DE LOKALITEIT VAN CYBERCRIMINALITEIT

EEN VERKENNEND ONDERZOEK NAAR DE LOKALE DIMENSIE VAN CYBERCRIMINALITEIT ONDER JONGEREN IN ROTTERDAM-ZUID

Universiteit Utrecht

Lisanne Tuk

6453910

M Sociology: Contemporary Social Problems

Nationaal Programma ROTTERDAM ZUID

De lokaliteit van cybercriminaliteit

Een verkennend onderzoek naar de lokale dimensie van cybercriminaliteit onder jongeren in Rotterdam-Zuid

Masterscriptie
Universiteit Utrecht
M Sociology: Contemporary Social Problems
Lisanne Tuk
6453910
Datum: 24 juni 2019
Woordenaantal: 21.682

Universiteit Utrecht

Nationaal Programma ROTTERDAM ZUID

Scriptiebegeleider: W.L. van ‘t Hul (MA)
Mastercoördinator: drs. S.B. Soeparman

Stagebegeleider: mr. L. van der Wees
Tweede lezer: Dr. Joyce Delnoij

Voorwoord

Voor u ligt mijn masterscriptie waarmee ik de Master Sociology: Contemporary Social Problems aan de Universiteit Utrecht afrond. In dit afstudeeronderzoek bestudeer ik cybercriminaliteit onder jongeren in Rotterdam-Zuid in opdracht van het Openbaar Ministerie Rotterdam (OM) en het Nationaal Programma Rotterdam Zuid (NPRZ). Het doel van het onderzoek is om een beeld te krijgen van cybercriminaliteit onder jongeren in Rotterdam-Zuid en te ondervinden welke partijen betrokken zijn bij beleid rondom cybercriminaliteit en op welke manieren zij een meer integrale aanpak kunnen ontwikkelen. Hoewel cybercriminaliteit op het eerste gezicht een globaal fenomeen lijkt en het onlogisch lijkt om dit fenomeen in een lokale context te bestuderen, verkent dit onderzoek de lokaliteit van cybercriminaliteit, omdat er een piek zichtbaar is in Rotterdam-Zuid met betrekking tot cybercriminaliteit.

Na de afronding van de vakken Criminology and Safety en Internet, Social Media and Networks heb ik tot mijn grote vreugde de kans gekregen om onderzoek te doen naar cybercriminaliteit. Hoewel ik voorheen geen expert was op dit gebied, heeft het onderwerp mij altijd aangesproken omdat het een nieuw en onbekend fenomeen is wat zelfs een ondermijnende invloed kan hebben op de maatschappij. Onderzoek naar dit onderwerp is nodig omdat de kennis die mede hieruit voortvloeit de basis is voor effectief beleid. Op deze manier grijp ik ook terug naar de vakken Policy, Research and Advice en Organisations, Theory and Research.

Voordat u deze scriptie verder tot zich neemt, wil ik graag een dankwoord richten aan allen die hebben bijgedragen aan de totstandkoming van deze scriptie. Allereerst wil ik mijn stagebegeleidster Loes van der Wees van het NPRZ bedanken voor het bieden van een toffe stageplek en de boeiende overleggen die ik mocht bijwonen. Daarnaast bedank ik Jacqueline Bonnes en Malika Chtatou van het OM voor de interessante opdracht en de verdere begeleiding binnen het OM. Ook wil ik mijn scriptiebegeleider Leonard van ’t Hul bedanken voor de fijne begeleiding tijdens het schrijven van mijn onderzoek. Tenslotte wil ik mijn dank uitspreken naar de scholen die hebben mee willen werken aan dit onderzoek, alle respondenten die de enquête hebben ingevuld en de respondenten die hebben meegewerkt aan een interview. Zonder hen was het niet mogelijk geweest om dit onderzoek tot een succesvol einde te brengen.

Veel leesplezier!

Lisanne Tuk

Inhoudsopgave

Lijst van tabellen en figuren

Tabellen

Figuren

Samenvatting

Cybercriminaliteit komt steeds vaker voor, ook onder jongeren. Het probleem van cybercriminaliteit is dat er geen temporale of ruimtelijke grenzen bestaan aan het internet, wat een integraal deel uitmaakt van cybercriminaliteit. Kwaadwillenden kunnen slachtoffers maken aan de andere kant van de wereld met slechts een muisklik. Dat heeft tot gevolg dat cybercriminaliteit een relatief nieuwe dreiging vormt en beleid ontwikkeld moet worden voor de bestrijding van cybercriminaliteit op basis van deze kenmerken (Lusthaus & Varese, 2017). Toch is cybercriminaliteit niet helemaal zonder ruimtelijke grenzen. Internettoegang is ongelijk verdeeld, waardoor de dichtheid van daders en potentiële slachtoffers geclusterd is (Yar, 2016). Volgens Näsi et al. (2015) verhoogt werkloosheid ook het risico op slachtofferschap van cybercriminaliteit, wat erop zou kunnen wijzen dat wijken met sociaaleconomische problemen een risicogebied zijn als het gaat om cybercriminaliteit. Een voorbeeld van zo'n risicogebied is Rotterdam-Zuid. De werkloosheid is daar namelijk relatief hoog, zeker onder jongeren, en veel criminaliteit vindt plaats in Rotterdam-Zuid (CBS, 2019b; Gemeente Rotterdam, 2019; NPRZ, 2019). Onder andere de General Theory of Crime, de Social Learning Theory, Routine Activity Theory en de General Strain Theory worden gebruikt om cybercriminaliteit te verklaren.

Het doel van deze scriptie is om te onderzoeken welke vormen van cybercriminaliteit in Rotterdam-Zuid voorkomen, hoe sociaaleconomische achterstanden deze kunnen verklaren en op welke manieren betrokken partijen een meer integrale aanpak kunnen ontwikkelen om cybercriminaliteit te verminderen. Dat gebeurt aan de hand van een beleidssegment en een wetenschappelijk segment. Het beleidssegment heeft betrekking op betrokken partijen die te maken hebben met cybercriminaliteit en zullen worden bestudeerd door middel van open interviews. Het wetenschappelijk segment van dit onderzoek zal aantonen dat lokaliteit een rol speelt bij cybercriminaliteit door middel van een enquête onder jongeren in Rotterdam-Zuid.

De resultaten tonen aan dat inwoners van Rotterdam-Zuid vooral slachtoffer zijn van virussen, phishing, internetoplichting en hacking. Dat verschilt niet van de inwoners van regio Rotterdam. Inwoners van Rotterdam-Zuid zijn wél vaker dader van cybercriminaliteit, en dan vooral van virussen, cyberpesten, password cracking, internetoplichting en hacking. Deze mate van slachtoffer- en daderschap worden beïnvloed door differentiële associatie, migratieachtergrond, tijdsbesteding, sociale kwetsbaarheid, opleidingsniveau en strain. Tenslotte is de factor 'Woonachtig in Rotterdam-Zuid' van significante invloed, maar is het nog onduidelijk welk mechanisme hier precies een rol bij speelt.

Het beleid dat betrokken partijen hanteren is vooral gericht op preventie en bestaat uit voorlichting en maatwerkoplossingen om de recidive van first offenders te voorkomen. De partijen lopen tegen de knelpunten aan dat er een tekort aan kennis en bewustzijn is bij veel organisaties in dit beleidsveld. Daarnaast is de denk- en werkwijze van organisaties nog niet ingericht op het fenomeen cybercriminaliteit. Om een integrale aanpak te ontwikkelen wordt kennisdeling en een samenwerkingsverband in de vorm van een Cyber Cirkel Coalitie geadviseerd.

1. Introductie

Op 22 januari 2019 arresteerde Politie Rotterdam zes personen wegens Marktplaatsfraude en phishing. De verdachten boden concerttickets aan via Marktplaats, maar leverden die vervolgens niet. Ze vroegen slachtoffers hun identiteit te verifiëren door een betaalverzoek, waarna slachtoffers op een phishingsite terecht kwamen en de verdachten vervolgens hun bankinformatie stalen en hun rekeningen plunderden (nu.nl, 2019). In het weekend van 18 en 19 mei 2019 werden 23 jongeren van 15 tot 23 jaar opgepakt vanwege het vermoeden dat zij geldezels zijn geweest; mensen die op verzoek van criminelen hun pinpas en pincode uitlenen. Ook in dit geval worden de slachtoffers goederen beloofd en niet geleverd en maken ze het geld over naar een van de bankrekeningen van de geldezels. Een aantal Officieren van Justitie, politieagenten, reclasseringsmedewerkers en advocaten zorgden tijdens dit actieweekend voor een straf op maat. Tijdens deze dagen werd een gesprek aangegaan met de jongeren waarin handvatten werden aangeboden om de volgende keer dat hen werd gevraagd om mee te doen aan criminele activiteiten 'nee' te zeggen.

De hierboven beschreven activiteiten zijn strafbare feiten. In het eerste geval is sprake van cyberfraude, in het tweede geval van witwassen en internetoplichting. In beide gevallen gaat het om cybercriminaliteit; een criminele activiteit waarbij wetten of regels worden geschonden en waarbij computers en computernetwerken een essentiële rol spelen (Kshetri, 2010). Een groot voordeel van dit type criminaliteit is dat het makkelijk, winstgevend en minder risicovol is dan misdaden die niet worden uitgevoerd met behulp van computers (Cárdenas et al., 2009). Cybercriminaliteit kan variëren van marktplaatsfraude en witwassen, zoals hierboven beschreven, tot high-tech crimes zoals DdoS-aanvallen.

Het probleem van cybercriminaliteit is dat er geen temporale of ruimtelijke grenzen bestaan aan de mogelijkheden om een vorm van cybercriminaliteit te plegen. Het internet is wereldwijd en kan daarom vierentwintig uur per dag worden gebruikt. Bovendien is er geen werkelijke afstand tussen twee punten in cyberspace, ofwel computers, waardoor kwaadwillenden toegang tot een doel kunnen krijgen met slechts een muisklik. Daders kunnen daardoor zomaar slachtoffers aan de andere kant van de wereld maken (Yar, 2016; Lusthaus & Varese, 2017). Dat heeft tot gevolg dat cybercriminaliteit een relatief nieuwe dreiging vormt en beleid ontwikkeld moet worden voor de bestrijding van cybercriminaliteit op basis van deze kenmerken (Lusthaus & Varese, 2017).

Toch is cybercriminaliteit niet helemaal zonder ruimtelijke grenzen. Internettoegang is ongelijk verdeeld, waardoor de dichtheid van daders en potentiële slachtoffers geclusterd is (Yar, 2016). Zo hebben inwoners van grote steden een grotere kans om slachtoffer te worden van cybercriminaliteit dan mensen die op het platteland wonen (Näsi et al., 2015; CBS, 2019a). Volgens Näsi et al. (2015) verhoogt werkloosheid ook het risico op slachtofferschap van cybercriminaliteit, wat erop zou kunnen wijzen dat wijken met sociaaleconomische problemen een risicogebied zijn als het gaat om cybercriminaliteit. Een

voorbeeld van zo'n risicogebied is Rotterdam-Zuid. De werkloosheid is daar namelijk relatief hoog, zeker onder jongeren (CBS, 2019b; Gemeente Rotterdam, 2019). Hoewel de criminaliteitscijfers afnemen, vond nog steeds 6,3% van de geregistreerde misdaden plaats in Rotterdam in 2018 en een derde van de verdachte transacties in regio Rotterdam vond plaats in Rotterdam-Zuid in 2016 (NPRZ, 2019). Dat suggereert dat ondermijnende criminaliteit relatief veel voorkomt in Rotterdam-Zuid en cybercriminaliteit mogelijk ook. Bovendien neemt cybercriminaliteit er toe; zo'n 6,2% van de computervredebreuken vindt hier plaats, een stijging is van honderd procent ten opzichte van 2017 (CBS, 2019c). Het Openbaar Ministerie (OM) ziet ook steeds meer zaken die betrekking hebben op internetoplichting door jongeren en zich afspelen in Rotterdam-Zuid. Naar aanleiding van deze waarnemingen zijn het Nationaal Programma Rotterdam Zuid (NPRZ) en het OM nieuwsgierig geworden naar de aard en omvang van cybercriminaliteit onder jongeren in Rotterdam-Zuid. Tot nu toe is het vrijwel onbekend in welke mate en vormen cybercriminaliteit voorkomt in Rotterdam-Zuid en of het dan vooral gaat om dader- of slachtofferschap. Op dit moment is het onduidelijk wie er over enige mate van kennis over cybercriminaliteit in dit gebied beschikt en als deze kennis er al is, is deze naar verwachting erg gefragmenteerd.

Het doel van deze scriptie is om te onderzoeken welke vormen van cybercriminaliteit in Rotterdam-Zuid voorkomen, hoe sociaaleconomische achterstanden deze kunnen verklaren en op welke manieren betrokken partijen een meer integrale aanpak kunnen ontwikkelen om cybercriminaliteit te verminderen. Dat gebeurt aan de hand van twee segmenten: een beleidssegment en een wetenschappelijk segment. Het beleidssegment heeft betrekking op betrokken partijen die te maken hebben met cybercriminaliteit en zullen worden bestudeerd door middel van open interviews. Het is nog onduidelijk wie de betrokken partijen precies zijn en daarom zal er een overzicht worden gemaakt van de betrokken partijen tijdens het onderzoek.

Het ontwikkelen van een effectieve aanpak is een pittige opgave vanwege de complexiteit van cybercriminaliteit. Om cybercriminaliteit aan te pakken of te voorkomen is strategische intelligentie nodig, wat bestaat uit het verzamelen van data, interpreteren en speculeren over ontwikkelingen, patronen, bedreigingen en kansen (Buono, 2014). De kennis die resulteert uit de interviews zal dus een bijdrage kunnen leveren aan de benodigde strategische intelligentie, wat de politie, het OM en Gemeente Rotterdam kunnen gebruiken bij het ontwikkelen van een effectieve aanpak van cybercriminaliteit. Ook zullen veel organisaties internationaal moeten samenwerken om cybercriminaliteit enige weerstand te kunnen bieden. Betrokken partijen maken zich erg zorgen over cybercriminaliteit en uit die angst werken ze samen met de overheid aan cybercriminaliteitsbestrijding. Er zullen echter nieuwe technologische ontwikkelingen blijven komen waardoor cybercriminelen de genomen maatregelen kunnen omzeilen (Martin & Rice, 2011).

Daarnaast is bewustzijn van de risico's van internetgebruik erg belangrijk en het is noodzakelijk om dit bewustzijn nu te verhogen, vooral bij reguliere medewerkers die dagelijks gebruik maken van het internet. Overheidscampagnes en simpele beveiligingsmaatregelen kunnen al zorgen voor een flinke

daling in cybercriminaliteit (Martin & Rice, 2011). Een goede maatregel is meer beveiliging dan alleen een wachtwoord, bijvoorbeeld met een token of vingerafdruk (Epps, 2017). Ook bij daders is bewustwording van belang, maar in dit geval ligt er meer nadruk op het herkennen van de schade die een cybercrimineel zou kunnen aanrichten en hoe dit gedrag gevolgen kan hebben voor de toekomst van de dader (Oosterwijk & Fischer, 2017).

