsvormen lastig te achterhalen is omdat het rapporteren van politie en justitie tijdens aangiftes vaak niet volledig is. Als er bijvoorbeeld een bedreiging heeft plaatsgevonden via internet, dan wordt dit alleen gerapporteerd als bedreiging. Ook stellen zes geïnterviewden dat mensen vaak geneigd zijn om geen aangifte te doen en dat er bij veel vormen van (cyber)criminaliteit de dader nooit in beeld komt.

3.3.2 Achtergrondkenmerken & Motieven

Wat is er bekend over de achtergrondkenmerken van jongeren die cybercrime in enge en ruime zin (of combinatie daarvan) plegen?
Wat is er bekend over de motieven van jongeren die cybercrime in enge en ruime zin (of combinatie daarvan) plegen?

Over de achtergrondkenmerken en motieven valt op basis van rechtspraak.nl niets te concluderen. Dit vanwege het feit dat er maar in een klein aantal zaken iets over benoemd werd. Ook uit de interviews kwam naar voren dat het moeilijk is een prototype dader voor cybercrime delicten te stellen. Hierdoor kunnen er op basis van de resultaten van beide onderzoeksmethoden dus geen duidelijke conclusies betreft de achtergrondkenmerken worden getrokken.

Wel bleek dat als er iets in rechtspraak.nl of in de interviews over de achtergrondkenmerken werd genoemd dit gedragsproblematiek, zoals ADHD of autistisch spectrum stoornis, betrof of dat er bij de dader sprake is van een cognitieve en/of emotionele ontwikkelingsachterstand, waarbij er ook sprake is van een laag geestesvermogen en zwakke begaafdheid. Toch moet men wel voorzichtig zijn met de conclusies die hieruit worden getrokken, omdat er, na zo bleek uit de interviews, ook een verband is tussen daders en

slachtoffers. Zo bleek uit eerder onderzoek, van de geïnterviewden uit de onderzoekssector, dat tweederde van de daders ook slachtoffers waren.

Alhoewel uit de interviews bleek dat opleidingsniveau en gebruikersintensiteit van belang zijn bij het plegen van cybercriminaliteit kan hier met behulp van rechtspraak.nl niets over gezegd worden. Wel het feit dat in de interviews naar voren komt dat het niet altijd 'einzelgängers' zijn die cybercriminaliteit plegen wordt ondersteunt met rechtspraak.nl. Zo bleek dat er in 17 zaken meerdere daders betrokken waren bij hetzelfde delict.

Ook het onderscheid tussen de vormen waar jongens en meisjes zich mee bezighouden dat uit de interviews naar voren komt kan niet worden ondersteund met rechtspraak.nl, want hieruit blijkt dat meisjes veelal niet als dader betrokken zijn bij cybercrime. Eveneens bleek uit de interviews dat meisjes dikwijls betrokken zijn bij cybercrime in ruime zin en hoewel dit vaker voor komt in rechtspraak.nl zijn meisjes hier toch niet als daders bij betrokken. Dit kan ook liggen aan het feit dat ze het in de interviews vooral hebben over treiter en pestgedrag tussen meisjes onderling via internet en hiervan worden geen zaken gevonden op rechtspraak.nl.

Met betrekking tot de motivatie van daders blijkt zowel uit de interviews als rechtspraak.nl dat het niet gaat om het financiële gewin, maar vooral de behoefte aan macht, aanzien, erbij willen horen, jaloezie en experimenteren met seksuele behoefte

3.3.3 Criminele carrière

Wat is er bekend over de criminele carrières van jongeren die verschillende vormen van cybercrime plegen en in welke mate plegen zij herhaaldelijk vormen van cybercrime?

Over de criminele carrières van jongeren met betrekking tot cybercriminaliteit valt met behulp van rechtspraak.nl niets te concluderen. Zo wordt er maar in een klein aantal zaken over recidive risico en of de dader althans gedetineerd is geweest gesproken. Uit de interviews daarentegen blijkt dat er onder alle participanten de indruk bestaat dat verdachten schrikken wanneer ze gepakt worden en helemaal geen intentie hadden om kwaad te verrichten. Ook bleek er uit de interviews dat er wel degelijk een groep is waarbij een carrière kan worden gezien. Bij deze groep zouden dan zaken als een laag IQ, sociale achterstand, middelenmisbruik en psychopathologie een rol spelen. Daarnaast kan trots zijn op je daad ook een voorspeller zijn voor het weer in herhaling vallen. Of dit ook daadwerkelijk factoren zijn die een voorspellende waarde hebben op het recidive risico is met behulp van rechtspraak.nl

niet te ondersteunen.

Al met al blijft het moeilijk om te zeggen of jongeren in herhaling vallen, niet alleen vanwege het feit dat daar in rechtspraak.nl in de meeste gevallen niets over wordt gezegd maar ook vanwege het feit dat cybercriminaliteit bij de politie vaak niet zo wordt geregistreerd. Ze registreren het vaak als gewoon bedreiging en dus niet via internet. Daardoor is het ook moeilijk te zeggen of ze ermee stoppen als ze een taakstraf hebben gekregen of doorgaan.

3.3.4 Specifieke risico's van digitaal gedrag

Zijn er op basis van alle gestelde onderzoeksvragen nog specifieke risico's die volgen uit het digitale gedrag van jongeren en hun mogelijke betrokkenheid als daders van cybercrime? Zo ja, welke?

Vooral uit de interviews komt naar voren dat jongeren die zich wel bezighouden met cybercrime in enge zin wel degelijk weten dat zij strafbaar zijn, maar ze weten dat de pakkans laag is. Een geïnterviewde uit de opsporingssector haalt dit gegeven uit het feit dat ze hun naam er niet onder zetten, maar een nickname gebruiken die voor hen belangrijk is, want dat is hun identiteit en is soms ook belangrijker dat hun echte identiteit. Hierdoor zijn ze ook minder verbonden met de echte wereld waarin er consequenties zijn voor je daden. Doordat jongeren weten dat ze toch niet gauw gepakt zullen worden zullen ze blijven doorgaan. Ze zullen betere tactieken gaan ontwikkelen, hun kennis uitbreiden waardoor ze nog meer schade aan de maatschappij kunnen gaan aanrichten.

Voor cybercrime in ruime zin geldt dat jongeren in de meeste gevallen niet eens weten dat ze strafbaar zijn. Dit is natuurlijk niet voor alle vormen van cybercriminaliteit in ruime zin. Zo weten jongeren wel degelijk dat het verspreiden van kinderporno strafbaar is, maar bijvoorbeeld uit wraak of jaloezie rondsturen van seksueel getinte beelden of belastende teksten weer niet. Hierbij handelen jongeren uit emotie en gaan onbewust een strafbare grens over. Wanneer ze dan gepakt worden heeft dit een negatief effect voor hun latere werkcarrière. Dus zullen jongeren bewuster moeten worden van hun gedrag op het internet. Daarnaast is er een verwevenheid tussen daders en slachtoffers. Zo bleek uit eerder onderzoek, van de geïnterviewden uit de onderzoekssector, dat tweederde van de daders ook slachtoffers waren.

Al met al is het internet een makkelijk medium om je delicten te plegen. Je bent anoniem,

ziet de gevolgen niet direct, het is sneller, bereikt meer mensen en je kunt je anders voordoen dan je bent. Door de voordelen van het internet en het experimenteergedrag dat bij de adolescentie periode hoort zullen jongeren sneller grenzen overschrijden en daarmee bewust of onbewust ook strafbare grenzen. Dit moet een halt toe worden geroepen, want het brengt een grote persoonlijke en ook maatschappelijke schade met zich mee. Daarbij zijn alle geïnterviewde het erover eens dat de strafmaat verhogen geen invloed heeft op het terugdringen van cybercriminaliteit onder jongeren maar dat de pakkans juist vergroot moet worden om deze criminaliteit tegen te gaan.