Het wetenschappelijk segment van dit onderzoek zal een bijdrage leveren aan de bestaande literatuur, namelijk door inzicht te bieden in de invloed van een sociaaleconomische wijkproblemen op cybercriminaliteit. Hoewel de wetenschappelijke literatuur voldoende handvatten biedt om cybercriminaliteit an sich te onderzoeken, is er weinig aandacht voor dit onderwerp met betrekking tot lokale gebieden (Maimon et al., 2013; Leukfeldt, 2015; Yar, 2016; Lusthaus & Varese, 2017). In 2018 is er ook onderzoek gedaan naar cybercriminaliteit in Rotterdam waarin het lokale component geen rol lijkt te spelen bij cybercriminaliteit vanwege het gebruik van digitale middelen (Van de Pavert, 2018). Het lokale is echter van belang bij een grensoverstijgend fenomeen als cybercriminaliteit, omdat een fysieke computer en de mens zelf een integraal deel blijven van cybercriminaliteit (Lusthaus & Varese, 2017). Deze computer bevindt zich op een bepaalde locatie en wordt bediend door een natuurlijk persoon die zich ook altijd op een geografische plaats zal bevinden.

Deze lokaliteit manifesteert zich in Rotterdam-Zuid, wat kampt met sociaaleconomische problemen als werkloosheid en een laag opleidingsniveau. Volgens Leukfeldt en Yar (2016) hebben werklozen en laagopgeleiden een grotere kans om slachtoffer te worden van gedigitaliseerde criminaliteit, waarbij het internet alleen een middel is. Bovendien zijn de internetvaardigheden van laagopgeleiden relatief beperkt, waardoor zij zich minder bewust zijn van risico's van internetgebruik en zich minder goed beveiligen, waardoor ze een grotere kans hebben om slachtoffer te worden (Van Deursen & Van Dijk, 2010). Vooral jongeren zijn vatbaar voor cybercriminaliteit omdat zij meer gebruik maken van het internet en daardoor een risicogroep vormen (Näsi et al., 2015). Op basis van de deze gegevens en de sociaaleconomische achterstanden in Rotterdam-Zuid kan Rotterdam-Zuid bestempeld worden als sociaal kwetsbaar. Van Damme en Pauwels (2010) omschrijven sociale kwetsbaarheid als bestaande uit armoede, een lage scholingsgraad, een onstabiele gezinsstructuur en een andere etnische afkomst. Aangezien al deze factoren sterk aanwezig zijn in Rotterdam-Zuid, zal het concept sociale kwetsbaarheid centraal staan in dit onderzoek.

Het wetenschappelijk segment bestaat uit een enquête die wordt afgenomen bij jonge bewoners van Rotterdam-Zuid tussen de veertien en drieëntwintig jaar. Er is gekozen voor een enquête omdat de betrokken partijen naar verwachting weinig kennis hebben over wat zich werkelijk afspeelt op Rotterdam-Zuid wat betreft cybercriminaliteit en handelen op basis van statistieken die vaak tekortschieten. De betrokken partijen die worden geïnterviewd hebben waarschijnlijk een bepaald beeld van cybercriminaliteit in Rotterdam-Zuid. Dit beeld zal naar voren komen tijdens de interviews. Daarnaast zullen de resultaten van de enquête een indicatie geven van de mate waarin cybercriminaliteit

voorkomt in Rotterdam-Zuid. De eerste vraag die centraal staat luidt als volgt: *Welke vormen van cybercriminaliteit komen vooral voor in Rotterdam-Zuid?*

Naast het feit dat het onduidelijk is in welke vormen cybercriminaliteit voorkomt en welke partijen hier kennis van hebben, is het onbekend deze voorkomende vormen van cybercriminaliteit verklaard kunnen worden. Daarom wordt er een tweede, verklarende onderzoeksvraag gesteld. De resultaten van het wetenschappelijk segment zullen hier leidend in zijn. De tweede onderzoeksvraag luidt: *Hoe kan cybercriminaliteit in Rotterdam-Zuid verklaard worden?*

Ten derde is het belangrijk te weten te komen in hoeverre de partijen al inspelen op de kennis waar zij over beschikken. Daarom is het van belang om te achterhalen welke maatregelen zij al hebben genomen om cybercriminaliteit zo veel mogelijk in te perken. De derde onderzoeksvraag luidt: *Welke maatregelen zijn er tot nu genomen om cybercriminaliteit te verminderen in Rotterdam-Zuid?*

Tenslotte zullen de eerste twee onderzoeksvragen informatie verschaffen over de situatie in Rotterdam-Zuid rond cybercriminaliteit, op basis waarvan maatregelen getroffen kunnen worden. Een deel van die maatregelen zal al terugkomen in het antwoord op de derde onderzoeksvraag, maar er wordt op basis van de nieuw verkregen gegevens en het huidige beleid advies gegeven voor toekomstig beleid. De resultaten van de twee segmenten van het onderzoek zullen samengevoegd leiden tot een antwoord op de volgende vraag: *Op welke manier(en) kunnen betrokken partijen cybercriminaliteit in Rotterdam-Zuid verminderen?*

Tot nu toe is bekend dat cybercriminaliteit naar verwachting wel aanwezig is in Rotterdam-Zuid, maar het is onduidelijk welke partijen hier zicht op hebben en in hoeverre dat een juiste representatie is van de werkelijkheid. Om helder te krijgen welke trends met betrekking tot cybercriminaliteit zich voordoen in Rotterdam-Zuid en welke betrokken partijen over relevante informatie beschikken, is het eerst noodzakelijk om een duidelijk beeld te schetsen van wat cybercriminaliteit nu precies is en hoe daders komen tot het plegen ervan. Daarnaast wordt ook toegelicht welke factoren bijdragen aan slachtofferschap. Na de theoretische achtergrond volgt de methodologie, waarin de twee segmenten worden toegelicht. In de resultatensectie worden de analyses van het wetenschappelijk segment en het beleidssegment beschreven en aan elkaar gekoppeld. Tenslotte zal de theorie weer aan de resultaten worden gekoppeld in de discussie en zal dit onderzoek besluiten met beleidsaanbevelingen die uit de discussie voortvloeien.

2. Theoretische achtergrond

De theoretische achtergrond zal eerst beschrijven wat er onder cybercriminaliteit wordt verstaan, welke onderverdelingen er zijn en wat de voor- en nadelen en de knelpunten bij het maken van beleid zijn. Daarna volgen verklaringen voor het daderschap en slachtofferschap van cybercriminaliteit, elk opgesplitst in sociaal-psychologische verklaringen en sociale verklaringen. De sociaal-psychologische verklaringen gaan meer in op de individuele kenmerken van een dader dan wel slachtoffer. De sociale kenmerken hebben betrekking op de omgeving waar een dader of slachtoffer zich in bevindt die er aan kunnen bijdragen dat een individu dader of slachtoffer wordt. Er is een onderscheid gemaakt tussen daderschap en slachtofferschap omdat er verschillende mechanismen en factoren van invloed zijn op de twee verschillende kanten van cybercrime. Daarnaast zullen ook wat factoren overlappen, omdat deze zowel daderschap als slachtofferschap beïnvloeden. Tenslotte is er een paragraaf gewijd aan de sociaaleconomische omstandigheden in Rotterdam-Zuid die de kansen op zowel dader- als slachtofferschap kunnen vergroten.

2.1 Cybercriminaliteit

Cybercriminaliteit is onder te verdelen in gedigitaliseerde criminaliteit en *high-tech cybercrimes.* Gedigitaliseerde cybercriminaliteit verwijst naar misdaden die ook al werden gepleegd zonder het internet, maar nu ook op een digitale manier kunnen worden uitgevoerd, bijvoorbeeld fraude (Choi, 2008). High-tech cybercrimes zijn misdaden die volledig afhankelijk zijn van het internet en zich pas ontwikkelden met de komst van het internet, zoals hacking en het installeren van malafide software (Furnell, 2002, zoals beschreven in Maimon et al., 2013). Hieronder volgt een classificatie van de typen cybercriminaliteit waar dit onderzoek zich vooral op zal richten. Wanneer er wordt gesproken over cybercriminaliteit wordt dus zowel gedigitaliseerde criminaliteit als high-tech cybercrimes bedoeld.

Tabel 1. Classificatie gedigitaliseerde criminaliteit en high-tech cybercrime.

Gedigitaliseerde criminaliteit	**High-tech cybercrime**
Pinpasfraude	Virus
Helpdeskfraude	Malware
Identiteitsfraude	Phishing
Terrorisme	Ransomware
Internetoplichting	Botnet
Cyberafpersing	Cryptojacking
Cyberstalking	DdoS-aanval
Cyberpesten	Hacking
Kinderporno	Defacing
	Password cracking

Cybercriminelen opereren vanuit het dark web. Dit is een onderdeel van het *deep web*, wat bestaat uit niet-zoekbare websites zoals medische databases en intranets. De meeste slachtoffers bevinden zich echter op het *surface web*, met alleen zoekbare websites die voor iedereen toegankelijk zijn (Maimon & Louderback, 2019). Cybercriminelen maken geen selectie van internetgebruikers om zo hun slachtoffers te vinden. In plaats daarvan zoeken ze naar ingangen bij browsers waardoor ze toegang kunnen krijgen tot gebruikers, waardoor veel potentiële slachtoffers kunnen worden bereikt (Leukfeldt, 2015).

Individuen zijn sneller geneigd om misdaden te plegen in de online dan in de offline wereld (Buono, 2014). Een voordelige bijkomstigheid voor cybercriminelen is dat het internet veel mogelijkheden biedt, en de winsten relatief groot en de kosten vrij laag zijn. De beloning die een cybermisdaad oplevert is relatief hoog in vergelijking met de lage inspanning en de pakkans. Daarbij hebben veel cybermisdaden een groot bereik, bijvoorbeeld met een advertentie op Marktplaats die veel potentiële slachtoffers kunnen zien. Als gevolg hiervan neemt het aantal cybercrimes toe (Cárdenas et al., 2009). Daarbij maken en handhaven staten erg divers beleid tegen cybercriminaliteit, wat de toename van cybercriminaliteit alleen maar versterkt omdat cybercriminelen weten dat de pakkans erg laag is (Cárdenas et al., 2009; Buono, 2014). Een probleem bij het maken van passend en effectief beleid is dat veel cyberaanvallen niet worden achterhaald, laat staan dat er aangifte van wordt gedaan. Daarom is er een groot *dark number*, i.e. het aantal cybercrimes dat wel plaatsvindt, maar niet bekend is bij politie en justitie.

Bovendien is het lastig om uitspraken te doen over welke mensen cybercriminaliteit plegen, omdat iedereen die in het bezit van een computer is de mogelijkheid heeft om misbruik te maken van het internet en schade toe te brengen op een andere plaats. Jongeren vormen een risicogroep, vooral als ze een cybersecurity-opleiding volgen waarin ze leren hoe een hack tot stand komt. Daarnaast zijn jongeren gevoelig voor ronseling door cybercriminelen. In Amsterdam zijn veel schoolverlaters van het mbo betrokken bij cybercriminaliteit en wellicht is dat in Rotterdam ook het geval ([#Online daders], z.d.).

2.2 Daderschap

2.2.1 Sociaal-psychologische verklaringen

Niet alleen de mogelijkheden en het gebrek aan risico's spelen een rol in het verklaren van cybercriminaliteit. De General Theory of Crime stelt dat individuen met weinig zelfcontrole vatbaarder zijn voor criminele kansen (Gottfredson & Hirshi, 1990, zoals beschreven in Maimon & Louderback, 2019). Mensen met weinig zelfcontrole zijn impulsiever, avontuurlijker, gericht op zichzelf en kunnen moeilijk de beloning uitstellen. De verantwoordelijkheid voor het aanleren van zelfcontrole ligt bij de opvoeding door de ouders, die goed toezicht moeten houden op hun kinderen en sancties moeten opleggen waar nodig. Dit proces duurt voort tot de adolescentie, waarna het niveau van zelfcontrole

stabiliseert (Jahankhani, 2018). Dit betekent dat jongeren hun zelfcontrole nog aan het ontwikkelen zijn en dus vatbaarder zullen zijn voor deelname aan cybercriminele activiteiten (Donner et al., 2014, zoals beschreven in Jahankhani, 2018; Marcum et al., 2014; Holt & Kilger, 2008; Bossler & Burruss, 2011). Op basis van deze theorie is de hypothese dat individuen met weinig zelfcontrole sneller geneigd zijn om zich schuldig te maken aan cybercriminaliteit.

Een andere verklaring voor het plegen van cybercriminaliteit kan worden afgeleid van Agnews (2001) General Strain Theory. Volgens Agnew is strain een gevolg van relaties waarin een individu niet wordt behandeld door anderen op de manier waarop hij behandeld wilt worden (Agnew, 1992, zoals beschreven in Agnew, 2001). Er zijn twee soorten strain: objectieve strain en subjectieve strain. Objectieve strain kan worden ervaren als gevolg van bepaalde gebeurtenissen of omstandigheden die de meeste mensen niet fijn vinden, bijvoorbeeld het verliezen van een dierbare. Subjectieve strain omvat gebeurtenissen of omstandigheden die mensen die deze gebeurtenissen hebben ervaren niet fijn vinden, bijvoorbeeld een scheiding als gevolg van een slecht huwelijk. Mensen die een goed huwelijk hadden zullen de scheiding anders beoordelen dan mensen die een slecht huwelijk hadden. Het ervaren van deze strains kan leiden tot het blokkeren van doelen, het verlies van positieve stimulansen en de opkomst van negatieve stimulansen. Strains leiden tot crimineel gedrag wanneer de strains worden gezien als onjuist, onproportioneel, worden geassocieerd met weinig sociale controle en druk creëren om daar op een criminele manier mee om te gaan (Agnew, 2001). Individuen kunnen bijvoorbeeld strain ervaren als gevolg van sociale kwetsbaarheid (i.e. niet in staat zijn om met gebeurtenissen om te gaan die het emotionele, fysieke of financiële welzijn negatief kunnen beïnvloeden als gevolg van armoede, een laag opleidingsniveau, een slechte gezinsstructuur en een etnische achtergrond) (Fisher et al., 2016; Van Damme & Pauwels, 2010). Bovendien missen sommige individuen de directe controle en conventionele middelen om op een legale manier met hun strain om te gaan (Baron, 2004). Daarnaast kunnen eerdere gebeurtenissen die individuen ervaren als negatief zorgen voor de ontwikkeling van strain, waardoor ‘coping skills’ afnemen en individuen sneller vervallen in (cyber)criminaliteit. De hypothese is daarom dat individuen die meer strain ervaren vaker dader zijn van cybercriminaliteit dan individuen die minder strain ervaren.

2.2.2 Sociale verklaringen

Naast de sociaal-psychologische verklaringen komen andere verklaringen vooral voort uit sociale kwetsbaarheid. De sociaaleconomische omstandigheden die soms reden geven om daar op een onconventionele manier mee om te gaan kunnen versterkt worden door andere sociale factoren die samen leiden tot crimineel gedrag.

De Social Learning Theory beweert dat imitatie en deviante associatie ervoor zorgen dat crimineel gedrag wordt aangeleerd (Maimon & Louderback, 2019). Deze theorie stelt dat individuen gedrag aanleren door te testen op welke gedragingen grotere beloningen volgen dan kosten. Ook als individuen criminele activiteiten in de fysieke wereld uitvoeren, kan dat leiden tot online crimineel

gedrag, omdat zij ontdekken dat cybercrime hogere beloningen en lagere risico's heeft (Jahankhani, 2018). Bossler en Burruss (2011) en Hutchings en Clayton (2016, zoals beschreven in Maimon & Louderback, 2019) rapporteren dat de kans dat individuen betrokken raken bij respectievelijk hacking en DdoS-aanvallen groter is wanneer zij kennissen hebben die zich hiermee bezig houden dan wanneer zij deze niet hebben. Omdat er relatief veel criminaliteit plaatsvindt in Rotterdam-Zuid, is de kans dat een individu iemand kent die betrokken is bij criminaliteit groter. Als individuen ontdekken dat het internet veel winstgevender is dan criminaliteit in de fysieke wereld, kunnen zij verwikkeld raken in de wereld van cybercriminaliteit. De hypothese is dus dat individuen die meer kennissen hebben die met cybercriminaliteit te maken hebben zelf ook vaker betrokken raken bij cybercriminaliteit.

Hirschi's (1969) Social Bond Theory, die stelt dat individuen worden weerhouden van crimineel gedrag door verbondenheid, geloof, betrokkenheid en toewijding aan een gemeenschap of organisatie, lijkt te verklaren waarom individuen zich aan regels binnen een gemeenschap houden (Cheng et al., 2013, zoals beschreven in Maimon & Louderback, 2019). Als individuen genoeg verbonden zijn aan, geloven in, betrokken zijn bij en toegewijd zijn aan een gemeenschap, zullen ze zich houden aan de regels die gelden binnen die gemeenschap. In een gemeenschap zoals Rotterdam-Zuid worden de centrale mechanismen van de Social Bond Theory beïnvloed door kenmerken van het stadsdeel. Etnische heterogeniteit zorgt voor minder vertrouwen, waardoor er minder contact en dus minder sociale cohesie is tussen bewoners (Putnam, 2007). Daarnaast speelt het inkomen een rol: in buurten met een lager gemiddeld inkomen is er minder contact tussen buren dan in buurten met een hoger gemiddeld inkomen (Tolsma et al., 2009). Bovendien is de buurtstabiliteit belangrijk voor de sociale cohesie in een buurt, welke verslechtert wanneer er veel mensen komen en gaan, wat vaak het geval is in wijken met sociaaleconomische achterstanden (Andersson & Bråmå, 2004; Gijsberts & Dagevos, 2007). De hypothese is dus dat slechtere sociale banden leiden tot meer betrokkenheid bij daderschap van cybercriminaliteit.

Ook sociale status speelt een rol bij daderschap. Sociale status bestaat uit inkomen, arbeidsniveau en opleidingsniveau (Ellis & McDonald, 2001). Volgens Ellis en McDonald (2001) is er een omgekeerde relatie tussen sociale status en crimineel gedrag, wat betekent dat mensen met een lage sociale status meer crimineel gedrag vertonen dan mensen met een hogere sociale status. Daarnaast geeft een lage sociale status redenen om weinig verwachtingen te hebben van een succesvolle toekomst en weinig zelfvertrouwen. Volgens Jennings, Gibson en Lanza-Kaduce (2009) vormen deze factoren een negatief zelfconcept, wat kan leiden tot gedragsproblemen, zoals het vertonen van crimineel gedrag. Omdat Rotterdam-Zuid een lage sociale status heeft, gebaseerd op een gemiddeld laag inkomen, een laag arbeidsniveau en een laag opleidingsniveau, zullen de inwoners sneller een negatief zelfconcept hebben en als gevolg daarvan crimineel gedrag kunnen vertonen. De hypothese is dus dat een lagere sociale status leidt tot meer betrokkenheid bij daderschap van cybercriminaliteit.

Ook opleidingsniveau speelt een rol bij daderschap. Uit het onderzoek van Marcum et al. (2014) is gebleken dat high-tech cybercrimes een hoge mate van intelligentie vereisen, en het dus

onwaarschijnlijk is dat mensen met een laag opleidingsniveau een hack uitvoeren. Aangezien het gemiddelde opleidingsniveau van inwoners van Rotterdam-Zuid relatief laag is, is de verwachting dat weinig high-tech cybercrimes vanuit dit gebied worden uitgevoerd (Gemeente Rotterdam, 2017).

2.3 Slachtoffers

Demografische factoren zijn van belang bij slachtofferschap van high-tech cybercrimes: vrouwen hebben een grotere kans om slachtoffer te worden van hacking en malware dan mannen, terwijl mannen meer kans hebben op slachtofferschap van cybercriminaliteit in het algemeen (Bossler & Holt, 2009; Näsi et al., 2015). Etniciteit en ras lijken geen effect te hebben. Leeftijd speelt wel een rol: hoe jonger, hoe groter de kans op slachtofferschap, maar alleen bij hacking en gedigitaliseerde criminaliteit (Leukfeldt & Yar, 2016). Daarnaast hebben mensen die aangeven dat hun leeftijdsgenoten of dat zij zelf betrokken zijn bij het plegen van cybercriminaliteit meer kans hebben om slachtoffer te worden (Choi, 2008; Wolfe et al., 2008; Bossler & Holt, 2009).

2.3.1 Sociaal-psychologische verklaringen

Ondanks het feit dat de cybercriminaliteitsstatistieken niet extreem hoog zijn, is de angst om slachtoffer te worden van cybercriminaliteit vrij groot (Wall, 2013, zoals beschreven in Maimon & Louderback, 2019). Dit gevoel van angst, of, objectiever, individuele inschatting van het risico van victimisering, komt onder andere tot stand door financiële impulsiviteit (Riesig, Pratt & Holtfreter, 2009). Impulsiviteit is het gebrek aan zorgen om toekomstige omstandigheden (Baumeister, 2002, zoals beschreven in Riesig et al., 2009), gekenmerkt door het niet kunnen weerstaan van verleidingen. Impulsieve mensen geven dan ook meer geld uit dan ze kunnen besteden, wat kan leiden tot schulden (Romal & Kaplan, 1995, zoals beschreven in Riesig et al., 2009). Omdat mensen zichzelf niet kunnen vertrouwen wat betreft hun financiële uitgaven, zijn ze banger om slachtoffer te worden van cybercriminaliteit.

2.3.2 Sociale verklaringen

Slachtofferschap wordt vaak gezien als onterecht en erg ingrijpend. Slachtoffers bevinden zich vaak in omgevingen met weinig sociale controle (Baron, 2004). In de online wereld is die sociale controle lager dan in de fysieke wereld, omdat er in de fysieke wereld mensen toevallig langs een verzamelplek voor jongeren kunnen lopen. In de online wereld is dat echter niet mogelijk. Jongeren kunnen ongemerkt op onveilige websites rondsurfen zonder dat hun voogden daar iets van weten.

Slachtofferschap van cybercriminaliteit kan verklaard worden met behulp van Routine Activity Theory. Volgens deze theorie komt deviant gedrag voort uit kansen, bestaande uit de aanwezigheid van een gemotiveerde dader en een gepast doel en de afwezigheid van een capabele beveiliger (Leukfeldt, 2015). De dader wordt gemotiveerd door vier elementen van het doel, namelijk waarde, inertie,

zichtbaarheid en toegankelijkheid (Leukfeldt & Yar, 2016). Waarde verwijst naar de waarde die daders toekennen aan hetgeen zij in hun bezit willen nemen. Inertie verwijst oorspronkelijk naar de draagbaarheid van het doel, maar bij cybercriminaliteit is er bijna geen sprake is van fysieke doelen. Inertie zou wel geïnterpreteerd kunnen worden als de technologische eigenschappen van een doel, omdat deze weerstand zouden kunnen bieden. Zichtbaarheid heeft betrekking op de zichtbaarheid van een internetgebruiker of van een object dat toebehoort aan de internetgebruiker. Toegankelijkheid verwijst naar het gemak waarmee de dader het doel kan bereiken. In cyberspace heeft dat betrekking op de zwakten van software of internetsystemen (Leukfeldt & Yar, 2016). Uit de toepassing van deze vier elementen is op te maken dat een hogere waarde, zichtbaarheid, draagbaarheid en toegankelijkheid van het doel de kans om slachtoffer te worden vergroot voor de eigenaar van het doel.

Op basis van de Routine Activity Theory zou je dus kunnen stellen dat mensen die rijker zijn meer zichtbare online activiteiten uitvoeren en meer gebruik maken van veelgebruikte programma's en browsers een hoger risico lopen om slachtoffer te worden van cybercriminaliteit. Daarnaast zijn er capabele beveiligers die criminele activiteiten op het web tegenhouden, zoals antivirussoftware en firewalls. Op basis daarvan is te verwachten dat mensen die minder goed beveiligd zijn tegen malware en virussen, en zich dus ook minder bewust zijn van het risico dat ze lopen en minder handig zijn met computers, een hoger risico lopen op slachtofferschap (Leukfeldt, 2015). Internetgebruikers die zich bewuster zijn van de risico's hebben dus ook minder kans om slachtoffer te worden omdat ze zich beter weten te weren tegen cybercrimes (Leukfeldt & Yar, 2016). Dit geldt niet voor low-tech phishing, waarbij telefoontjes of e-mails worden gebruikt om inloggegevens te achterhalen en die vervolgens te gebruiken in de offline wereld. Voor high-tech phishing, zoals het installeren van malafide software, blijkt echter dat het doorbrengen van veel tijd op het internet een risicoverhogende factor is, zoals bijvoorbeeld downloaden, online gamen of veelvuldig gebruik van populaire webbrowsers (Leukfeldt, 2015). Daarom wordt gehypothetiseerd dat meer tijd besteden op het internet leidt tot meer slachtofferschap.

Angst om slachtoffer te worden van cybercriminaliteit komt ook voort uit sociale kwetsbaarheid (Riesig, Pratt & Holtfreter, 2009). Sociaal kwetsbare mensen hebben een hoger risico om niet om te kunnen gaan met gebeurtenissen die hun emotionele, fysieke of financiële welzijn negatief kunnen beïnvloeden (Fisher et al., 2016). Sociale kwetsbaarheid is gebaseerd op armoede, scholingsgraad, gezinsstructuur en etnische afkomst (Van Damme & Pauwels, 2010). Mensen die relatief arm zijn, een lage scholingsgraad hebben, een gezinsstructuur die een prettige opvoeding ondermijnt, bijvoorbeeld gescheiden ouders of een eenoudergezin, en een andere etnische achtergrond hebben dan de Nederlandse, zijn sociaal kwetsbaarder dan mensen die niet in deze omstandigheden leven. Deze mensen zijn daarom minder in staat om om te gaan met de economische gevolgen van slachtofferschap, wat mensen beangstigt en waardoor mensen met een laag inkomen en minderheden een hoger slachtofferrisico aangeven (Riesig et al., 2009). Deze angst is niet ongegrond: volgens het onderzoek van Fisher et al. (2016) zijn sociaal kwetsbare mensen ook vaker slachtoffer. Aangezien Rotterdam-

Zuid een lage sociaaleconomische status (SES) heeft, en dus veel mensen sociaal kwetsbaar zijn, zullen zij meer angst hebben om slachtoffer te worden van cybercriminaliteit dan mensen met een hogere SES. Daarom wordt gehypothetiseerd dat een hogere sociale kwetsbaarheid een grotere kans op slachtofferschap in de hand werkt.

De kans om slachtoffer te worden is groter wanneer individuen kennissen hebben die zich afwijkend gedragen op het internet, maar niet per se kleiner wanneer individuen hun digitale apparaten beveiligen met antivirusprogramma's of firewalls (Bossler & Holt, 2009; Maimon et al., 2013). Daarnaast zorgen persoonlijke vaardigheden op het internet voor een vermindering van de kans op slachtofferschap (Holt & Bossler, 2013), waar veel tijd besteden op het internet die kans juist verhoogt (Yucedal, 2010, zoals beschreven in Maimon & Louderback, 2019; Leukfeldt & Yar, 2016; Reyns, 2015; Wang et al., 2015). Hoogopgeleiden hebben vaker een computer in huis en beschikken over meer vaardigheden als het gaat om het bedienen van die computer en kunnen vaak de technologische ontwikkelingen redelijk bijhouden. Aan de andere kant maken ze tegelijkertijd ook meer gebruik van het internet, wat het risico om slachtoffer te worden van cybercriminaliteit weer verhoogt (Van Deursen & Van Dijk, 2010). Dat geldt ook voor jongeren (Näsi et al., 2015). Hoogopgeleiden hebben minder kans om gehackt te worden (Van Wilsem, 2013, zoals beschreven in Maimon & Louderback, 2019), maar de kans is wel groter dat zij slachtoffer worden van de installatie van malware en fraude (Leukfeldt & Yar, 2016). Bij gedigitaliseerde criminaliteit, zoals consumentenfraude, hebben laagopgeleiden en werklozen een grotere kans om slachtoffer te worden, wellicht omdat ze geld willen besparen (ibid). Op basis hiervan zou gesteld kunnen worden dat laag opgeleide jongeren een risicogroep vormen als het gaat om cybercriminaliteit.

Daarnaast zorgen immigranten ervoor dat de digitale wegen naar hun thuisland open blijven door te communiceren met familie in het thuisland en internationale websites te bezoeken, waardoor toegang en dus ook een aanval op computers in andere landen via binnenlandse computers eenvoudig wordt voor potentiële cybercriminelen. Deze verbinding maakt het ook voor cybercriminelen in het buitenland mogelijk om toegang te krijgen tot binnenlandse computersystemen. Immigranten onderhouden dus het internationale karakter van cybercriminaliteit (Leukfeldt & Yar, 2016). Individuen wiens ouders allebei uit het buitenland komen hebben dan ook een grotere kans om slachtoffer te worden van cybercriminaliteit (Näsi et al., 2015).

Bovenstaande studies geven de indruk dat inwoners van gebieden die gekenmerkt worden door de genoemde factoren een hoger risico lopen om te maken te krijgen met cybercriminaliteit dan inwoners die niet in zulke gebieden wonen. Een voorbeeld van zo'n gebied is Rotterdam-Zuid. Veel inwoners zijn laag of middelbaar opgeleid, wat impliceert dat zij minder vaak beschikken over een computer en hun vaardigheden op het internet minder ontwikkeld zijn, waardoor ze vatbaarder zijn voor cyberrisico's (Van Deursen & Van Dijk, 2010). Daarnaast heeft Rotterdam-Zuid een relatief hoog aantal inwoners met een migratieachtergrond (62%, zie Tabel 1). Daarom is het risico dat deze inwoners

slachtoffer worden of deels bijdragen aan de toegankelijkheid van binnenlandse computersystemen vanuit het buitenland groter.

2.4 Context Rotterdam-Zuid

Om een goede koppeling te maken tussen theorieën rondom cybercriminaliteit en Rotterdam-Zuid, is er wat meer context nodig. Rotterdam-Zuid is het gedeelte van Rotterdam dat onder de Nieuwe Maas ligt en bestaat uit drie wijken: Charlois, Feijenoord en Ijsselmonde. Rotterdam-Zuid is een achterstandsgebied met iets meer dan 200.000 inwoners. De bevolkingssamenstelling van Rotterdam-Zuid is heel divers. Niet alleen huisvest Rotterdam de meeste nationaliteiten in Nederland, maar inwoners met een migratieachtergrond maken ook een groot deel uit van de Rotterdamse bevolking (Gemeente Rotterdam, 2019). Tabel 1 toont de verhoudingen tussen inwoners zonder en met migratieachtergrond. Jongeren worden hier gedefinieerd als personen in de leeftijd van dertien tot en met vierentwintig jaar.