4. Discussie

Doordat jongeren steeds mobieler worden en steeds makkelijker met internet omgaan is de kans dat ze in aanraking komen met cybercriminaliteit groter. Internet wordt steeds toegankelijker en is een anoniem medium waar jongeren ook steeds meer de voordelen van inzien. In dit beschrijvende onderzoek is er dan ook getracht inzicht te krijgen in zowel de vormen van cybercrime in Nederland waarbij jongeren tot 18 jaar betrokken zijn, als hun achtergrondkenmerken, motieven en criminele carrières. Deze inzichten zijn verkregen met behulp van twee onderzoeksmethoden; analyse van zaken uit rechtspraak.nl en interviews. Door gebruik te maken van twee verschillende onderzoeksmethoden kan er worden bekeken of de resultaten van beide onderzoeksmethoden met elkaar overeenkomen of verschillen, en kunnen de resultaten elkaar aanvullen.

Vormen

Als eerst is er uit de resultaten gebleken dat cybercriminaliteit in ruime zin dikwijls meer onder jongeren tot 18 jaar plaatsvindt dan cybercrime in enge zin. De vormen van cybercrime in ruime zin die in dit onderzoek naar voren komen en vooral voorkomen zijn: kinderporno, sexting en bedreiging. Daarbij blijkt alleen uit de interviews dat cyberpesten en grooming ook veelvuldig voor komt onder jongeren. Een reden waarom dit niet teruggevonden wordt in rechtspraak.nl is dat pesten niet strafbaar is en er dus ook geen aangiftes voor worden gedaan. Voor grooming geldt dat hier vaak geen aangiftes voor worden gedaan en het dus ook moeilijk zichtbaar is. Hierdoor kan het probleem cybercrime groter zijn dan het lijkt. Wanneer deze resultaten worden vergeleken met eerder onderzoek dan blijkt dat in dit onderzoek er andere vormen naar voren komen. Zo vonden Leukfeldt et al. (2010) dat vooral de vormen e-fraude, haatzaaien op internet, hacken en verspreiden van kinderporno voorkomen onder jongeren. Een reden voor dit verschil kan liggen in het feit dat Leukfeldt et al (2010) hun onderzoek hielden onder 12-24 jarigen en dit onderzoek is gebaseerd op jongeren tot 18 jaar.

Verder is uit beide onderzoeksmethoden gebleken dat er bij cybercrime in enge zin vrijwel geen combinaties zijn met cybercrime in ruime zin of offline criminaliteit. Voor cybercrime in ruime zin ligt dit anders. Hier wordt bij beide onderzoeksmethoden wel een combinatie gevonden met offline criminaliteit. Zo kan een conflict beginnen op internet en eindigen in een mishandeling.

Achtergronden

Wanneer er wordt geprobeerd het gedrag van de jongere met betrekking tot cybercriminaliteit te verklaren blijkt dat het ASE-model (De Vries et al., 1988) in combinatie met het Sociaal-Ecologisch Model van Bronfenbrenner (1979) goed kan worden toegepast. Zo blijkt uit de interviews dat jongeren kennis hebben van computers en doordat ze veel achter de computer zitten meer vaardigheden opbouwen, wat ook overeenkomt met onderzoek van Livingstone en Helsper (2007). Daarnaast weten jongeren dat de pakkans laag is, maar weten ze niet altijd dat ze strafbaar bezig zijn. Dit kunnen redenen zijn om crimineelgedrag te vertonen.

Voor het verklaren van het effect van sociale invloed op crimineel gedrag is er gebruik gemaakt van het Sociaal Ecologisch Model van Bronfenbrenner (1979). Deze stelt dat een jongere wordt beïnvloed door vier verschillende niveaus: de jongere zelf, het gezin, school en vrienden, en maatschappelijk en cultureel niveau. Al deze vier niveaus komen ook terug in dit onderzoek. Zo zijn er persoonlijkheidskenmerken zoals: (licht) autistisch, introvert, een cognitieve en emotionele achterstand, en laag IQ, uit beide onderzoeksmethoden naar voren gekomen als factoren die verband kunnen houden met daderschap van cybercriminaliteit.

Over de rol die het gezin in het geheel speelt komt in dit onderzoek niet veel naar voren. Wel blijkt uit de interviews dat de omgeving een ondersteunende rol kan spelen bij het voorkomen van crimineel gedrag. Over schoolprestaties wordt zowel in de interviews als in rechtspraak.nl niets genoemd. Wel blijkt dat jongeren vanwege hun motivatie om bij de groep te willen horen of om aanzien/macht te krijgen ze het gedrag vertonen. Dus zoals Bronfenbrenner al stelt speelt het gezin en de vrienden wel degelijk een rol bij het verklaren van (cyber)crimineel gedrag.

Wat betreft het maatschappelijk en cultureel niveau komt er naar voren dat er een kloof is tussen ouder en kind. Zo hebben veel jongeren toegang tot internet, maar is er geen controle van ouders op het computergebruik. Ze hebben in mindere mate een sociale binding. Dit is in overeenstemming met de bindingstheorie van Hirsch (1969) die ervan uit gaat dat jongeren die delinquentgedrag vertonen te weinig sociale controle hebben ervaren van onder andere hun ouders, familie, vrienden en school. Jongeren die weinig of geen contact hebben met hun ouders of familie, hebben het idee dat ze toch niets te verliezen hebben want ze horen als het ware niet bij een sociaal netwerk en worden niet aangesproken op hun delinquentgedrag. Het feit dat er geen tot weinig sociale controle is op de jongeren wat betreft computergebruik kan een mogelijke reden zijn tot het vertonen van crimineel gedrag, maar hier moet nog eerst meer onderzoek naar gedaan worden.

Over de zelfeffectiviteit is bekend uit de resultaten dat jongeren hun vaardigheden

ontwikkelen door meer achter internet te zitten. Door meer vaardigheden te ontwikkelen kunnen ze deze ook op meerdere terreinen inzetten en daarmee ook strafbare grenzen overgaan. Dat ze de strafbare grens overgaan hebben jongeren niet altijd in de gaten, maar ze weten wel dat de pakkans erg laag is. Wanneer hun ervaring is dat zij zich vrijuit kunnen bewegen op het internet zonder daar de consequenties van te ondervinden dan zullen ze dat gedrag ook blijven voortzetten.

Ondank dat het model goed toepasbaar is in dit onderzoek kan er op basis van de gevonden resultaten toch geen duidelijke conclusies worden getrokken. Dit aangezien het feit dat er op rechtspraak.nl in de meeste zaken niets over wordt genoemd en zodoende de uitspraken in de interviews niet voldoende kunnen worden getoetst. Daarnaast zeggen de geïnterviewden ook allen dat het moeilijk is een prototype dader te stellen.

Motieven

Verder blijkt uit het onderzoek dat er verschillende motieven zijn voor het plegen van cybercrime. Om een verklaring te geven voor de motivatie wordt er gebruik gemaakt van de Rationele Keuze Theorie (RKT) of de Routine Activiteiten Theorie (RAT). Uit dit onderzoek blijkt dat jongeren niet altijd stilstaan bij de consequenties, maar gewoon handelen. Hierbij denken ze dus niet rationeel na over de keuzes die ze hebben. Dit is dus in tegenstelling tot wat de RKT stelt en komt meer overeen met wat de RAT stelt. Jongeren hebben een motief om een delict te plegen, zoeken of hebben daarbij een (makkelijk) slachtoffer en voeren dit uit via internet aangezien ze weten dat hier de pakkans laag is. Verder blijkt dat de meest gangbare motieven voor het plegen van cybercriminaliteit, behoefte aan macht, aanzien, erbij willen horen, jaloezie en experimenteren met seksuele behoefte, zijn. Hierbij speelt financieel gewin in de meeste gevallen geen rol. Deze resultaten komen veelal overeen met eerder gevonden motieven uit onderzoek van Geffen et al. (2005) en Kerstens en Stol (2012).

Criminele carrière

Over de criminele carrière kan met behulp van beide methodes geen duidelijke conclusies worden getrokken. Zo bestaat er de gedachte onder de geïnterviewden dat de grootste groep jongeren wel schrikt wanneer ze opgepakt worden en het dan niet nog een keer zullen doen. Dit komt overeen met wat Ferwerda (1992) en Janssen (1989) stellen dat crimineelgedrag leeftijdsgebonden 'kickgedrag' is, dat voortkomt uit het experimenteergedrag.