Tabel 2. Bevolkingssamenstelling Rotterdam-Zuid[1]

	Inwoners zonder migratieachtergrond		**Inwoners met migratieachtergrond**		**Totaal aantal inwoners**	
	Totaal	Jongeren	Totaal	Jongeren	Totaal	Jongeren
Feijenoord	23.528 (31,4%)	1.871	51.442 (68,6%)	7.509	74.970	9.380
Ijsselmonde	29.643 (49,3%)	2.205	30.451 (50,7%)	4.441	60.094	6.646
Charlois	23.634 (35,2%)	1.878	43.580 (64,8%)	5.811	67.214	7.689
Rotterdam-Zuid	76.805 (38,0%)	5.952	125.473 (62,0%)	17.761	202.278	23.713
Rotterdam	313.634 (49,1%)	19.518	324.547 (50,9%)	46.825	638.181	66.343

2.4.1 Problematiek in Rotterdam-Zuid

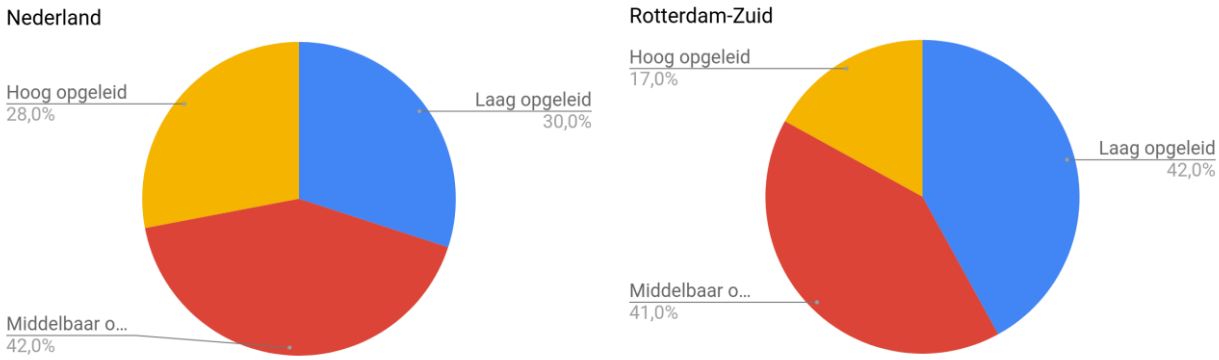
Veel inwoners van Rotterdam-Zuid hebben problemen met hun eigen woning of het vinden van een geschikte woning. De prijs van de woning ligt boven hun budget of ze hebben problemen met de verhuurder. Bovendien is wonen in Rotterdam-Zuid vooral aantrekkelijk voor mensen met een lager inkomen: 68% van de mensen die verhuizen naar Charlois, Feijenoord of Ijsselmonde heeft een laag inkomen. Soms zijn de problemen zo vergevorderd dat mensen in een opvang wonen, niet zelfstandig wonen of binnenkort geen onderdak meer hebben. Het NPRZ is op dit moment bezig met groot

[1] Aangepast van "Rotterdam in Cijfers", door Gemeente Rotterdam. Verkregen via https://rotterdam.buurtmonitor.nl/jive?cat_open=Beleidsthema%27s/Demografie/.

onderhoud in Vreewijk en er komen veel nieuwe voorzieningen rond winkelcentrum Zuidplein (NPRZ, 2019).

Daarnaast is er in Rotterdam een mismatch tussen onderwijsrichting en vraag op de arbeidsmarkt. Veel leerlingen kiezen een richting waarin het aantal banen afneemt en ze niet in Rotterdam aan het werk kunnen, wat kan leiden tot werkloosheid. Het NPRZ tracht leerlingen meer te laten kiezen voor sectoren die wel kansrijk zijn, zoals techniek, haven, zorg en voedingsmiddelen. Bovendien is een opleiding na het vmbo niet altijd de eerste keuze van jongeren, omdat zij soms het criminele pad verkiezen boven een opleiding (NPRZ, 2019). Daarnaast is het gemiddelde opleidingsniveau van Rotterdam-Zuid relatief laag vergeleken met dat van andere steden. Het gemiddelde opleidingsniveau ligt net onder het Nederlands gemiddelde. Figuur 1 toont het gemiddelde opleidingsniveau van de beroepsbevolking van Rotterdam-Zuid en Nederland in 2017.

Figuur 1. Gemiddeld opleidingsniveau Nederland en Rotterdam-Zuid

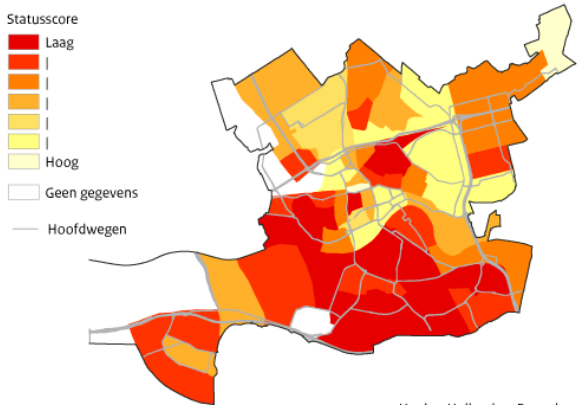


Noot: Bron: CBS, Sociaal Statistisch Bestand. Aangepast van "Feitenkaart Opleidingsniveau Rotterdam op gebieds- en buurtniveau 2017", door Gemeente Rotterdam, 2017.[2]

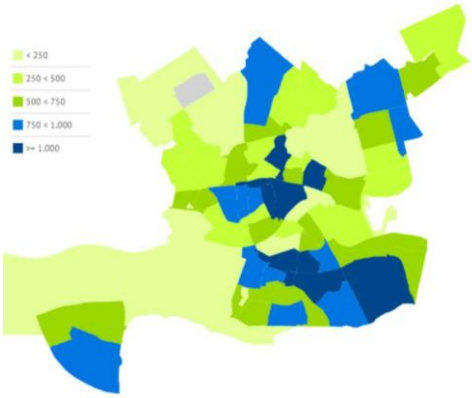
Bovendien is de werkloosheid in regio Rijnmond met 8,2% het hoogst van Nederland. De werkloosheid in wijken in Rotterdam-Zuid ligt altijd net een beetje boven het gemiddelde in Rotterdam (5,9% in 2016) (Gemeente Rotterdam, 2019). Daarbij is de werkloosheid onder inwoners met een migratieachtergrond (6,4%) flink hoger dan inwoners zonder migratieachtergrond (2,8%). De werkloosheid onder jongeren van 15 tot 25 jaar is het hoogst (6,6%) (CBS, 2019b). Verbonden aan en gebaseerd op werkloosheid is sociaaleconomische status (SES). In Figuur 2 is te zien dat Rotterdam-Zuid een lagere SES heeft dan de andere delen van Rotterdam. De SES is gebaseerd op gemiddeld inkomen, het percentage mensen met een laag inkomen, het percentage laagopgeleiden en het percentage werklozen (Volksgezondheidenzorg.info, 2017).

[2] Geraadpleegd via https://rotterdam.buurtmonitor.nl/handlers/ballroom.ashx?function=download&id=443&rnd=0.7711963653236316.

Figuur 2. Sociaaleconomische status[3]



Figuur 3. Misdrijven in 2018[4]



Rotterdam-Zuid is een hotspot wat betreft ondermijnende criminaliteit. Hoewel de criminaliteitscijfers afnemen, vond nog steeds 6,3% van de geregistreerde misdaden plaats in Rotterdam in 2018 (CBS, 2019c). Figuur 3 toont het aantal misdrijven in Rotterdam in 2018. Ook hier is zichtbaar dat de meeste misdrijven plaatsvinden in het zuiden van Rotterdam. Op basis van de patronen die zichtbaar zijn op bovenstaande kaarten van Rotterdam kan verwacht worden dat criminaliteit samenhangt met sociaaleconomische status. In 2016 vond een derde van de verdachte negenduizend transacties in regio Rotterdam plaats in Rotterdam-Zuid, wat suggereert dat ondermijnende criminaliteit erg aanwezig is in Rotterdam-Zuid (NPRZ, 2019). Bovendien neemt cybercriminaliteit in zijn geheel toe, maar vooral in Rotterdam is een flinke stijging zichtbaar: 6,2% van de computervredebreuken (*hacks*) vond hier plaats, een stijging van honderd procent ten opzichte van 2017 (CBS, 2019c).

2.4.2 Verweven problematiek

Vanwege de grootte van Rotterdam-Zuid zijn de problemen op gebied van werk, wonen, onderwijs en veiligheid wijd verspreid geraakt (Schram, Scherpenisse & Van Twist, 2018). Niet alleen zijn deze problemen zichtbaar in verschillende wijken in Rotterdam-Zuid, ze zijn ook sterk met elkaar verweven, waardoor het vaak lastig is om causale verbanden waar te nemen. Om enige vat op deze problemen te krijgen hebben lokale overheden, woningcorporaties, onderwijsinstellingen, lokale ondernemers en bewoners besloten samen te werken ter verbetering van het gebied, wat in 2012 heeft geleid tot de oprichting van het NPRZ. Dit samenwerkingsverband tracht de achterstandsproblemen te bestrijden en zo de levensomstandigheden in Rotterdam-Zuid te verbeteren en doelt om Rotterdam-Zuid in 2031 op het gemiddelde niveau te brengen van de vier grote steden in Nederland: Amsterdam, Den Haag, Utrecht

[3] Bron: SCP. Overgenomen van Volksgezondheidenzorg.info, 2017. Verkregen via https://www.volksgezondheidenzorg.info/onderwerp/sociaaleconomische-status/regionaal-internationaal/regionaal#node-sociaaleconomische-status/

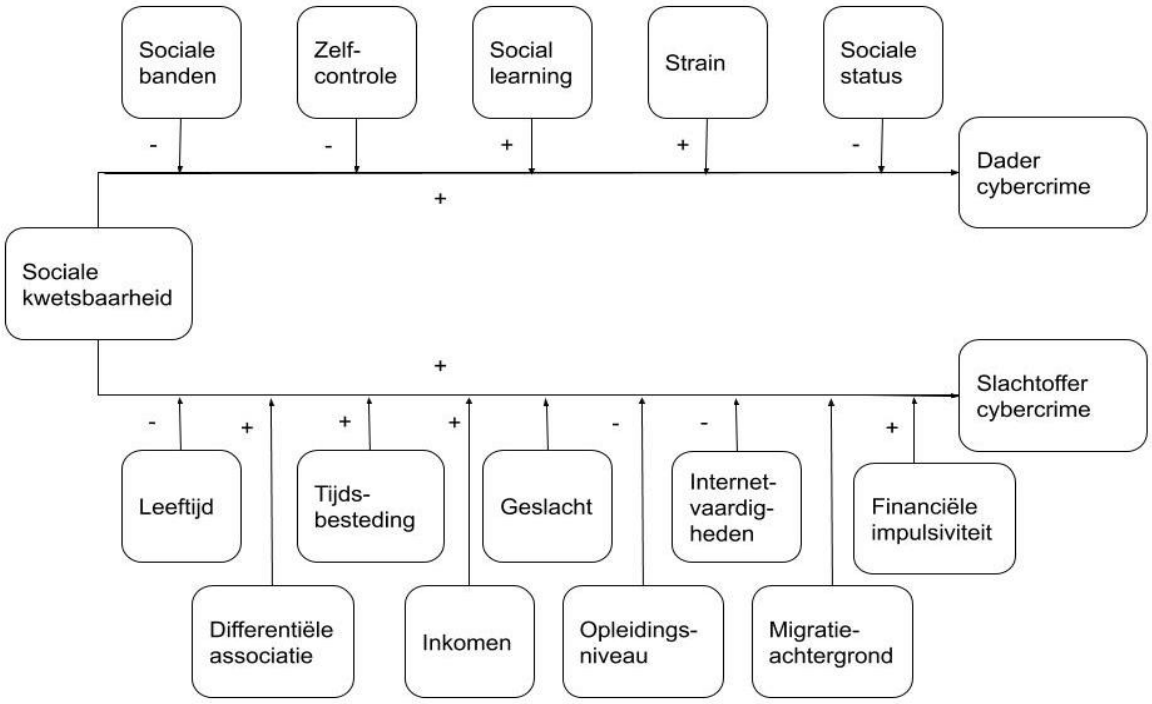
[4] Overgenomen van Gemeente Rotterdam, 2018. Verkregen via https://rotterdam.buurtmonitor.nl/jive?cat_open=Beleidsthema%27s/Leefbaarheid%20en%20veiligheid.

en Rotterdam (NPRZ, 2019). In 2014 is er naast het NPRZ een andere aanpak ontwikkeld voor het bestrijden van ondermijnende criminaliteit, omdat dit in hoge mate aanwezig is in Rotterdam-Zuid, sterk is verweven met andere problemen en ook de kansen om te groeien ondermijnt (Schram et al., 2018).

De verwevenheid van de problematiek is goed zichtbaar in de situatie van jongeren in Rotterdam-Zuid. Jongeren die opgroeien in achterstandswijken hebben over het algemeen minder kansen en een minder ondersteunend sociaal netwerk. Dat heeft echter niet hetzelfde effect op elk individu en daarnaast spelen andere factoren ook een rol. Zo wordt sociale ongelijkheid bijvoorbeeld gereproduceerd door ongelijke toegang tot hulpbronnen, zoals geld, werk, opleiding en huisvesting. Daarnaast is er ook niet altijd een aansluiting tussen een geschikte baan en individuele competenties, die vaak nog in ontwikkeling zijn (Tan & Spies, 2014). Zo hebben risicogebieden als Rotterdam-Zuid veel werklocaties langs de snelweg en weinig vervoersmogelijkheden om bij zulke locaties te komen, waardoor inwoners kunnen lijden onder vervoersarmoede (Bastiaanssen, Martens & Polhuijs, 2013). Inwoners van Rotterdam-Zuid kunnen ernstige sociale gevolgen ervaren als gevolg van het onvermogen om zich zo te verplaatsen dat ze een volwaardig lid van de samenleving kunnen zijn. Dit kan bijvoorbeeld leiden tot werkloosheid, wat kan resulteren in sociale uitsluiting, waarbij mensen “de aansluiting met veel banen, diensten, voorzieningen en sociale netwerken zijn verloren.” (p.2). Als gevolg hiervan kunnen inwoners van Rotterdam-Zuid niet optimaal sociaal integreren en zich niet persoonlijk ontwikkelen (Bastiaanssen et al., 2013).

Tot nu toe is beschreven hoe daderschap en slachtofferschap kunnen worden verklaard en is naar voren gekomen dat daarbij veel factoren een rol spelen. Deze verklaringen zijn echter nog niet getoetst met betrekking tot een lokaliteit zoals Rotterdam-Zuid. Op basis van bovenstaande kenmerken van Rotterdam-Zuid is de verwachting dat de verklaringen die zijn genoemd in de theoretische achtergrond sterker gelden voor inwoners van Rotterdam-Zuid dan voor inwoners van andere gebieden. Figuur 4 toont de theoretische relaties tussen de concepten in het conceptueel model en Tabel 3 ondersteunt dit model met de hypothesen die dit onderzoek zal toetsen. Het doel van deze scriptie is tenslotte om te onderzoeken welke vormen van cybercriminaliteit in Rotterdam-Zuid voorkomen, hoe sociaaleconomische achterstanden deze kunnen verklaren en op welke manieren betrokken partijen een meer integrale aanpak kunnen ontwikkelen om cybercriminaliteit te verminderen. De eerste twee elementen zullen worden getoetst in het wetenschappelijk segment door middel van afname van een enquête onder jongeren tussen de veertien en drieëntwintig jaar uit Rotterdam-Zuid. Het laatste element zal vooral naar voren komen in het beleidssegment, waarbij betrokken partijen worden geïnterviewd.

Figuur 4. Conceptueel model



Tabel 3. Overzicht hypothesen

Concept	Hypothese
Daderschap	
Sociale kwetsbaarheid	H1: Hoe sociaal kwetsbaarder een individu, hoe vaker het individu betrokken is bij het plegen van cybercriminaliteit.
Zelfcontrole	H2: Hoe minder zelfcontrole, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.
Strain	H3: Hoe meer strain individuen ervaren, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.
Social learning	H4: Hoe meer kennissen van een individu betrokken zijn bij cybercriminaliteit, hoe vaker het individu betrokken is bij het plegen van cybercriminaliteit.
Sociale banden	H5: Hoe zwakker de banden met de gemeenschap, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.
Sociale status	H6: Hoe lager de sociale status, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.
Slachtofferschap	
Gender	H7: Mannen hebben een grotere kans om slachtoffer te worden van cybercriminaliteit dan vrouwen.
Sociale kwetsbaarheid	H8: Hoe sociaal kwetsbaarder een individu, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.
Leeftijd	H9: Hoe jonger een individu, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.
Differentiële associatie	H10: Hoe meer kennissen van een individu betrokken zijn bij cybercriminaliteit, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.
Opleidings-niveau	H11: Hoe lager het opleidingsniveau, hoe groter de kans om slachtoffer te worden van gedigitaliseerde criminaliteit.
Werkstatus	H12: Hoe lager de werkstatus, hoe groter de kans om slachtoffer te worden van gedigitaliseerde criminaliteit.
Rijkdom	H13: Hoe rijker een individu is, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.
Financiële impulsiviteit	H14: Hoe financieel impulsiever mensen zijn, hoe banger ze zijn om slachtoffer te worden van cybercriminaliteit.
Internet-vaardigheden	H15: Hoe minder computervaardigheden een individu bezit, hoe groter de kans voor dat individu om slachtoffer te worden van cybercriminaliteit.
Tijdsbesteding	H16: Hoe meer tijd mensen besteden op het internet, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.
Migratie-achtergrond	H17: Mensen met een migratieachtergrond hebben een grotere kans om slachtoffer te worden van cybercriminaliteit dan mensen zonder migratieachtergrond.
Woonplaats	H18: Inwoners van Rotterdam-Zuid hebben een grotere kans om te maken te krijgen met cybercriminaliteit dan mensen die niet in Rotterdam-Zuid wonen.

3. Methode

Dit onderzoek maakte gebruik van mixed methods. Er is gekozen voor mixed methods omdat het doel van het onderzoek is om een beeld te krijgen van cybercriminaliteit in Rotterdam-Zuid en om te onderzoeken wat het huidige beleid is en hoe de betrokken partijen een integrale aanpak kunnen bewerkstelligen. Deze twee onderzoeksdoelen vereisen een andere benadering wat betreft methoden, omdat een beeld van cybercriminaliteit vertaald kan worden naar een kwantitatieve studie, hier genoemd wetenschappelijk segment, en de verkenning van het beleid het best vertaald kan worden naar een kwalitatieve studie, hier genaamd beleidssegment. Hoewel het beleidssegment niet direct wetenschappelijk genoemd wordt, betreft het hier wel een wetenschappelijke, kwalitatieve studie. Het wetenschappelijk segment en het beleidssegment bieden gronden om wetenschappelijke uitspraken te doen. Het beleidssegment geeft daarnaast ook suggesties voor beleid.

3.1 Wetenschappelijk segment: Enquêttering onder jongeren

Het wetenschappelijk segment omvat de studie van het vóórkomen van cybercriminaliteit onder jongeren in Rotterdam-Zuid door middel van de verspreiding van een enquête onder jongeren van veertien tot drieëntwintig jaar. Beleidsmakers en overheidsorganen gaan vaak te werk naar aanleiding van politiestatistieken. De statistieken aangaande cybercriminaliteit zijn echter erg beperkt en er is een groot *dark number* (WODC, 2019). Deze enquête is een aanvulling op de bestaande kennis over cybercriminaliteit omdat deze een indicatie geeft van wat er werkelijk plaatsvindt wat betreft cybercriminaliteit in Rotterdam-Zuid. De enquête is specifiek verspreid onder jongeren, omdat zij meer gebruik maken van het internet, waardoor ze een hoger risico lopen om slachtoffer te worden van cybercriminaliteit. Juist daarom verschaffen zij belangrijke informatie omtrent dit onderwerp (Näsi et al., 2015).

Er is gekozen voor een enquête omdat dit een eenvoudige en betrouwbare manier is om uitspraken te doen over een populatie op basis van een representatieve steekproef. Bovendien kunnen jongeren cybercriminaliteit zien als een gevoelig onderwerp, zeker als het om daderschap gaat, waardoor ze liever anoniem willen blijven. Een enquête is dan een goede garantie van anonimiteit. Het doel van de enquête is om een beeld te vormen van in hoeverre cybercriminaliteit voorkomt in Rotterdam-Zuid en met welke demografische of sociale factoren cybercriminaliteit samenhangt, om dit fenomeen op basis van deze factoren te verklaren. De enquête bevat vragen over verschillende typen cybercriminaliteit, denk aan phishing e-mails of oplichting via websites. Voor elk type cybercriminaliteit werd dit bevraagd. De respondenten konden per cybermisdaad aanvinken of ze slachtoffer zijn geweest of wel eens een misdaad hebben gepleegd via het internet. Er is ook gevraagd of zij leeftijdsgenoten, vrienden, familieleden of kennissen hebben die zich schuldig maken aan cybercriminaliteit en of de respondenten hen wel eens hebben geholpen.

3.1.1 Dataverzameling en steekproef

Allereerst werd de enquête verspreid op middelbare scholen, mbo-scholen en hogescholen in Rotterdam-Zuid. Kinderen tot achttien jaar hebben leerplicht in Nederland en na hun achttiende hebben jongvolwassenen de plicht om een startkwalificatie te halen (een startkwalificatie is een diploma havo, vwo, mbo niveau 2 of hoger). Daarom zijn middelbare en mbo-scholen een handige manier om jongeren te benaderen. Een nadeel van deze methode is dat bepaalde groepen jongeren niet de kans krijgen om de enquête in te vullen, omdat ze bijvoorbeeld vroegtijdig zijn gestopt met de opleiding of hun opleiding hebben afgerond. Daarnaast kan het zijn dat scholen of ouders geen toestemming willen geven. Naast verspreiding via scholen is de enquête ook verspreid via de sociale media LinkedIn en Facebook en het persoonlijke netwerk. Tezamen hebben deze methoden een steekproef van 161 respondenten opgeleverd.

Een deel van de scholieren stroomt na de middelbare school door naar het hbo of de universiteit. Het is moeilijker om deze scholieren te bereiken, omdat er maar één hogeschool is gevestigd in Rotterdam-Zuid, namelijk InHolland. Om dit probleem op te lossen, zijn de Hogeschool Rotterdam en Erasmus Universiteit bezocht en is de enquête daar verspreid. Daarbij is in de enquête een onderscheid gemaak tussen respondenten die wonen in Rotterdam-Zuid en respondenten die elders wonen. Op deze manier is het beter mogelijk om de hypothesen over verschillen tussen hoog- en laagopgeleiden te toetsen en er zal sprake zijn van een meer representatieve steekproef. Door middel van het enquêteren van studenten van de hogeschool en de universiteit is de steekproef ook representatiever wat betreft leeftijd, omdat hier niet alleen jongeren zijn van veertien tot achttien jaar, maar ook van achttien tot drieëntwintig jaar.

Daarnaast hebben de middelbare scholen in Rotterdam-Zuid vooral leerlingen met een migratieachtergrond, waar hogescholen en universiteiten ook meer variatie in kunnen aanbieden, omdat mensen uit de hele omgeving van Rotterdam een vervolgopleiding in deze stad kunnen kiezen. Vanwege het hoge percentage mensen met een migratieachtergrond in Rotterdam-Zuid, is er op middelbare scholen in Rotterdam-Zuid een hoger percentage leerlingen met een migratieachtergrond dan op mbo- of hogescholen of de universiteit, omdat deze zich voornamelijk in andere stadsdelen bevinden en dus ook bewoners uit andere stadsdelen aantrekken. Het benaderen van hbo- of universitaire studenten verhoogt dan ook de kans op een representatieve steekproef wat betreft etnische diversiteit.

Het enquêteren van jongeren onder de achttien jaar vereist toestemming van de school of ouders. Als de school toestemming geeft, is het niet meer nodig om toestemming te vragen aan de ouders, omdat de school op dat moment verantwoordelijk is voor de leerlingen. De scholen is om toestemming gevraagd door middel van een brief waarin het doel van het onderzoek staat beschreven en de leerlingen of studenten worden verzekerd van anonimiteit en vertrouwelijke behandeling van hun respons. Daarnaast kan het zo zijn dat leerlingen die slachtoffer zijn geweest van zedendelicten via het internet of cyberpesten de vragen niet of niet eerlijk willen beantwoorden. Daarom werd in de enquête zeer duidelijk gemaakt dat de antwoorden van de respondenten anoniem blijven en alleen worden

gebruikt in het kader van het onderzoek. Bovendien is het ook mogelijk dat daders van cybercriminaliteit niet in de enquête wilden toegeven dat ze een misdaad via het internet hebben gepleegd. Ook in dit geval bleek duidelijk dat het een anonieme en vertrouwelijke enquête is en dat het doel van het onderzoek is om te ondervinden in welke mate cybercriminaliteit voorkomt in Rotterdam-Zuid en hoe dat verklaard kan worden, niet om daders via de enquête aan te geven bij de politie.

3.1.2 Operationalisatie

Aan het begin van de enquête is aan de respondenten gevraagd hun demografische kenmerken in te vullen, zoals leeftijd, geslacht, etnische afkomst, arbeidsstatus, opleidingsniveau en woonplaats. De variabele leeftijd is verdeeld in de categorieën 'Jonger dan 14 jaar', '14 tot 16 jaar', '17 tot 20 jaar', '21 tot 23 jaar' en 'Ouder dan 23 jaar' omdat de verwachting is dat er verschillen zijn tussen bepaalde leeftijdscategorieën wat betreft internetvaardigheden, maar ook wat betreft het in aanraking komen met cybercriminaliteit. Bij de variabele geslacht konden de respondenten kiezen uit 'Man', 'Vrouw' of 'Anders'. Bij de variabele 'etnische afkomst' is er gekozen voor een open vraag, omdat met name Rotterdam-Zuid veel etniciteiten huisvest en het onderzoek niemand bij voorbaat wil uitsluiten. Een oplossing zou zijn om de meest voorkomende etniciteiten als antwoordcategorie op te nemen en ook een optie 'Anders, namelijk:' toe te voegen, maar mensen met een andere etniciteit dan de genoemde etniciteiten zouden zich dan benadeeld kunnen voelen. Arbeidsstatus werd gemeten aan de hand van de volgende antwoordcategorieën: 'Student', 'Werkloos', 'Verzorger', 'Deeltijd werkzaam', 'Voltijd werkzaam' of 'Anders, namelijk:'. Dezelfde antwoordcategorieën gelden voor de arbeidsstatus van de ouders. Ook werd gevraagd naar het opleidingsniveau van de respondenten, waarbij respondenten konden kiezen uit de antwoordcategorieën 'Basisschool', 'Vmbo/mavo', 'Havo', 'Vwo', 'MBO', 'HBO' of 'WO'. Tenslotte werd er gevraagd naar de woonplaats en wijk waar de respondent woont, omdat uit de enquête moet blijken of respondenten uit Rotterdam-Zuid meer of minder met cybercriminaliteit te maken hebben dan respondenten die niet uit Rotterdam-Zuid komen. Ook dit is een open vraag.

Het centrale deel van de enquête bestond uit de vragen over verschillende soorten cybercriminaliteit. Onder andere de typen cybercriminaliteit die worden genoemd in de bestaande literatuur zijn in de enquête opgenomen (Leukfeldt & Yar, 2016). De volgende typen cybercriminaliteit kwamen daarin naar voren: een virus, malware, phishing, ransomware, botnet, cryptojacking (geld verdienen door cryptogeld te verkrijgen, bijvoorbeeld de bitcoin), pinpasfraude, helpdeskfraude, identiteitsfraude, terrorisme of bedreiging, DDoS-aanvallen, hacking, internetoplichting (bijvoorbeeld marktplaatsfraude), defacing, password cracking, cyberafpersing, cyberstalking, cyberpesten en kinderporno. Bij elk type cybercriminaliteit konden de respondenten aanvinken in welke hoedanigheid ze daarmee te maken hebben gehad: 'Ik heb hier niet mee te maken gehad', 'Ik ben slachtoffer geworden van [cybercrime] en heb hier schade aan ondervonden', 'Ik heb met [cybercrime] te maken gehad, maar heb ervoor kunnen zorgen dat er geen schade gemaakt kon worden', 'Ik heb wel eens geprobeerd om

[cybercrime] te plegen', 'Ik pleeg regelmatig [cybercrime]' of 'Anders, namelijk:'. Er is een beschrijving toegevoegd bij elk type cybercriminaliteit om te voorkomen dat respondenten invullen dat ze niet met dit type cybercriminaliteit te maken hebben gehad omdat ze het niet herkenden. Er is gekozen om zowel slachtofferschap als daderschap te toetsen in dezelfde vraag ten behoeve van de lengte van de enquête. Daarbij is rekening gehouden met het beperkte concentratievermogen van jongeren en het zou als belastend kunnen worden ervaren als de jongeren ook nog eens twee vragen per cybermisdaad zouden moeten beantwoorden. Bij de analyse werd er onderscheid gemaakt tussen gedigitaliseerde en high-tech cybercriminaliteit op basis van de classificatie in Hoofdstuk 3.

Het eerste concept dat aan bod kwam in de enquête is zelfcontrole (Hirshi, 1969). Zelfcontrole is het vermogen van een individu om reacties en humeuren aan te passen (Baumeister, 2002, zoals beschreven in D'Hont, 2009). Zelfcontrole werd gemeten op basis van een 7-punts Likertschaal met dertien items die ontwikkeld is door Tangney et al. (2004, zoals beschreven in D'Hont, 2009). Deze schaal bevat stellingen over luiheid, discipline, verleidingen, prioriteren en vooruitdenken. De schaal heeft een hoge interne consistentie in dit onderzoek (α = 0,846) en de stellingen zijn eenvoudig geformuleerd, zodat jongeren ze gemakkelijk kunnen begrijpen.

Een tweede concept is differentiële associatie, wat volgens de Social Learning Theory inhoudt dat individuen het gedrag van hun leeftijdsgenoten overnemen (Maimon & Louderback, 2019). Differentiële associatie is gemeten door de respondenten aan te laten geven in hoeverre hun kennissen wel eens te maken hebben gehad met cybercriminaliteit in een open vraag in de enquête.

Ten derde is sociale cohesie belangrijk in het verklaren van cybercriminaliteit. Volgens Wittebrood (z.d.) bestaat sociale cohesie uit vier dimensies: gemeenschappelijke waarden en normen, sociale controle, sociale interactie en identificatie met de buurt. Sociale cohesie is gemeten aan de hand van stellingen die gebaseerd zijn op deze vier dimensies. De respondenten werd gevraagd om aan te geven in hoeverre ze het eens waren met de stellingen op basis van een 7-punts Likertschaal (α = 0,928).

Het vierde concept dat betrekking heeft op daderschap is strain. Strain is het gevolg van veel factoren die spanning kunnen veroorzaken bij een individu. De factoren die in onderzoek worden meegenomen zijn financiële situatie, gezinssamenstelling en sociaaleconomische status (SES) op basis van de arbeidsstatus van de respondent en de ouders van de respondent. Financiële situatie werd gemeten aan de hand van het inkomen en het bezit van een eigen laptop, tablet en mobiele telefoon door respondenten. Bij de variabele 'inkomen' konden de respondenten kiezen uit een aantal categorieën, namelijk 'Ik krijg een uitkering', 'Ik heb geen inkomen' of één van de inkomensklassen die daarna volgden in categorieën met een grootte van tienduizend euro, steeds oplopend tot en met 'Meer dan €75.000'. Het persoonlijke bezit van een laptop, tablet of mobiele telefoon konden de respondenten aangeven in het meerkeuzeraster bij de vraag over het gebruik van digitale apparaten. Bij de variabele 'gezinssamenstelling' konden de respondenten aangeven of ze bij twee ouders, gescheiden ouders of één ouder, in een opvang of zelfstandig wonen en of ze broertjes of zusjes hebben.