Daarentegen stellen geïnterviewden ook dat er altijd wel een groep is die weer recidiveert, maar bij deze groep zullen factoren als psychopathologie, sociale achterstand en een laag IQ

een rol spelen. Dit komt overeen met de gevonden resultaten van Van der Laan en Blom (2010). Alleen hebben zij gevonden dat in 2008 42% van de jongeren weer was gerecidiveerd. Of dit daadwerkelijk ook zo is kan er met behulp van dit onderzoek niet worden geconcludeerd. Dit vanwege het feit dat de gevonden resultaten uit de interviews niet met behulp van rechtspraak.nl kunnen worden ondersteund, omdat er maar in acht zaken wordt gesproken over recidiverisico of dat het een destijds gedetineerde verdachte is of niet.

Specifieke risico's van digitaal gedrag

Zowel cybercrime in ruime- als enge zin brengt veel schade toe aan de maatschappij. Alles wat op internet wordt geplaatst gaat er niet zo weer vanaf, iedereen kan het lezen/zien. Daarnaast zien daders niet direct de gevolgen en impact van hun gedrag op slachtoffers en zullen daardoor mogelijk hun gedrag voortzetten. Volgens geïnterviewde zullen de daders die cybercrime in enge zin plegen daarbij betere tactieken gaan ontwikkelen en hun kennis gaan uitbreiden waardoor ze nog meer schade aan de maatschappij kunnen gaan aanrichten.

Daarnaast komt naar voren in de interviews dat jongeren die cybercrime in ruime zin plegen zich vaak niet realiseren dat zij strafbaar bezig zijn en dus ook niet weten welke impact het op henzelf heeft wanneer ze gepakt worden door de politie. Zij zullen dus bewust moeten worden gemaakt van de grenzen van (strafbaar)gedrag en de impact die het heeft op slachtoffers en henzelf, wanneer ze gepakt worden.

Tevens is er een verwevenheid tussen daders en slachtoffers blijkt uit zowel de interviews als eerder onderzoek van geïnterviewden uit de onderzoekssector. Hierdoor blijft men in een vicieuze cirkel en deze moet doorbroken worden om zo de maatschappelijke en persoonlijke schade terug te brengen.

Limitaties

Uit bovenstaande resultaten blijkt al wel dat beide onderzoeksmethoden zowel hun voor delen als beperkingen hebben. Zo is rechtspraak.nl een database waarin 230.000 uitspraken in beschreven staan. Zo heb je dus een veelheid aan zaken, die op basis van hun uniekheid zijn verkozen om in de database te komen, waardoor je dus een uitgebreid kader hebt waarin je kunt zoeken. Zoals beschreven in hoofdstuk 2 is er gezocht met verschillende zoektermen. Doordat deze zoektermen heel breed waren kwam er veel ruis in de zoekresultaten naar voren. Hierbij was het niet mogelijk om specifiek te zoeken, de database was hiervoor nog niet voldoende ontwikkeld. Om deze beperking zoveel mogelijk te ondervangen is er gezocht met

termen die in de rechtspraak gehanteerd worden, zoals bijvoorbeeld: verdachten in plaats van daders, geautomatiseerd netwerk en telecommunicatie netwerk. Ook is er gewerkt met inter-beoordelaarsbetrouwbaarheid. Twee onderzoekers hebben de database doorzocht en hebben de helft van elkaars gevonden zaken nogmaals geanalyseerd met behulp van de inclusie- en exclusie criteria. Hierdoor is er getracht de betrouwbaarheid van de gevonden zaken en kenmerken te vergroten.

Een andere beperking van rechtspraak.nl is dat er niet bij alle zaken wat genoemd over bijvoorbeeld de achtergrondkenmerken of mate van recidive. Dit kan te maken hebben met het feit dat zij dit alleen beschrijven wanneer het invloed heeft op de uitspraak van de zaak. Hierdoor kan er dus niet gesteld worden dat er in de gevonden zaken, die betrekking hebben op cybercrime, er bijna tot geen sprake is van recidive risico of dat zij allen first-offenders zijn en er dus geen sprake is van een criminele carrière. Hiertoe is er te weinig informatie. Hetzelfde geldt voor achtergrondkenmerken. Hierdoor kunnen er geen generalisaties worden gemaakt over achtergrondkenmerken van jongeren in het algemeen die cybercrime plegen. Toch wordt het nadeel dat niet alle informatie bij elke zaak vermeld staat ondervangen door interviews af te nemen bij mensen die in hun werk te maken hebben met cybercriminaliteit en jongeren. Zo kunnen geïnterviewden op basis van hun ervaringen en kennis wel achtergrondkenmerken weergeven.

Tevens is er nog een voordeel van het analyseren van zaken uit de database rechtspraak.nl. Zo is dit een makkelijk toegankelijke database waar iedereen zo bij kan komen en welke eveneens vaak wordt vernieuwd zodat je op de hoogte blijft van nieuwe zaken.

Verder is er naast het analyseren van zaken in rechtspraak.nl ook nog gebruik gemaakt van het afnemen van interviews. Hierdoor kan er worden gekeken of de resultaten van beide onderzoeksmethoden elkaar ondersteunen, tegenspreken en/of aanvullen. Een interview is een doelgericht gesprek tussen twee of meer personen (Kahn & Cannel, 1957). Ter vergroting van de betrouwbaarheid is er in dit onderzoek voor gekozen om altijd twee of meer onderzoekers bij het interview aanwezig te laten zijn. Één persoon nam het interview af en de ander(en) notuleerden. Hierdoor is er extra controle op wat en hoe een geïnterviewde iets weergeeft en of het juist genotuleerd wordt.

Verder blijkt dat de interview methode goed aansluit bij de onderzoeksvragen. Zo is dit een beschrijvend/verkennend onderzoek en Cooper en Schindler (1998) stellen daarover dat er dan goed gebruik gemaakt kan worden van de interview methode. Toch zitten er ook beperkingen aan de interview methode. Zo is er gevraagd naar ervaringen en kennis, maar geïnterviewden hadden wel de neiging om te praten vanuit ideeën. Om er toch voor te zorgen

dat geïnterviewden dit niet deden werd er nadrukkelijk vermeld dat het ging om de ervaringen en kennis van de geïnterviewden en werd dit ook herhaald tijdens het interview. Niettemin blijft een interview subjectief en daardoor is er ook voor gekozen om tien belangrijke sleutelfiguren, die werkzaam zijn binnen het gebied van cybercriminaliteit en jongeren te interviewen, zodat er naderhand een algeheel beeld van cybercriminaliteit kan worden geschetst. Al deze geïnterviewden kwamen uit verschillende bedrijfstakken en verschillende delen van het land, waardoor de verkregen informatie gezamenlijk een goed algeheel beeld kan geven. Daarentegen bestaat er bij het afnemen van interviews altijd de kans dat er niet de juiste vragen worden gesteld, of er niet genoeg wordt doorgevraagd. Dit gegeven is ondervangen door een aantal dezelfde vragen op verschillende manieren terug te laten komen in het interview. Hierdoor kan men kijken of de geïnterviewde de vragen op dezelfde manier beantwoord en ze daarmee ook begrepen heeft. Daarnaast zijn er door de geïnterviewden geen getallen genoemd. Daardoor kan er niet met zekerheid kan worden gezegd in welke mate bepaalde vormen van cybercriminaliteit zich nu daadwerkelijk voor doet, onder jongeren.