Het laatste concept dat in dit onderzoek van belang is voor daderschap is sociale status. Sociale status bestaat uit inkomen, arbeidsniveau en opleidingsniveau. Deze drie variabelen werden al gemeten als demografische factoren aan het begin van de enquête. Inkomen werd gemeten zoals hierboven beschreven. De drie variabelen tellen samen op tot een bepaalde score die een indicatie geeft van de sociale status.

In de theorie kwam ook naar voren dat rijke mensen meer kans hebben om slachtoffer te worden dan arme mensen. De meeste jongeren zullen echter nog niet veel eigen vermogen hebben en het is de vraag of zij weten wat hun ouders verdienen. Dat zegt dan nog niets over hun eigen slachtofferschap. De enquête bevat vragen over bijbaantjes van leerlingen of studenten en of ze een eigen computer hebben. Deze vragen kunnen een indicatie geven over de relatieve welvaart van de respondenten.

Internetvaardigheden werden gemeten aan de hand van een 7-punts Likert-schaal op basis van vijf items ($\alpha = 0{,}912$). Daarnaast is het belangrijk om te meten hoeveel tijd de respondenten besteden op het internet, wat zij konden invullen op basis van een inschatting van het aantal uren dat ze per week op het internet besteden. Daarbij is het van belang dat er een onderscheid wordt gemaakt tussen internetgebruik op de computer thuis en op school en internetgebruik via mobiele apparaten, zoals mobiele telefoons en iPads, omdat mobiele apparaten vaak minder goed zijn beveiligd. De respondenten werd gevraagd per digitaal apparaat in te vullen waar ze dat apparaat vooral voor gebruiken, waarbij ze konden kiezen uit ‘Ik gebruik dit apparaat nooit’, ‘Ik gebruik dit apparaat niet om het internet te gebruiken’, ‘Downloaden van het internet’, ‘Online gamen’, ‘Informatie opzoeken via Google, Google Chrome, Yahoo!, Firefox, Internet Explorer, Microsoft Edge of Safari (Apple)’, ‘Informatie opzoeken via andere webbrowsers’, ‘Werken met Microsoft Office (Word, Excel, PowerPoint, etc.)’, ‘Sociale media’, ‘Online shoppen’ of ‘Anders’. Daarna konden de respondenten aanvinken welke van hun digitale apparaten zijn voorzien van één soort virusbeveiliging en welke van meer soorten virusbeveiliging. Ten slotte konden respondenten zelf invullen wat zij denken dat de risico’s zijn van internetgebruik.

Niet alleen werkelijk slachtofferschap is van belang. Ook angst om slachtoffer te worden is belangrijk bij het maken van een indicatie van cybercriminaliteit in Rotterdam-Zuid. Deze angst komt vooral voor bij sociaal kwetsbare en financieel impulsieve mensen. Sociale kwetsbaarheid is gemeten door middel van armoede, scholingsgraad, gezinsstructuur en etnische afkomst (Van Damme & Pauwels, 2010). In dit onderzoek werd armoede vertaald naar een lage SES, geoperationaliseerd als het werknemerschap van de vader, waarbij werkloosheid van de vader een lage SES, en dus armoede, indiceert. Scholingsgraad heeft betrekking op de opleiding die de student nu volgt of heeft afgerond, wat al in het eerste deel van de enquête naar voren komt. Gezinsstructuur verwijst naar de samenstelling van het gezin: ouders zijn samen, ouders zijn gescheiden, wel of geen broertjes en zusjes, of een eenoudergezin (ibid). Financiële impulsiviteit werd gemeten aan de hand van hun levensstijl, uitgaven, het weerstaan van verleidingen en vertrouwen in zichzelf, waarbij de respondenten hier een indicatie van kunnen geven op een 7-punts Likertschaal ($\alpha = 0{,}609$).

3.1.3 Analytische strategie

De data uit de enquête werd geanalyseerd door middel van meervoudige regressie. Een regressieanalyse kan de sterkte bepalen tussen twee variabelen, waarbij gedigitaliseerde criminaliteit en high-tech cybercriminaliteit de afhankelijke variabele zijn. Daarbij kan de mate waarin iemand te maken krijgt met cybercriminaliteit worden voorspeld als de onafhankelijke variabele verandert. Meervoudige regressie maakt gebruik van meerdere onafhankelijke variabelen om de afhankelijke variabele te voorspellen. Dat is nodig in dit onderzoek omdat het onbekend is welke vormen van cybercriminaliteit voorkomen en welke factoren cybercriminaliteit veroorzaken. Daarom is er voor elke hypothese een aparte meervoudige regressieanalyse uitgevoerd. De demografische gegevens zijn gebruikt als controlevariabelen, tenzij ze al onderdeel zijn van een van de variabelen die in de regressievergelijking is opgenomen. In deze regressieanalyse is ook een interactievariabele van de betreffende variabele en sociale kwetsbaarheid opgenomen om te testen of het gaat om een interactieverband of een verband met meerdere verklarende variabelen.

De betrouwbaarheid iss gewaarborgd door gebruik te maken van eerder gebruikte schalen voor het meten van zelfcontrole (Tangney et al., 2004, zoals beschreven in D'Hont, 2009), sociale cohesie (Wittebrood, z.d.) en financiële impulsiviteit (Van Damme & Pauwels, 2010). Op deze manier is het mogelijk het onderzoek te reproduceren en soortgelijke resultaten te verkrijgen. De schalen zijn op betrouwbaarheid getest. Deze onderzoeksmethode is valide omdat niet alleen de schalen eerder gebruikt zijn en dus voldoende meten wat ze meten, maar ook omdat objectieve factoren als opleidingsniveau, sociaaleconomische status en leeftijd in verband worden gebracht met cybercriminaliteit. Aan de hand hiervan wordt gemeten of sociaaleconomische achterstanden samenhangen met cybercriminaliteit.

3.2 Beleidssegment: Verkenning van kennis onder betrokken partijen

Tot nu to is het onduidelijk in hoeverre er sprake is van cybercriminaliteit in Rotterdam-Zuid en welke kennis daarover is, wat de ontwikkeling van een effectieve aanpak hindert. Het doel van het beleidssegment is daarom om te onderzoeken over welke kennis de betrokken partijen beschikken en op welke manieren de betrokken partijen een meer integrale aanpak kunnen ontwikkelen ter bestrijding van cybercriminaliteit in Rotterdam-Zuid. Om dit te bewerkstelligen voerde ik een klein explorerend kwalitatief onderzoek uit door middel van open interviews met de belanghebbenden die betrokken (zouden moeten) zijn bij de aanpak van cybercriminaliteit in Rotterdam-Zuid. Er is voor open interviews gekozen omdat er zeer weinig tot geen kennis lijkt te zijn over cybercrime in Rotterdam-Zuid. Daardoor is het moeilijk om een meer gestructureerde onderzoeksmethode te gebruiken. Open interviews maken het mogelijk om een open en explorerende structuur te hanteren en de respondent zoveel mogelijk kennis te laten delen, zonder te veel gestuurd te worden door vragen. Naast de interviews werden er ook schriftelijke documenten aangeleverd. Op deze manier bestaat het beleidssegment van het onderzoek uit tweeledige kennis, wat samen met het wetenschappelijk segment triangulatie vormt. Het OM heeft

ook daadwerkelijk kennisdocumenten verstrekt. Deze documenten bevatten kennis over cybercriminaliteit in Rotterdam en vullen daarmee de enquête en interviews aan.

3.2.1 Dataverzameling

Er zijn interviews gehouden met ambtenaren van Gemeente Rotterdam, Politie Rotterdam afdeling cyberintelligence, Politie Rotterdam Zuidplein, het Openbaar Ministerie, Reclassering Nederland, Veiligheidsalliantie Rotterdam, Jongerenwerk op Zuid, de National High Tech Crime Unit, de Cyberwerkplaats en de stadsmarinier van Rotterdam-Zuid. Deze partijen hebben te maken met cybercriminaliteit en jongeren, een combinatie die essentieel is in kader van dit onderzoek. Binnen deze organisaties is gezocht naar personen die veel inzicht hebben in cybercriminaliteit, bij voorkeur in Rotterdam-Zuid. De organisaties die betrokken zijn bij cybercriminaliteit zijn niet altijd voornamelijk gericht op Rotterdam-Zuid en daarom kwam Rotterdam-Zuid niet in alle interviews naar voren. De respondenten zijn geworven door middel van contactpersonen van het NPRZ en contactpersonen die werden geworven tijdens overleggen.

De interviews zijn vastgelegd met een spraakopname van een smartphone. Deze smartphone is in het persoonlijke bezit van de onderzoeker en werd met uiterste zorgvuldigheid beschermd. De respondenten zijn er mondeling van verzekerd dat de opnames en transcripten worden verwijderd nadat de scriptie met voldoende resultaat is afgerond. De opnames en transcripten worden niet verder verspreid en zijn zorgvuldig bewaard. Bovendien hebben de respondenten de transcripten kunnen inzien en schriftelijk toestemming kunnen geven voordat ze in de scriptie werden verwerkt. De respondenten zijn allen werkzaam namens een organisatie, welke bepaalde belangen en prioriteiten heeft. Het is mogelijk dat de resultaten van het onderzoek door het perspectief van de organisatie van de respondent zijn gekleurd.

3.2.2 Operationalisatie en analyse

Het beleidssegment bestaat uit drie elementen: kennis, beleid en behoefte. Deze driedeling is gemaakt op basis van de onderwerpen die tijdens de eerste interviews aan bod kwamen. Om beleid te ontwikkelen is eerst kennis nodig over de trends van een bepaald fenomeen en de urgentie waarmee het fenomeen aangepakt dient te worden. Daarom is in de interviews en beleidsdocumenten allereerst aandacht besteed aan de kennis die aanwezig is over cybercriminaliteit in Rotterdam-Zuid. Het eerste topic is daarom het belang van cybercriminaliteit voor de organisatie waar de respondent werkzaam is of van waaruit het document is gepubliceerd. Het tweede topic bestaat uit verklaringen voor cybercriminaliteit (in Rotterdam-Zuid) en het derde topic is het perspectief van de respondent of de organisatie op cybercriminaliteit.

Het tweede element heeft betrekking op beleid. Daarbij is ingegaan op de twee topics huidig beleid en toekomstig beleid, waarbij vaak ook knelpunten van het huidige beleid naar voren komen. Het

is van belang om te achterhalen welk beleid er nu is, tegen welke knelpunten respondenten aanlopen en welk beleid respondenten voor zich zien, omdat er bij de ontwikkeling van een integrale aanpak rekening gehouden kan worden met de knelpunten en de visie op de toekomst van elke betrokken partij, zodat zoveel mogelijk knelpunten kunnen worden geëlimineerd en een zo effectief mogelijke aanpak kan worden ontwikkeld.

Het derde element is behoefte. Het gaat in dit element vooral om de behoefte aan kennis, kennisdeling of capaciteit. Zoals al eerder genoemd is kennis belangrijk om een basis te vormen voor beleid, als een *evidence based policy*. Daarnaast kunnen betrokken partijen behoefte hebben aan samenwerking met andere organisaties, omdat veel verschillende organisaties te maken hebben met cybercriminaliteit. Er is echter nog niet zo'n samenwerkingsverband, omdat de aanpak van het onderwerp bij veel partijen nog in de kinderschoenen staat en elke organisatie onafhankelijk bezig is met de ontwikkeling van een aanpak. Er zijn opzettelijk geen subtopics of concrete vragen bij de subtopics aan de topiclijst toegevoegd, omdat het doel van de interviews en de documentenanalyse is om de respondent zoveel mogelijk informatie te laten geven en de topics te behandelen zoals de respondent de topics ziet.

Nadat de interviews hebben plaatsgevonden, zijn de interviews getranscribeerd en vervolgens geanalyseerd met behulp van het analyseprogramma NVivo. Allereerst heeft de analyse plaatsgevonden aan de hand van open codering, zodat de algemene onderwerpen die de respondenten benoemen bij elkaar komen. Tijdens axiaal coderen werden de open codes met behulp van memo's verder uitgesplitst naar subcodes. Deze subcodes zijn verder gedefinieerd en gesorteerd tijdens selectief coderen. Op basis van dit coderingsproces werden betekenisvolle kennis en informatie gerapporteerd en gekoppeld aan de resultaten van het kwantitatieve onderzoek.

Bij de analyse van de kennisdocumenten is een soortgelijke codering gebruikt. Ook deze analyse is uitgevoerd met behulp van het analyseprogramma NVivo. Ten eerste is de belangrijkste informatie uit elk kennisdocument gecategoriseerd op basis van onderwerp. Daarna is deze informatie verder uitgesplitst in subonderwerpen en specifieker gedefinieerd en gesorteerd. Op deze manier is er bij de analyse van de kennisdocumenten ook sprake van de drie fasen open coderen, axiaal coderen en selectief coderen. Om te voorkomen dat er veel herhaling in de resultatensectie voorkomt, zijn de resultaten van zowel de interviews als de documentenanalyse voor zover mogelijk direct gekoppeld aan de resultaten van de kwantitatieve analyse op basis van de hypothesen zoals geformuleerd in het theoretisch kader.

De betrouwbaarheid is gewaarborgd door gebruik te maken van *peer review*, omdat deze manier van externe revisie ervoor zorgt dat meerdere analisten tot eenzelfde analyse komen en het onderzoek daardoor betrouwbaar, en dus herhaalbaar is. Deze peer review is uitgevoerd door medestudenten. Externe validiteit is gewaarborgd door het kiezen van respondenten op basis van diversiteit in beroep en de organisatie waar de respondenten hun beroep uitvoeren. Het is de bedoeling dat er per betrokken organisatie één of twee personen worden geïnterviewd, zodat er met de informatie uit deze interviews

een breed beeld ontstaat van cybercriminaliteit in Rotterdam-Zuid waarbij verschillende perspectieven centraal staan, niet alleen het perspectief van bijvoorbeeld de politie. Vervolgens werd de interne validiteit gewaarborgd door de resultaten van het onderzoek te delen met de respondenten, zodat zij de resultaten kunnen beoordelen.

4. Resultaten

In de resultatensectie komen eerst de resultaten van de enquête naar voren in het wetenschappelijk segment. Deze resultaten geven antwoord op de eerste twee onderzoeksvragen. Per hypothese wordt besproken of het getoetste verband significant is en of het gaat om een moderatie of mediatie. Er zal meer aandacht worden besteed aan de relaties die wel significant zijn dan aan relaties die niet significant zijn. De resultaten worden samengevat in een overzichtelijke tabel.

Daarnaast komen de interviews en beleidsdocumenten naar voren in het beleidssegment. Deze gegevens zullen een antwoord vormen op de derde onderzoeksvraag en zullen uiteindelijk uitmonden in de vierde onderzoeksvraag die uitgebreid wordt behandeld in Hoofdstuk 6: Beleidsaanbevelingen. De resultaten van de analyse van de interviews en beleidsdocumenten worden behandeld op basis van concepten die resulteren uit de analyse.