Tenslotte stellen sommige auteurs dat het onderscheid tussen cybercrime en traditionele delicten niet helder te maken is (Hulst & Neve, 2009; McCusker, 2006). Delinquenten handelen niet binnen de kaders van de wet. Het is wellicht zo dat zij bij het plegen van traditionele delicten steeds meer ICT gebruiken. Zoals bijvoorbeeld diefstal; vroeger werd je op straat beroofd, en tegenwoordig is er steeds meer sprake van dat dit via het internet gebeurd, door bijvoorbeeld iemand zijn account te hacken. Behalve inhoudelijke redenen om aan te nemen dat de traditionele criminaliteit aan het veranderen is, zijn er redenen om aan te nemen dat deze ontwikkeling niet helder naar voren komt uit de politiesystemen. Zo komt er in de interviews nadrukkelijk naar voren dat cybercriminaliteit vaak niet zo in de aangiftes wordt vermeld door de politie. Dit zelfde gegeven blijkt ook uit onderzoek van Hartel, Junger, & Wieringa (2010). Zij stellen dat politie soms de minder goed begrepen ICT-aspecten van het delict, niet opnemen in de aangifte. Zo wordt fraude gepleegd met behulp van een internet, vaak geclassificeerd als gewone fraude, zonder dat daarbij vermeld wordt welke rol ICT daarbij heeft gespeeld (Hartel, Junger, & Wieringa, 2010). Om deze reden is het moeilijk zicht te krijgen op de aard en omvang van cybercriminaliteit onder jongeren in Nederland en zal er eerst nog vervolg onderzoek moeten worden verricht voordat er interventies kunnen worden ontworpen om deze vorm van criminaliteit onder jongeren in Nederland de hand te bieden.

5. Aanbevelingen

Na het beantwoorden van de onderzoeksvragen en de discussies die deze resultaten opleveren, kunnen aanbevelingen worden geformuleerd, die suggesties bieden voor verder onderzoek op het gebied van cybercriminaliteit en jeugd. Dit verdere onderzoek zal de betrokkenheid van jongeren bij cybercriminaliteit, hun achtergrondkenmerken en de mate van recidive verder vormgeven.

Allereerst zou er doormiddel van het aanpassen van de manier van registratie van aangiftes duidelijk kunnen worden gemaakt wanneer ICT middelen een rol hebben gespeeld in het delict. Zodoende kan er een duidelijker beeld worden gevormd van het probleem cybercriminaliteit onder jongeren in Nederland.

Onderzoek naar achtergrondkenmerken van jongeren die cybercriminaliteit plegen
Het blijkt uit onderzoek dat er mogelijk wel degelijk achtergrondkenmerken zijn die kenmerkend zijn voor jonge cybercriminelen. Toch is het nog niet duidelijk of deze kenmerken gegeneraliseerd kunnen worden naar jonge cybercriminelen over het algemeen of alleen naar een jonge cybercriminelen die zich met een specifieke vorm van cybercrime bezighouden. Middels het analyseren van politiedossiers en onderzoek onder de jongeren zelf kan hier meer inzicht in verkregen worden. Daarnaast zou er ook onderzoek kunnen worden verricht naar verschillen tussen cybercriminaliteit waar jongens en meisjes zich mee bezighouden. Verder zou opleidingsniveau mogelijk ook nog een rol kunnen spelen bij verschillende vormen van cybercriminaliteit en daar zou dan ook nog verder onderzoek naar kunnen worden gedaan.

Onderzoek naar invloed van het gezin, vrienden en school op jongeren die cybercriminaliteit plegen.
Er is gebleken dat er geen tot weinig sociale controle is op de jongeren wat betreft computergebruik en dit kan mogelijk een reden zijn tot het vertonen van (cyber)crimineelgedrag. Daarnaast blijkt uit onderzoek van Bosman (2011) dat jongeren het toezicht ook weinig effectief vinden. Deze bevindingen kunnen in een vervolg onderzoek verder uitgediept worden, vanwege de mogelijke rol van ouders, vrienden en school in het voorkomen of aanpakken van cyber crimineelgedrag. Hierbij moet aandacht besteed worden aan de vraag waarom ouders relatief weinig toezicht bieden. Dit zou bijvoorbeeld te maken

kunnen hebben met het feit dat ouders zelf misschien in mindere mate computerkennis hebben er vanuit gaan dat een jongere door zijn computerkennis wel weet hoe alles werkt. Ook is gebleken dat vrienden en school mogelijk een rol kunnen spelen bij het voorkomen van cybercriminaliteit. Positieve groepsdruk kan hierbij een beschermende factor zijn. Toch is de rol hiervan niet duidelijk en is het wenselijk dat hier vervolg onderzoek naar gedaan wordt. Hierbij kan er mogelijk gebruik worden gemaakt van een experimentele setting, waarbij er een groep jongeren is die positief wordt ondersteund en/of controle ervaart van ouders en het effect op hun internetgedrag en een groep die geen positieve ondersteuning en/of controle van ouders ervaart.

Onderzoek naar criminele carrières van jongeren die cybercriminaliteit plegen.
Vanwege het feit dat er in dit onderzoek niet is kunnen concluderen of jongeren die cybercriminaliteit plegen vaak weer in herhaling vallen en een criminele carrière opbouwen of niet, is het wenselijk dat hier vervolg onderzoek naar verricht wordt. Zodoende kan men interventies gaan opstellen om recidive, bij jongeren die cybercriminaliteit plegen, te voorkomen. Een vervolg onderzoek zal zich dan moeten richten op het analyseren van strafdossiers, Halt-dossiers en dossiers van HKE.

Referenties

Ajzen, I. (1988). *Attitudes, personality and behavior*. Milton Keynes: Open university press.

Bauwens, J., Pauwels, C., Lobet-Maris, C., Poulet, Y., & Walrave, M. (2009). *Cyberteens, cyberrisks cybertools. Les teenager et les TIC, risqué et oppertunités*. Gent, Academia Press.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76, 169-217.

Bosker, J., Witteman, C., & Hermanns, J. (2013). Do intervention plans meet criteria for effective practice to reduce recidivism? How probation officers forget about social capital and basisc needs. *European Journal of Probation, 5*, 1, 65-85.

Bosman, E. (2011). *Treiteren, schelden, bedreigen en buitensluiten: Jongeren en de keerzijde van de digitale wereld - Een kwalitatief en kwantitatief onderzoek naar oordelen over en ervaringen met digitaal asociaal gedrag ten opzichte van regulier asociaal gedrag door Nederlandse jongeren.* Master scriptie universiteit Twente.

Bronfenbrenner, U. (1979). *The ecology of human development: Experiments by nature and design.* Harvard University Press, Cambridge, Massachusetts.

Brug, J., Schaalma, H., Kok, G., Meertens, R. M., & Van der Molen, H. T. (2003). *Gezondheidsvoorlichtingen gedragsverandering. Een planmatige aanpak*. Assen: Koninklijke Van Gorcum BV.

Centraal Bureau voor de Statistiek (2012). *ICT gebruik van personen naar persoonskenmerken*. Verkregen op 28 juni 2013 via http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=71098NED&D1=33&D2=0-2&D3=a&VW=T en http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=71098NED&D1=69&D2=0-2&D3=a&VW=T

Erikson, E. H. (1995). *Identity: Youth and crisis*. New York: W.W. Norton & Company.

Eysenk, H.J. (1996). Personality and crime: Where do we stand? *Psychology, Crime and Law*, *2,* (3), 143-152.

Felson, M. (2003). The Routine Activity Approach as a General Crime Theory. In E. McLaughlin, J. Muncie & G. Hughes (Eds.). *Criminological perspectives Essential Readings 2nd edition*. London: Sage, 160-166.

Ferwerda, H.B. (1992). *Watjes en ratjes. Een longitudinaal onderzoek naar het verband tussen maatschappelijke kwetsbaarheid en jeugdcriminaliteit*. Groningen: Wolters-Noordhof B.V.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, and behavior*. New York: Wiley.

Geffen, van, C.L.W., Gumbs, T. T., Feltzer, M. J. A., Vlugt, van der, H., & Hellings, E. (2005). *Relatie tussen persoonlijkheidseigenschappen en risicogedrag bij Antilliaanse jongeren op Curaçao.* Afstudeerrichting Kinder- en Jeugdpsychologie. Tilburg: Universiteit van Tilburg.

Griffiths, J. (1995). Normative and Rational Choice Accounts of Human Social Behavior. *European Journal of Law and Economics,* 2, 285-299.

Hartel, P., Junger, M., & Wieringa, R. (2010). *Cyber-crime science = crime science + information security.* Report. Enschede: Universiteit Twente. Verkregen van http://eprints.eemcs.utwente.nl/18500/

Heiden-Attema, N., & Bol, van der, M.W. (2000*). Moeilijke jeugd: risico- en protectieve factoren en de ontwikkeling van delinquent gedrag in een groep risicojongeren.* Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum.

Heijkants, A.A.H., & Snijder, B. (1999). *Risicogedrag van jongeren en persoonlijkheid.* Doctoraalscriptie Kinder- en Jeugdpsychologie. Tilburg: Universiteit van Tilburg.

Hirschi, T. (1969). *Causes of delinquency.* Los Angeles: University of California Press

Hof, van 't, C., & Haan, J. de (eds.). (2006) *De digitale generatie: Welke rol speelt ICT in het leven van jongeren?* Jaarboek ICT & Samenleving. Amsterdam: Boom.

Huisman, W. (2001). *Tussen winst en moraal. Achtergronden van regelnaleving en regelovertreding door ondernemingen*. Den Haag : Boom Juridische uitgevers. 45-71, 137-167.

Hulst, R.C., & Neve, van der, R.J.M. (2008*). High-tech crime, soorten criminaliteit en hun daders.* WODC rapport, Meppel: Boom Juridisch uitgevers.

Hulst, R.C., & Neve, van der, R.J.M. (2009). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: Boom Juridische uitgevers, WODC.

Janssen, J. (1989). Delinquentie als 'crime de passage'. *Jeugd en Samenleving*, 19, 2-3, 114-129.

Junger-Tas, J., Steketee, M., & Moll, M. (2008). *Achtergronden van jeugdcriminaliteit en middelengebruik.* Verkregen op 7 januari, 2013, via http://www.verwey-jonker.nl/jeugd/publicaties/beleid/achtergronden_van_jeugddelinquentie_en_middelengebruik_

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

Kowalski, R., Limber, S., & Agatston, P. (2008). *Cyberbullying: Bullying in the digital age*. Malden: Blackwell Publishers.

Kromhout, M., & San, van, M. (2003). *Schimmige werelden. Nieuwe etnische groepen en jeugdcriminaliteit.* Meppel: Boom juridische uitgevers.

Laan, van der, A. M., & Blom, M. (2005). *Jeugddelinquentie: risico en bescherming: jeugdmonitor zelfgerapporteerde jeugdcriminaliteit*. WODC. Ministerie Veiligheid en Justitie.

Laan, van der, A. M., & Blom, M. (2010). *Jeugdcriminaliteit in de periode 1996-2010: Ontwikkelingen in zelfgerapporteerde daders, door de politie aangehouden verdachten en strafrechtelijke daders op basis van de Monitor Jeugdcriminaliteit 2010*. WODC. Ministerie Veiligheid en Justitie.

Leijenhorst, van, L. (2010). *Why teens take risks: a neurocognitive analysis of developmental changes and individual differences in decision-making under risk.* Thesis Leiden University. Enschede: Print Partners Ipskamp B.V.

Leukfeldt, E. R., Domenie, M. L. & Stol, W. Ph. (2010). *Verkenning Cybercrime in Nederland 2009*. Den Haag: BJU.

Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: children, young people and the digital divide. *New media & society*, 9, 4, 671-696. Doi:10.1177/1461444807080335.

Loeber, R. (1998). Ontwikkelingspaden en risicopatronen voor ernstige jeugddelinquentie en hun relevante interventies: Nooit te vroeg en nooit te laat. In: W. Koops & W. Slot (Red.), *Van lastig tot misdadig*. Houten: Bohn Stafleu van Loghum.

Loeber, R., Slot, N.W., & Sergeant, J.A. (2001) *Ernstige en gewelddadige jeugddelinquentie: Omvang, oorzaken en interventies.* Houten/Diegem: Bohn Stafleu Van Loghum.

Luijpers, E.T.H. (2000) *Intentie tot exploratie, sociale binding en delinquent gedrag van Nederlandse jongeren.* Verkregen op 25 februari, 2009, via http://igitur-archive.library.uu.nl/dissertations/1914276/full.pdf

McCusker, R. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime, law and social change*, 46, 257--273.

Mooren, van der, C.T. (2006). *Opvoeding op school en in het gezin: Onderzoek naar de samenhang tussen opvoeding en de houding van jongeren ten opzichte van sociale grenzen.* Proefschrift rijksuniversiteit Groningen.

NCSC. (2012). *Handreiking Cybercrime: van herkenning tot aangifte*. Den Haag: nationaal Cyber Security Centrum.

Ploeg, van der, J.D., & Scholte, E.M. (1990). *Lastposten of slachtoffers van de samenleving.* Rotterdam: Lemniscaat.

Pratt, T. C., Holtfreter, K., Reisig, M.D. (2010). Routine Online Activity and Internet Fraud Targetting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47 (3), 267-296.*

Rooij, van, T., & Eijnden, R. van den. (2007). *Monitor internet en jongeren 2006 en 2007: Ontwikkelingen in internetgebruik en de rol van opvoeding*. Rotterdam: IVO.

Sampson, R.J. & Laub, J. (1993). *Crime in the making- Pathways and turning points through life.* Cambridge, Harvard University Press.

Schols, M., Duimel, M., & Haan, de, J. (2011). *Hoe cultureel is de digitale generatie? Het internetgebruik voor culturele doeleinden onder schoolgaande tieners.* Den Haag: Sociaal en Cultureel Planbureau.

Siegel, L.J. (2010). *Criminology. Theories, Patterns, and Typologies*. Belmont: Wadsworth.

Smet, de, S., & Mahjoub, S. (2008). *Op het scherp van het net: Een verkennende studie over jongeren, internet en betaalseks*. Anderlecht: Impresor.

Stol, W.Ph. (2004) Trends in cybercrime. *Justitiële Verkenningen*, 30, 8, 76-94.

Stol, W.Ph. (2004) *Handhaven: eerst kiezen, dan doen. Technische mogelijkheden en beperkingen.* Den Haag: Ministerie van Justitie.

Stol, W.Ph. (2008) Cybercrime. In W.Ph. Stol en A.Ph. van Wijk (red.), *Inleiding criminaliteit en opsporing,* Den Haag: BJU; pp. 65-77.

Stol, W.Ph. (2008) De politie. In W.Ph. Stol en A.Ph. van Wijk (red.), *Inleiding criminaliteit en opsporing,* Den Haag: BJU; pp. 137-150

Stol, W. Ph., Leukfeldt, E. R., & Klap, H. (2012). Cybercrime en politie; een schets van de Nederlandse situatie anno 2012. *Justitiële Verkenningen*, 38(1), 25-39.

Ultee, W. C., Arts, W.A., & Flap, H.D. (2003). *Sociologie: vragen, uitspraken en bevindingen.* Groningen/Houten: Wolters-Noordhoff.

Uggen, C. (2000). Work as a turning point in the life course of criminals: A duration model of age, employment and recidivism. *American Sociological Review*, 65, 4, 529-546.