4.1 Wetenschappelijk segment

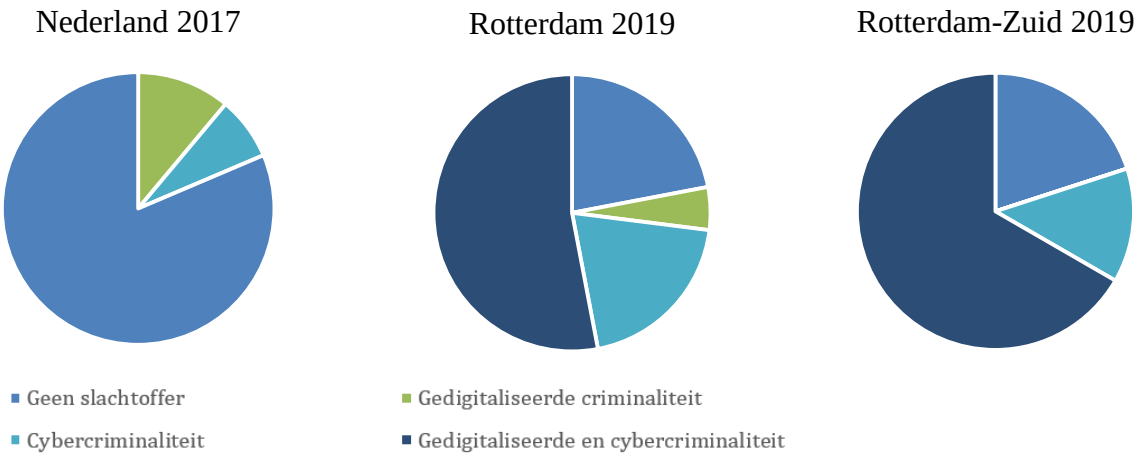
Het wetenschappelijk segment toetst achttien hypothesen aan de hand van een enquête die is uitgezet onder jongeren van 14 tot 23 jaar die woonachtig zijn in Rotterdam-Zuid (N = 161). De steekproef bevat jongeren van alle leeftijden die dit onderzoek op het oog heeft (μ = 20.54). Daarnaast bevat de steekproef meer vrouwen dan mannen (59% vrouw, 39,8% man, 1,2% anders). De meeste respondenten wonen in de omgeving van Rotterdam, 40 respondenten wonen in Rotterdam-Zuid. Tabel 3 toont de woonplaats van de respondenten.

Tabel 4. Beschrijving steekproef naar woonplaats.

	Frequentie	**Percentage**
Buiten Rotterdam	103	64.0
Andere wijken Rotterdam	18	11.2
Rotterdam, Feijenoord	8	5.0
Rotterdam, Charlois	16	9.9
Rotterdam, Ijsselmonde	16	9.9
Totaal	161	100.0

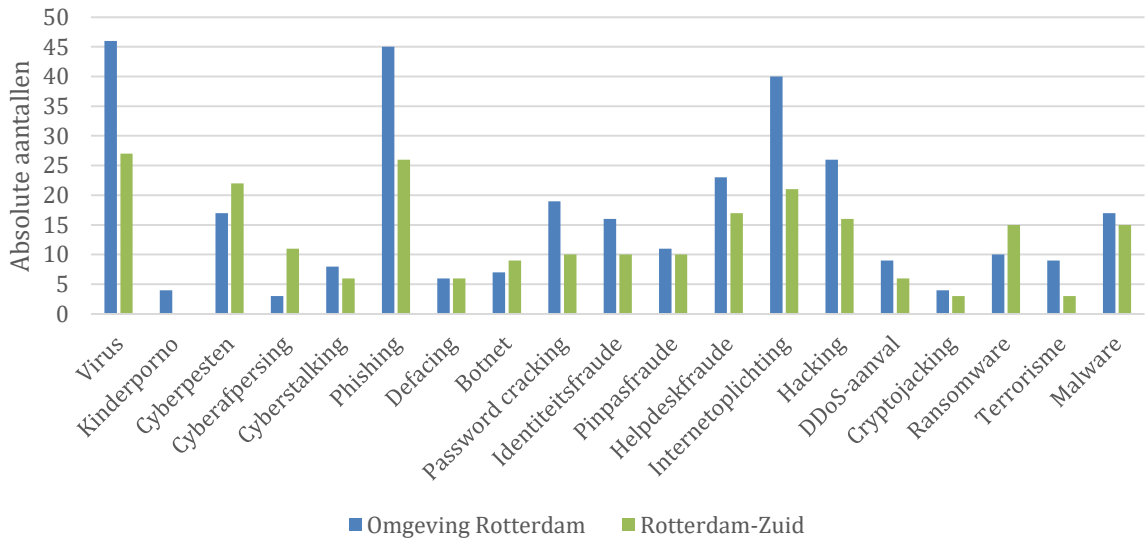
N = 161

Figuur 5. Slachtofferschap in Nederland (2017), Rotterdam en Rotterdam-Zuid (2019).

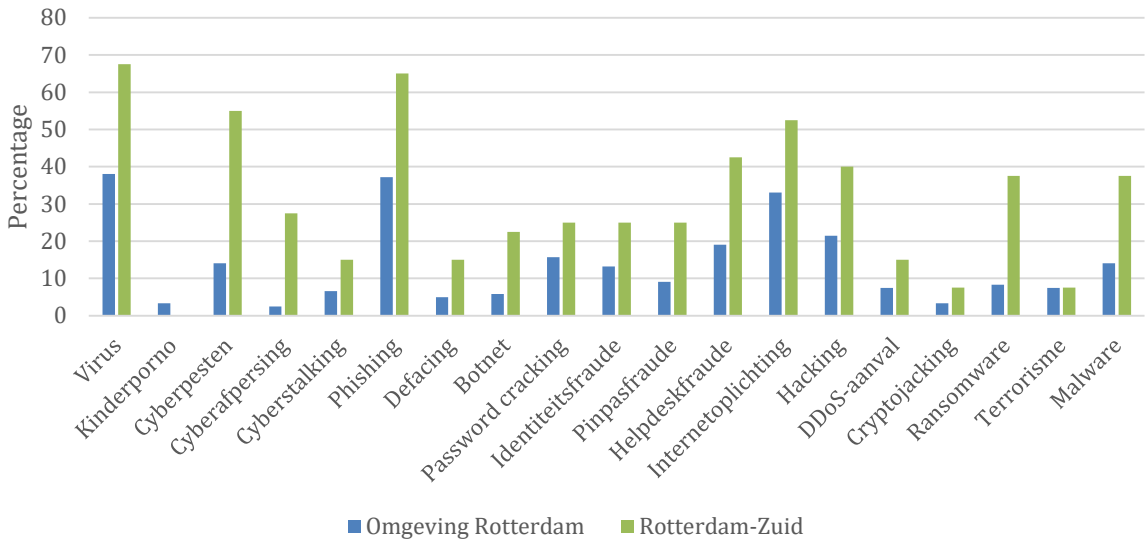


In Figuur 5 is het slachtofferschap in Nederland, Rotterdam en Rotterdam-Zuid te zien. Ongeveer 80% van de Nederlanders was geen slachtoffer van cybercriminaliteit in 2017. In Rotterdam en Rotterdam-Zuid is dat slechts iets minder dan een kwart van de inwoners. De meerderheid van de inwoners van Rotterdam (Zuid) geeft aan slachtoffer te zijn geweest van zowel gedigitaliseerde criminaliteit als cybercriminaliteit (53% in Rotterdam, 66% in Rotterdam-Zuid). Iets minder dan een kwart van de bewoners van Rotterdam geeft aan slachtoffer te zijn geweest van cybercriminaliteit en 5% geeft aan slachtoffer te zijn geweest van gedigitaliseerde criminaliteit. 11,1% van de Nederlanders gaf aan slachtoffer te zijn geweest van gedigitaliseerde criminaliteit en 7,5% gaf aan slachtoffer te zijn geweest van cybercriminaliteit.

Figuur 6a. Slachtofferschap naar type cybercriminaliteit in absolute aantallen.

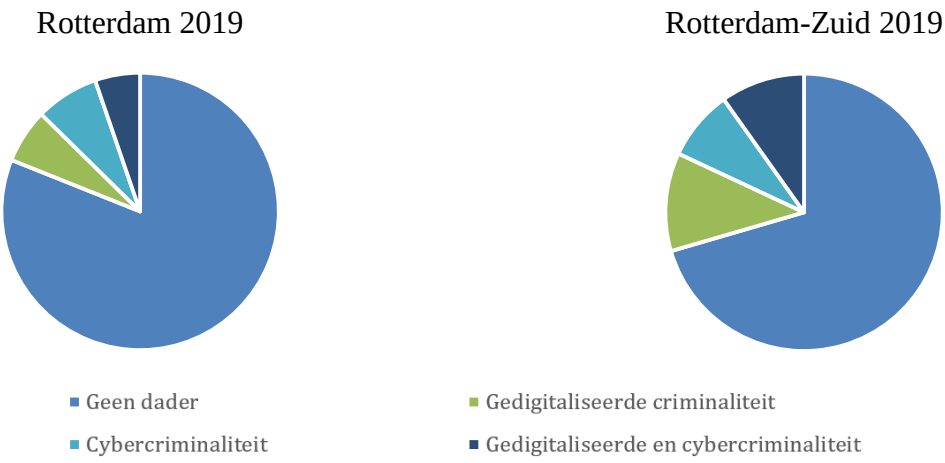


Figuur 6b. Slachtofferschap naar type cybercriminaliteit in percentages.



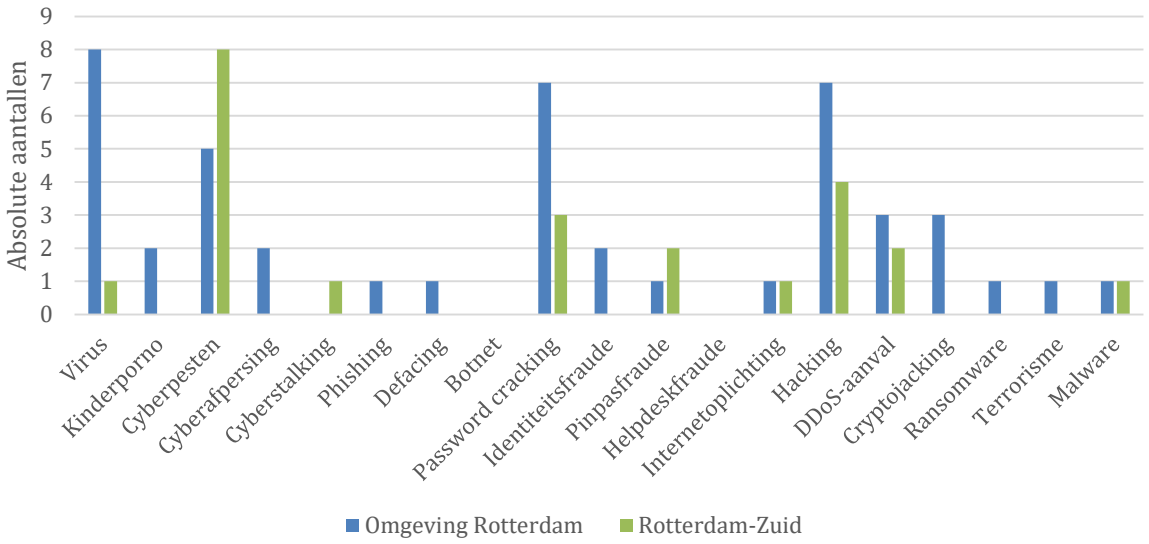
Figuur 6 laat zien van welke soorten cybercriminaliteit de respondenten aangaven slachtoffer te zijn geweest. De typen cybercriminaliteit waar aandacht aan is besteed zijn: virussen, kinderporno, cyverpesten, cyberafpersing, cyberstalking, phishing, defacing, botnet, password cracking, identiteitsfraude, pinpasfraude, helpdeskfraude, internetoplichting, hacking, DdoS-aanval, cryptojacking, ransomware, terrorisme en malware. Figuur 6a bevat de gegevens over de absolute aantallen van het slachtofferschap van de respondenten. De meest voorkomende soorten cybercriminaliteit zijn virussen, phishing, internetoplichting en hacking. Deze delicten komen meer voor buiten Rotterdam-Zuid dan in Rotterdam-Zuid. Figuur 6b bevat slachtofferschap in percentages van de steekproef, onderverdeeld in ‘Omgeving Rotterdam’ en ‘Rotterdam-Zuid’. Ook hier komen dezelfde soorten cybercriminaliteit naar voren, maar lijken deze soorten cybercriminaliteit in verhouding meer voor te komen in Rotterdam-Zuid.

Figuur 7. Daderschap in Rotterdam en Rotterdam-Zuid (2019).

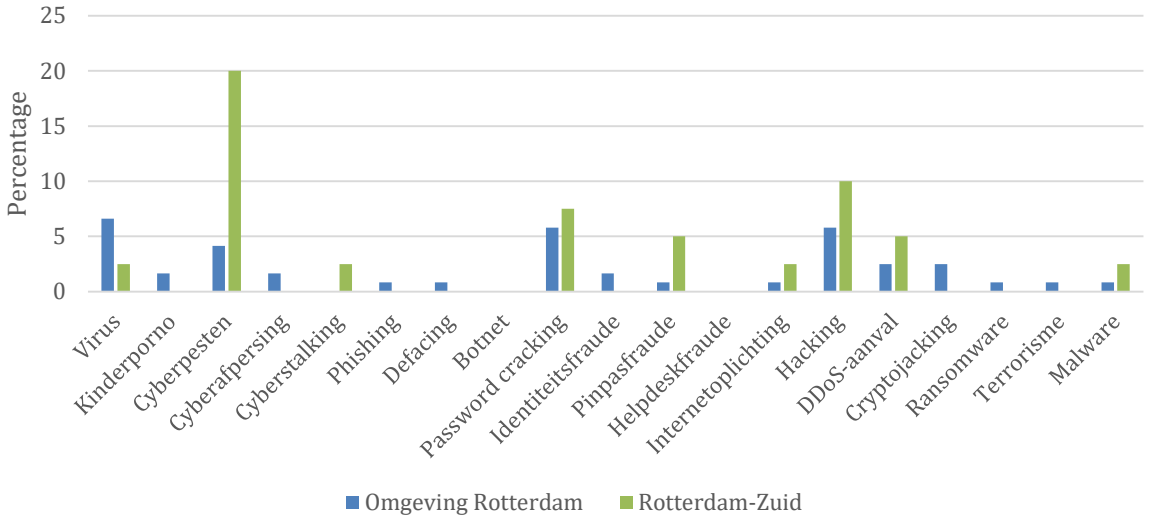


In Figuur 7 is het daderschap in Rotterdam en Rotterdam-Zuid te zien. Er wordt hier geen vergelijking gemaakt met Nederland, omdat de gegevens rondom daderschap in Nederland onbekend zijn. 80% van de Rotterdammers gaf aan nog nooit een cybermisdaad te hebben gepleegd of geprobeerd te plegen. 5% gaf aan zich wel eens schuldig te hebben gemaakt aan gedigitaliseerde criminaliteit, 6% aan cybercriminaliteit en 4% aan beide typen. Hier is wel een duidelijk verschil zichtbaar met Rotterdam-Zuid: 30% van de respondenten uit Rotterdam-Zuid geeft aan wel eens een cybermisdaad te hebben gepleegd. 12% van de respondenten heeft zich wel eens schuldig gemaakt aan gedigitaliseerde criminaliteit, 8% aan cybercriminaliteit en 10% aan beide typen.

Figuur 8a. Daderschap naar type cybercriminaliteit in absolute aantallen.



Figuur 8b. Daderschap naar type cybercriminaliteit in percentages.