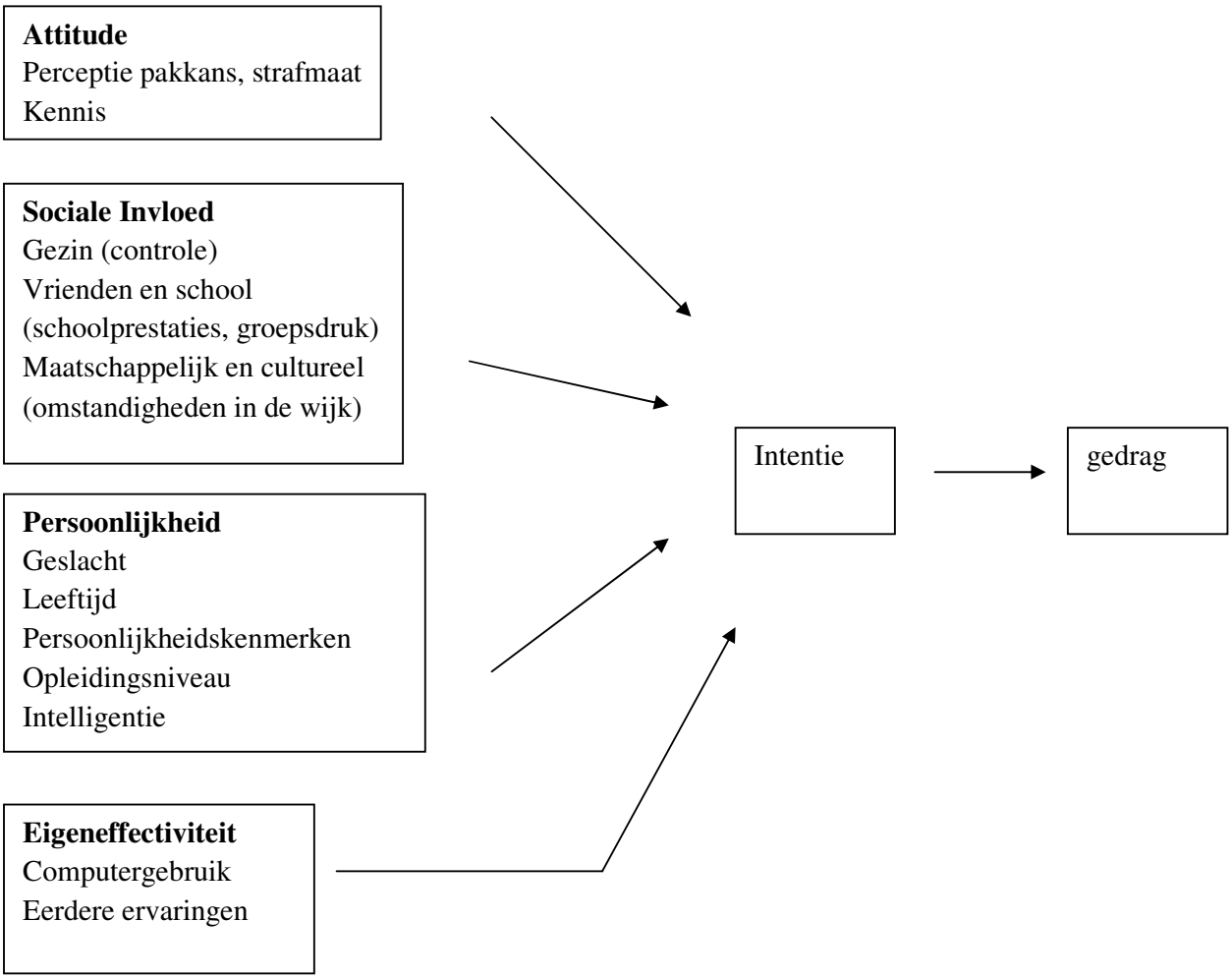
Vries, de, H., Dijkstra, M., & Kuhlman, P. (1988). Self-efficacy: The third factor besides attitude and subjective norm as a predictor of behavioral intentions. *Health Education Research*, 3. 273-282

Wilsem, van, J. (2010). Ditgitale en Traditionele Bedreiging Vergeleken: Een Studie Naar Risicofactoren van Slachtofferschap. *Tijdschrift voor Criminologie*, 52 (1), 73-87.

Witteveen, W.J. (2010). De retoriek van een onpartijdige waarnemer. (Review of the book The Idea of Justice, A. Sen, 2009). *De Academische Boekengids, 2010, 82*, 3-5.

Wright, B.R., Entner, A., Caspi, T.,Moffitt, R.A.,Miech, R., & Silva,P. (2001). Reconsidering the relationship between SES and delinquency: Causation but not correlation. In: J.G. Weis, R. D. Crutchfield & G.S. Bridges (Eds.), *Juvenile Delinquency Readings* (2nded., 115-123). Thousand Oaks: Pine Forge Press. (Eerste publicatie 1999).

Bijlage I Procesmodel



Bijlage II Tabel Zoektermen

Tabel 2.Zoektermen

Art. 138ab, minderjarige verdachte	Cyberpesten	Hacken, minderjarige verdachte
Art. 138b, minderjarige verdachte	Cyberpesten, minderjarige verdachte	Hacken, jeugd
Art. 138c, minderjarige verdachte	Cyberpesten, jeugd	Hacken, jeugdstrafrecht
Art. 139d, minderjarige verdachte	Cyberpesten, jeugdstrafzaken	Internet, minderjarige
Art. 161, minderjarige verdachte	Cyberstalking, minderjarige verdachte	Internet, jeugd
Art. 232, minderjarige verdachte	Cyberstalking, jeugd	Internet, jeugdstrafzaken
Art. 240b, minderjarige verdachte	Cyberstalking, jeugdstrafzaken	Kinderporno, minderjarige
Art. 248 e, minderjarige verdachte	Digitale afpersing, minderjarige verdachte	Kinderporno, jeugd
Art. 273, minderjarige verdachte	Digitale afpersing, jeugd	Phishing, minderjarige
Art. 273d, minderjarige verdachte	Digitale afpersing, jeugdstrafzaken	Phishing, jeugd
Art. 317, minderjarige verdachte	Ddos, minderjarige	Spam, minderjarige verdachte
Art. 350a, minderjarige verdachte	Ddos, jeugd	Spam, jeugd
Art. 350b, minderjarige verdachte	Fraude, minderjarige verdachte	Spam, jeugdstrafrecht
Art. 362, minderjarige verdachte	Fraude, jeugd	Telecommunicatie, minderjarige verdachte
Computer, minderjarige	Fraude, jeugdstrafzaken	Telecommunicatie, jeugd
Computer, jeugd	Geautomatiseerd werk, jeugd	Telecommunicatie, jeugdstrafzaken
Computernetwerk, jeugd	Geautomatiseerd werk, minderjarige	Virtueel amulet, minderjarige
Computernetwerk, jeugdstrafrecht	Grooming, minderjarige	Virtueel amulet, jeugd
Computernetwerk, minderjarige verdachte	Grooming, jeugd	Virtuele diefstal, minderjarige verdachte
Cyber, jeugd	GSM, jeugd	Virtuele diefstal, jeugd
Cyber, minderjarige	GSM, minderjarige verdachte	Virtuele diefstal, jeugdstrafzaken
Cybercrime, minderjarige verdachte		

Bijlage III Uitnodiging

Geachte heer/mevrouw…,

In opdracht van het WODC voert de vakgroep Psychologie van Conflict, Risico, en Veiligheid van de Universiteit Twente een verkennend onderzoek uit naar cybercriminaliteit in Nederland waarbij jongeren tot 18 jaar betrokken zijn als dader. Wij willen met dit onderzoek inzicht verkrijgen in de achtergronden (oorzaken, daderkenmerken, pleegwijzen en situationele invloeden) van cybercriminaliteit.

In het kader van dit onderzoek willen wij graag een aantal personen interviewen die in hun werk te maken hebben met cybercriminaliteit in Nederland. Naar onze indruk voldoet u bij uitstek aan dit profiel, en we zouden het daarom zeer waarderen als u ons in een interview meer zou willen vertellen over uw ervaringen over dit onderwerp.
Dit interview zal ongeveer een uur van uw tijd in beslag nemen. Het is mogelijk om dit interview telefonisch of face-to-face (op een locatie van uw voorkeur) te houden.
We hopen van harte dat u bereid bent om uw medewerking aan dit interview te verlenen. Graag ontvangen wij, via een reply op deze mail of u wilt deelnemen. Hierbij kunt u desgewenst een geschikte datum aangeven voor afname van het interview. Een van ons zal daarna contact met u opnemen voor het maken van een concrete afspraak.

Hopende op een spoedige reactie,
Met vriendelijke groet,
Prof. dr. E. Giebels
Dr. Ir. P.W. De Vries
Dr. S. Zebel
Dr. M. Kuttschreuter
K. Egberink, masterstudent CRV
L. D. Slot, masterstudent CRV

Bijlage IV Informed Consent

Enschede,

Deelnemers aan het onderzoek 'Probleemverkenning Cybercrime en Jeugd',

Dit onderzoek is een verkenning van cybercriminaliteit in Nederland, gepleegd door jongeren tot 18 jaar. Het wordt uitgevoerd door onderzoekers en studenten van de opleiding Psychologie aan de Universiteit Twente, in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).
Het doel van dit onderzoek is om inzicht te krijgen in de achtergronden (oorzaken, daderkenmerken, pleegwijzen en situationele invloeden) van cybercriminaliteit waarbij jongeren betrokken zijn. In het kader van dit onderzoek interviewen wij dan ook sleutelfiguren, die in hun werk, te maken hebben met cybercriminaliteit in Nederland. Tijdens het interview zullen we u vragen naar uw specifieke ervaringen, en kennis over dit onderwerp. Graag willen wij u uw toestemming vragen om dit gesprek te mogen opnemen, zodat wij later de mogelijkheid hebben het interview gedetailleerd uit te werken voor het onderzoek. Deze opnamen zijn alleen bestemd voor het onderzoek en zullen niet beschikbaar zijn aan anderen dan de onderzoekers.
Alle informatie zal strikt vertrouwelijk behandeld worden. De resultaten van het onderzoek zullen gebruikt worden om voor het WODC een rapport uit te brengen over cybercriminaliteit. Hierbij zal er zorg worden gedragen dat dit volledig zonder mogelijke identificatie van de participanten gebeurt. U kunt op ieder moment het onderzoek stop zetten en de toestemming alsnog in te trekken.

Als u na het onderzoek nog vragen heeft kunt u contact opnemen met k.egberink@student.utwente.nl of l.d.slot@student.utwente.nl

.

Ik heb dit formulier gelezen en stem er mee in,

....

Datum Handtekening participant

Bijlage V Interview

Interview Cybercriminaliteit

Introductie

Welkom. Hartelijk dank dat u mee wilt werken aan dit interview. Zoals eerder gezegd wordt er momenteel onderzoek gedaan naar Cybercriminaliteit in Nederland uitgevoerd door onafhankelijke onderzoekers en studenten van de Universiteit Twente. Het doel van dit onderzoek is: het in kaart brengen van de vormen en mate van cybercriminaliteit gepleegd in Nederland waarbij tot 18 jaar betrokken raken als daders. Cybercriminaliteit wordt in de literatuur als volgt gedefinieerd: 'Elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.'

Met dit onderzoek wordt getracht inzicht te bieden in de achtergronden (zoals de oorzaken, daderkenmerken, pleegwijzen en situationele invloeden) van deze criminaliteit. In het kader van dit onderzoek interviewen wij zoveel mogelijk partijen, die in hun werk, te maken hebben met jongeren die criminaliteit plegen, en dan specifiek cybercriminaliteit .

Voor ons is het uitermate belangrijk om uw ervaringen over dit onderwerp te horen. We zijn daarbij met name geïnteresseerd in uw kennis en ervaringen met jongeren waarvan vaststaat dat zij cybercriminaliteit hebben gepleegd. Daarbij willen wij u vragen om zo open mogelijk te zijn en zoveel mogelijk te vertellen over het onderwerp.

De verwachte duur van het interview is ongeveer een uur.

Heeft u nog vragen voor we beginnen?

Ik stel voor ons gesprek in 2 delen te splitsen:
1. U eerst de gelegenheid geven om in uw eigen woorden te vertellen op welke manier u te maken krijgt met cybercrime in Nederland gepleegd door jongeren tot 18 jaar, en wat uw belevingen daarbij zijn.
2. Aan de hand van een aantal thema's verder doorpraten. Daarom heb ik hier een map met een aantal dingen die ik niet wil vergeten te vragen en zal ik af en toe aantekeningen maken.

Gedurende het interview de volgende twee punten ten alle tijden in de gaten houden:

1. *Doelgroep: Jongeren van 12 tot 18 jaar.*
2. *Cybercrime in het onderscheid tussen enge en ruime zin*

Deel 1
Eigen woorden

Parafraseren, samenvatten, gevoelsreflectie: Voor alle onderdelen geldt doorvragen: Waarom denkt u dat? Hoe ging dat dan? Kunt u een voorbeeld geven? Wat gebeurde er daarna?

1. Hoe heeft u in uw werkveld te maken met cybercriminaliteit?
2. Wanneer heeft u te maken met cybercriminaliteit onder jongeren tot 18 jaar?

3. Wat kunt u vertellen over de achtergrondkenmerken van de daders van cybercriminaliteit? (ook motieven, pleegwijze)

Er wordt in de literatuur een onderscheid gemaakt tussen cybercriminaliteit in enge en in ruime zin. Hieronder wordt verstaan:

Cybercriminaliteit in enge zin/ cybercrime:
Strafbare gedragingen die niet zonder tussenkomst van ICT gepleegd kunnen worden. Kenmerkend is dat de ICT structuur zelf (en de daarin of daarmee opgeslagen gegevens) het doel van de actie zijn.

Cybercriminaliteit in ruime zin/ gedigitaliseerde criminaliteit:
Onder cybercrime in ruime zin worden strafbare gedragingen verstaan die met behulp van ICT worden uitgevoerd. ICT wordt dan ter ondersteuning gebruikt bij het plegen van anderszins traditionele criminaliteit.

4. Herkent u deze vormen van cybercriminaliteit?
5. Op welke manier ziet u dit onderscheid terug in uw werk?
6. Is er een onderscheid in daders van cybercriminaliteit in enge zin en in ruime zin? Zo ja, welke?
7. Er is een verschil tussen legaal en illegaal downloaden. Denkt u dat mensen op de hoogte zijn van dit verschil en heeft u veel te maken met deze kloof?

8. Wat is uw ervaring met illegaal downloaden?
9.(Er wordt veel geschreven over zowel dalende als geen dalende trend) Wat is uw mening daarover? Heeft u daar ook een verklaring voor?

Deel 2
Thema's

Voor alle onderdelen geldt doorvragen: Waarom denkt u dat? Hoe ging dat? Kunt u daar een voorbeeld van geven? Wat gebeurde er daarna?

Graag zou ik nu met u verder praten over een aantal thema's die te maken hebben met cybercriminaliteit. Ik zou graag willen beginnen met verschillende vormen van cybercriminaliteit die zich kunnen voordoen.

2.1 Vormen (inzicht in verschillende vormen en combinaties van cybercriminaliteit die zich voordoen)

De focus ligt op de eigen ervaringen van mensen, dus ervaringen in hun eigen werkzaamheden.

Cybercriminaliteit in enge en in ruime zin
1. Welke manier/vorm van cybercriminaliteit in enge zin komt u veel tegen?
2. Welke manier/vorm van cybercriminaliteit in ruime zin komt u veel tegen?
3. Bij welke vormen van cybercriminaliteit zijn jongeren veelal betrokken?
4. Is er een verschil met volwassen daders die cybercriminaliteit plegen? (Wat is het verschil)
5. Is er een verschil met daders die conventionele criminaliteit plegen? (Wat is het verschil)

Combinaties van cybercriminaliteit in enge en ruime zin
6. Heeft u wel eens te maken met combinaties van cybercrime in enge en in ruime zin in uw werkveld?
7. Welke combinaties komen veelal voor?

8. In welke mate zijn jongeren beneden de 18 jaar daarbij betrokken in uw werk?
9. Is er een overlap te ontdekken tussen daders van beide categorieën?

2.2 Achtergrondkenmerken en motieven (Inzicht in achtergrondkenmerken en motieven van daders)

In het begin van het interview hebben we ook al even gesproken over mogelijke achtergrondkenmerken en motieven van daders van cybercriminaliteit. Graag willen wij hier verder op in gaan.

1. Welke achtergrondkenmerken ziet u vaak terug bij jongeren die cybercriminaliteit plegen?
   - In hoeverre speelt persoonlijkheid een rol bij het in aanraking komen met cybercriminaliteit?
   - Zijn deze achtergrondkenmerken een voorspeller voor het eventueel plegen van cybercriminaliteit?
2. In welke mate wijkt dit type jongere af van degenen die offline criminaliteit plegen? (Zijn deze achtergrondkenmerken anders dan bij dader van offline criminaliteit?)
3. Welke achtergrondkenmerken zijn vooral te herkennen in uw werk bij cybercrime in enge zin en welke bij ruime zin?
4. Jongeren hebben verschillende drijfveren om cybercriminaliteit te plegen? Wijken deze af van de offline criminaliteit? Zo ja, in welke mate?
5. Wat is volgens u een van de belangrijkste drijfveren voor jongeren?
6. In hoeverre speelt de omgeving een rol bij het in aanraking komen met cybercriminaliteit?

Mogelijke punten die als achtergrondkenmerken/motieven kunnen gelden

- Persoonlijkheid (high sensation seekers)	
- Opleidingsniveau	
- Hoge mate van computer kennis	
- Thuissituatie	
- Vrienden	
- Sociaal economische status	
- Financiele problemen	
- Cultuur	
- Verveling	
- Drugs- alcoholgebruik	

2.3 Criminele carrières (Inzicht in herhaling van criminele daden en daarmee opzetten van een criminele carrière)

1. In hoeverre plegen jongeren herhaaldelijk cybercriminele misdaden?
2. In hoeverre vervallen jongeren, die in aanraking zijn geweest met politie & justitie voor cybercrime misdaden in herhaling? Hoe is dit bij jongeren die conventionele misdaden plegen?
3. Is er sprake van een toename van jongeren die cybercriminaliteit plegen?
4. Wat is het verschil met jongeren die conventionele criminaliteit plegen?
5. Welke factoren zijn van invloed of een jongere in herhaling valt?

Mogelijke punten die van invloed kunnen zijn op criminele carrières

- Recidive	
- Gevangenisstraf / ernst	
- Pakkans	

2.4 Ontstaanswijze (Inzicht in ontstaan van cybercriminaliteit)

Jongeren komen op veel verschillende manieren in aanraking met cybercriminaliteit. Ik zou het nu graag met u willen hebben over de ontstaanswijze van cybercriminaliteit.

1. Op welke manier raken jongeren betrokken bij cybercriminaliteit?
2. Wat zijn factoren die van invloed kunnen zijn op het ontstaan van cybercrime onder jongeren tot 18 jaar?

Mogelijke punten die van invloed kunnen zijn op ontstaanswijze

- Invloed van vrienden	
- Computer kennis	
- Financiële problemen	
- Computer gebruik/stimulatie	
- Geïntegreerd door de mogelijkheden van computers	

2.5 Werk- en pleegwijze (Inzicht in werk- en pleegwijze)

We hebben het net gehad over de ontstaanswijze van cybercriminaliteit onder jongeren. U heeft daarbij verschillende punten genoemd die hierbij van belang zijn. Dan zou ik nu graag door willen gaan op de werk- en pleegwijzen van daders van cybercriminaliteit.

1. Is er een bepaalde werkwijze die gebruikt wordt door jongeren die cybercriminaliteit plegen? In welke manier verschilt dit met 'offline' criminaliteit?
2. Wat is de werkwijze van jongeren bij cybercrime in enge zin? In welke manier verschilt deze werkwijze van jongeren bij online criminaliteit in ruime zin?
3. Welke kennis is nodig om cybercriminaliteit te plegen?
    - Hoe komen jongeren aan kennis om cybercriminaliteit te plegen?
4. Welke rol speel de beschikbare kennis van computers tegenwoordig in het plegen van cybercriminaliteit?
5. Is er verschil in kennis niveau tussen jongeren die online of offline criminaliteit plegen?

Mogelijke punten die van invloed zijn bij de werk- en pleegwijze

- Benodigde kennis	
- Bezitten van kennis	
- Verkrijgen van kennis	

2.6 Perceptie daders cybercriminaliteit (Inzicht in hoe jonge daders tegen hun criminele daden aankijken)

Graag zouden wij ook nog wat willen weten over de perceptie van daders van cybercriminaliteit, als u daar iets over kunt zeggen. Hoe kijken zij volgens u aan tegen cybercriminaliteit en in hoeverre is dit van invloed op de mate waarin ze cybercriminaliteit plegen?

1. In hoeverre zijn jongeren op de hoogte van het feit dat wat ze doen strafbaar is? Hoe zien ze zichzelf als daders?
2. Verschilt dat tussen cybercriminaliteit in enge en in ruime zin?
3. Hebben deze jongeren een andere perceptie t.a.v. cybercriminaliteit dan t.a.v. conventionele criminaliteit?
4. In hoeverre zijn ze op de hoogte van de pakkans en de strafmaat?
5. In hoeverre spelen de risico's, die het plegen van cybercriminaliteit met zich meebrengt, een rol in de percepties van jonge daders?
6. In hoeverre zijn de straffen bekend bij jongeren?
7. Hoe speelt de persoonlijkheid/omgeving een rol in de manier hoe jongeren aankijken tegen

2.7 Aanpak & consequenties(Inzicht in hoe politie & justitie handelen en de gevolgen van cybercriminaliteit)

Politie en justitie spelen een belangrijke rol binnen dit onderwerp. Ik zou het graag met u willen hebben over de rol van politie en justitie.

1. Hoe pakt justitie en politie cybercriminaliteit aan? Hoe valt cybercriminaliteit te herkennen in de aangifte, opsporing en vervolging door politie en justitie? Heeft politie en justitie volledig zicht op en goede mogelijkheden om cyberdaders op te sporen en te vervolgen? Zou dit anders moeten? Zo ja, hoe?
2. Wat zijn de gevolgen wanneer een jongere gepakt is voor cybercriminaliteit? Hoe verschilt dit met de gevolge voor jongeren die conventionele misdaden plegen?
3. In hoeverre heeft dit gevolg invloed op het feit of ze in herhaling vallen?
4. In hoeverre krijgen jongeren een gevangenisstraf voor cybercriminaliteit?
5. Wat vindt u van de vervolging van cybercriminaliteit?
6. Wat is de rol van de media in de aanpak van cybercriminaliteit?
7. Wat is de impact van cybercriminaliteit? Wat voor type gevolgen zijn er bij cybercriminaliteit in enge zin en in ruime zin?

Zijn er nog zaken die niet aan bod zijn gekomen?

Als laatste willen wij u vragen of u na dit interview nog beschikbaar bent voor eventuele vragen en/of kritische opmerkingen?

Hartelijk dank voor uw medewerking!

Begrippenlijst

Cybercriminaliteit:
Elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.'

Cybercriminaliteit in enge zin:
Strafbare gedragingen die niet zonder tussenkomst van ICT gepleegd kunnen worden. Kenmerkend is dat de ICT structuur zelf (en de daarin of daarmee opgeslagen gegevens) het doel van de actie zijn.

Cybercriminaliteit in ruime zin:
Onder cybercrime in ruime zin worden strafbare gedragingen verstaan die met behulp van ICT worden uitgevoerd. ICT wordt dan ter ondersteuning gebruikt bij het plegen van anderszins traditionele criminaliteit.

Bijlage VI Zoekopdrachten

In tabel 4 staan de zoekopdrachten en de daarmee opgeleverde hits en ook de bruikbare hits. Hierbij zijn alle dubbele zaken bij de verscheidene zoekopdrachten buiten beschouwing gelaten.

Tabel 4. Zoekopdrachten en opgeleverde hits

Zoekopdracht	**Aantal hits**	**Bruikbare hits**
Computer, minderjarige	492	
Internet, minderjarige	477	10
Kinderporno, minderjarige	323	
Computer, jeugd	298	3
Internet, jeugd	258	19
GSM, jeugd	99	1
GSM, minderjarige verdachte	98	
Kinderporno, jeugd	67	
Geautomatiseerd werk, minderjarige	52	
Telecommunicatie, jeugd	52	1
Fraude, jeugd	51	
Fraude, minderjarige verdachte	37	
Grooming, minderjarige	31	
Telecommunicatie, minderjarige verdachte	27	
Geautomatiseerd werk, jeugd	22	3
Digitale afpersing, jeugd	15	
Digitale afpersing, minderjarige verdachte	10	1
Internet, jeugdstrafzaken	10	
Telecommunicatie, jeugdstrafzaken	6	

Hacken, minderjarige verdachte	4	1
Hacken, jeugd	4	1
Grooming, jeugd	4	
Phishing, minderjarige	4	1
Cyberstalking	3	
Virtuele diefstal, minderjarige verdachte	3	
Virtuele diefstal, jeugd	3	
Virtueel amulet, minderjarige	3	1
Virtueel amulet, jeugd	3	1
Cybercrime, minderjarige verdachte	2	
Digitale afpersing, jeugdstrafzaken	2	
GSM, jeugdstrafzaken	1	
Spam, minderjarige verdachte	1	1
Spam, jeugd	1	