Figuur 8a laat zien van welke soorten cybercriminaliteit de respondenten aangaven dader te zijn geweest. De meest voorkomende soorten cybercriminaliteit waar de respondenten zich schuldig aan hebben gemaakt zijn virussen, cyberpesten, password cracking, internetoplichting en hacking. Deze delicten komen meer voor buiten Rotterdam-Zuid dan in Rotterdam-Zuid, behalve internetoplichting en cyberpesten. Figuur 8b bevat daderschap in percentages van de steekproef, onderverdeeld in 'Omgeving Rotterdam' en 'Rotterdam-Zuid'. Ook hier komen dezelfde soorten cybercriminaliteit naar voren, maar lijken cyberpesten, password cracking en hacking in verhouding meer voor te komen in Rotterdam-Zuid.

Hierna volgen de resultaten van de meervoudige regressieanalyse. Tabel 5 en 6 tonen het regressiemodel met respectievelijk afhankelijke variabele 'Slachtofferschap' en 'Daderschap'. Tabel 7 en 8 (zie Bijlage 2) tonen de regressieanalyses met interactievariabelen met respectievelijk afhankelijke variabelen 'Slachtofferschap' en 'Daderschap'. Tabel 9 (zie Bijlage 2) toont de regressieanalyse met de variabelen die naar verwachting een mediërend verband hebben.

Tabel 5. Resultaten meervoudige regressie (slachtofferschap).

	Algeheel slachtofferschap				Slachtofferschap gedigitaliseerde criminaliteit				Slachtoffershap cybercriminaliteit			
Variabele	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**
			.176	3.286			.120	2.463			.160	3.060
Sociale kwetsbaarheid	-.039	-.353			-.508	-.363			-.030	-.406		
Impulsiviteit (tegenover zelfcontrole)	.416	.970			.075	.031			.325	1.148		
Sociale status	-	-			-	-			-	-		
Internetvaardigheden	.012	.049			.047	.425			-.030	.699		
Financiële impulsiviteit	-.186	-.470			-.111	-.595			-.012	-.046		
Sociale cohesie	.012	.044			.114	.910			-.086	-.491		
Differentiële associatie door kennissen	2.332	1.781			1.705***	2.763			.605	.699		
Differentiële associatie door vrienden	1.872	1.837			.750	1.562			1.116	1.657		
Geslacht	-.104	-.299			.050	.024			-.175	-.758		
Leeftijd	-.006	-.010			.220	.093			-.273	-.723		
Migratieachtergrond	1.595	1.924			.213	.050			1.355**	2.475		
Inkomen	.061	.151			-.048	-.254			.150	.569		
Arbeidsstatus	.293	1.116			.073	.625			.194	1.183		
Tijdsbesteding	.469 *	2.043			.128	1.187			.326*	2.154		
Opleidingsniveau	.058	.205			.025	.183			.022	.119		
Strain	-.008	-.319			-.066	-1.485			-.075	-1.266		

Noot: N=161, *p <.05, **p <.02, ***p <.01

Tabel 6. Resultaten meervoudige regressie (daderschap).

	Algeheel daderschap				Daderschap gedigitaliseerde criminaliteit				Daderschap cybercriminaliteit			
Variabele	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**
			.168	3.173			.156	2.992			.121	2.485
Sociale kwetsbaarheid	.014	.674			.036*	2.891			-.018	-.690		
Impulsiviteit (tegenover zelfcontrole)	.071	.874			.045	.931			-.012	-.111		
Sociale status	-	-							-	-		
Internetvaardigheden	.053	1.197			.030	1.131			.092	1.616		
Financiële impulsiviteit	.164*	2.242			.083	1.890			.118	1.263		
Sociale cohesie	.004	.081			.013	.424			-.055	-.854		
Differentiële associatie door kennissen	.121	.490			.052	.353			.241	.759		
Differentiële associatie door vrienden	-.085	-.443			-.056	-.482			.176	.714		
Geslacht	-.040	-.607			-.048	-1.214			-.126	-1.494		
Leeftijd	.110	1.018			.027	.421			.173	1.245		
Migratieachtergrond	.299	1.910			.173	1.837			.097	.485		
Inkomen	.033	.439			-.012	-.274			.202*	.251		
Arbeidsstatus	-.012	-.251			.001	.018			-.120*	-1.993		
Tijdsbesteding	.087*	2.017			.016	.597			.084	1.509		
Opleidingsniveau	-.157***	-2.912			-.032	-.984			-.287***	-4.182		
Strain	.051***	2.960			.042***	3.116			.034	1.605		

Noot: N=161, *p <.05, **p <.02, ***p <.01

De eerste hypothese die werd getest is de relatie tussen sociale kwetsbaarheid en daderschap van cybercriminaliteit. Uit de regressieanalyse blijkt dat deze relatie inderdaad bestaat, maar het is een zeer zwakke relatie en geldt alleen voor gedigitaliseerde criminaliteit (B = .036; $t(1) = 2.891$; p<.05). Sociale kwetsbaarheid voorspelt ook een significant deel van daderschap van cybercriminaliteit (R^2= .156; F = 2.992; p<.05). Daarmee kan Hypothese 1 worden aangenomen, met de opmerking dat dit alleen geldt voor gedigitaliseerde criminaliteit. Deze relatie bestaat echter niet tussen sociale kwetsbaarheid en slachtofferschap van cybercriminaliteit. Daarom kan Hypothese 8 worden verworpen. Dit alles betekent dat hoe sociaal kwetsbaarder een individu is, hoe waarschijnlijker dat dit individu dader wordt van gedigitaliseerde criminaliteit.

Zelfcontrole, hier getoetst als impulsiviteit, bleek een zwakke, significante positieve invloed te hebben op de relatie tussen sociale kwetsbaarheid en daderschap (B = .027; $t(1) = 2.642$; p<.001). Dat betekent dat zelfcontrole inderdaad een afzwakkende invloed heeft op de relatie tussen sociale kwetsbaarheid en daderschap, maar dat geldt wederom alleen voor gedigitaliseerde criminaliteit. Daarnaast voorspelt impulsiviteit een significant deel van deze relatie (R^2= .190; F = 4.938; p<.05). Dit betekent dat Hypothese 2 kan worden aangenomen, echter met de kanttekening dat dit alleen geldt voor gedigitaliseerde criminaliteit. Dit betekent dat impulsiviteit het daderschap van gedigitaliseerde criminaliteit als gevolg van sociale kwetsbaarheid licht afzwakt.

In het verband tussen sociale kwetsbaarheid en daderschap blijkt de variabele strain een mediërende variabele te zijn. Er is een significant verband tussen sociale kwetsbaarheid en strain (B=.468; $t(1) = 9.370$; p<.001), waarbij ook 74,4% van het verband verklaard wordt door deze variabele (F = 64.812, p<.05). Er is ook een significant verband tussen strain en daderschap (B=.051; $t(1) = 2.960$, p<.005), waarbij een klein, maar significant deel van het verband wordt verklaard (R^2= .047, F = 8.759, p<.005). Op basis van deze gegevens kan Hypothese 3 worden aangenomen. Strain wordt significant beïnvloed door opleidingsniveau (B = -.917; $t(1)$= -7.252; p<.001) en arbeidsstatus (B=-1.354; $t(1)$=-12.357; p<.001). Dit betekent: hoe sociaal kwetsbaarder een individu, hoe meer strain deze persoon ervaart, hoe waarschijnlijker het is dat dit individu dader is van cybercriminaliteit.

Het aantal kennissen van een individu dat betrokken is bij cybercriminaliteit heeft een positieve significante invloed op daderschap van cybercriminaliteit (B=1.455; $t(1) = 2.605$; p<.001). Dat betekent dat hoe meer kennissen van een individu betrokken zijn bij cybercriminaliteit, hoe vaker het individu ook betrokken raakt bij het plegen van cybercriminaliteit. Daarnaast heeft social learning ook een afzwakkende invloed op de relatie tussen sociale kwetsbaarheid en daderschap van cybercriminaliteit (B=-.0138; $t(1)$ = -.2.215; p<.05). Dat betekent dat social learning het daderschap van high-tech cybercriminaliteit als gevolg van sociale kwetsbaarheid licht afzwakt. Samen verklaren deze twee relaties 9.9% van het verband (F= 2.848, p<.05). Op basis van deze gegevens kan Hypothese 4 worden aangenomen, met de kanttekening dat dit verband alleen geldt voor high-tech cybercriminaliteit.

Er is ook een verband tussen differentiële associatie en slachtofferschap. Differentiële associatie heeft een positieve, significante invloed op slachtofferschap van gedigitaliseerde criminaliteit

(B = 1.705; $t(1) = 2.763$); p<.001). Differentiële associatie verklaart een significant deel van dit verband (R^2= .120; F = 2.463, p<.05). Hypothese 10 kan daarom worden aangenomen, met de kanttekening dat dit verband alleen geldt voor gedigitaliseerde criminaliteit. Dat betekent dat hoe meer kennissen van een individu te maken hebben met cybercriminaliteit, hoe vaker het individu slachtoffer is van gedigitaliseerde criminaliteit. Differentiële associatie wordt significant beïnvloed door arbeidsstatus (B = .036; $t(1) = 2.275$; p<.05) en wonen in Rotterdam-Zuid (B = .201; $t(1) = 3.338$, p<.001). Deze variabelen verklaren 17,6% van differentiële associatie (F= 5.610; p<.05).

Tijdsbesteding medieert de relatie tussen sociale kwetsbaarheid en slachtofferschap. Er is een negatieve, significante relatie tussen sociale kwetsbaarheid en tijdsbesteding (B = -.121; $t(1) = -2.986$; p<.001). Sociale kwetsbaarheid verklaart een significant deel van de tijdsbesteding (R^2= .049; F= 2.107; p<.05). Er is een positieve, significante relatie tussen tijdsbesteding en slachtofferschap (B = .469, $t(1) = 2.043$, p<.05). Tijdsbesteding verklaart een significant deel van slachtofferschap (R^2=.176; F= 3.286; p<.05). Dit betekent dat Hypothese 16 kan worden aangenomen. Hoe sociaal kwetsbaarder individuen zijn, hoe meer tijd zij besteden op het internet, hoe vaker ze slachtoffer zijn van cybercriminaliteit.

Tenslotte heeft migratieachtergrond een significante invloed op slachtofferschap, alleen geldig voor high-tech cybercriminaliteit (B = 1.355; $t(1) = 2.475$; p<.001). Mensen met een migratieachtergrond zijn dus vaker slachtoffer van high-tech cybercriminaliteit. Migratieachtergrond verklaart een significant deel van slachtofferschap van cybercriminaliteit (R^2= .160; F= 3.060, p<.05). Op basis van deze gegevens kan Hypothese 17 worden aangenomen. Migratieachtergrond wordt significant beïnvloed door arbeidsstatus (B = -.046; $t(1) = -2.074$; p<.05) en wonen in Rotterdam-Zuid (B = .471; $t(1) = 6.030$; p<.001). Deze variabelen samen verklaren 28,4% van de migratieachtergrond (F= 10.978, p<.05).

Hoewel de interactieverbanden de geformuleerde hypotheses niet kunnen bevestigen, is de dummyvariabele Rotterdam-Zuid in al deze verbanden wel significant. Dat betekent dat wonen in Rotterdam-Zuid een zekere invloed heeft in dat verband. Op basis hiervan kan Hypothese 18 worden aagenomen. Het is echter opmerkelijk dat alleen deze variabele daar een significant verband geeft, terwijl andere variabelen die naar verwachting ook een rol spelen, geen significante invloed hebben. Voor de overige hypothesen is geen significant verband gevonden en op basis daarvan kunnen de hypothesen worden verworpen. Tabel 7 geeft een overzicht van de hypothesen, de aanname of verwerping van de hypothesen en welk type verband er bij de hypothese hoort.

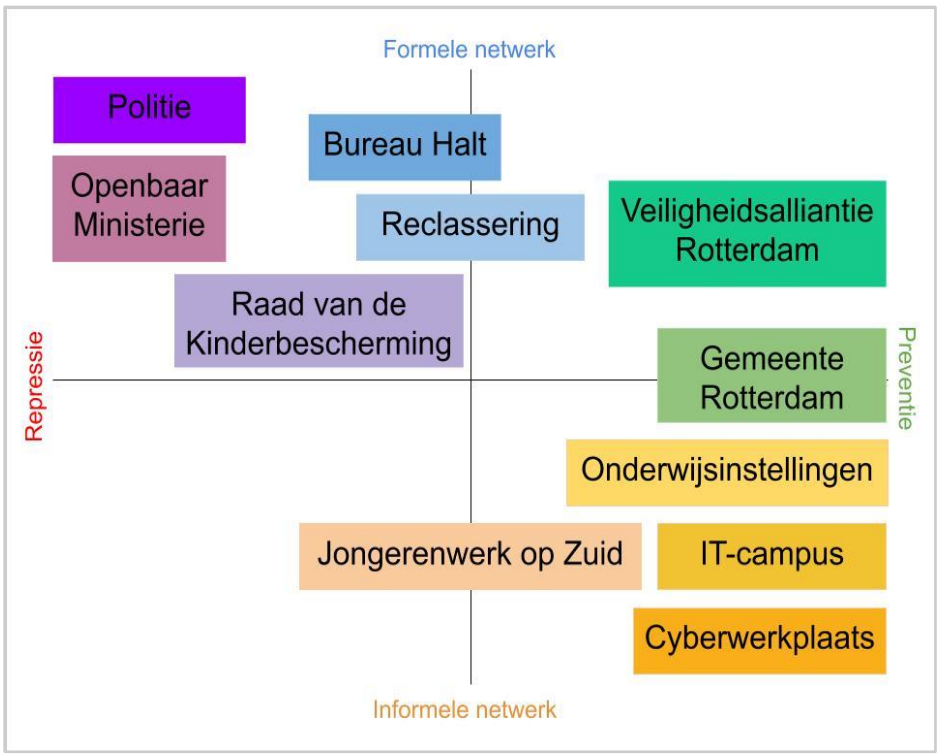
Tabel 7. Overzicht resultaten hypothesen

Concept	Hypothese	Oordeel	Type verband
Sociale kwetsbaarheid	H1: Hoe sociaal kwetsbaarder een individu, hoe vaker het individu betrokken is bij het plegen van cybercriminaliteit.	Aangenomen (gedig.crim.)	Lineair
Zelfcontrole	H2: Hoe minder zelfcontrole, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.	Aangenomen (gedig.crim.)	Moderatie
Strain	H3: Hoe meer strain individuen ervaren, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.	Aangenomen	Mediatie
Social learning	H4: Hoe meer kennissen van een individu betrokken zijn bij cybercriminaliteit, hoe vaker het individu betrokken is bij het plegen van cybercriminaliteit.	Aangenomen (cybercrimin.)	Moderatie
Sociale banden	H5: Hoe zwakker de banden met de gemeenschap, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.	Verworpen	Geen verband
Sociale status	H6: Hoe lager de sociale status, hoe vaker individuen betrokken zijn bij het plegen van cybercriminaliteit.	Verworpen	Geen verband
Gender	H7: Mannen hebben een grotere kans om slachtoffer te worden van cybercriminaliteit dan vrouwen.	Verworpen	Geen verband
Sociale kwetsbaarheid	H8: Hoe sociaal kwetsbaarder een individu, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.	Verworpen	Geen verband
Leeftijd	H9: Hoe jonger een individu, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.	Verworpen	Geen verband
Differentiële associatie	H10: Hoe meer kennissen van een individu betrokken zijn bij cybercriminaliteit, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.	Aangenomen (gedig.crim.)	Lineair
Opleidingsniveau	H11: Hoe lager het opleidingsniveau, hoe groter de kans om slachtoffer te worden van gedigitaliseerde criminaliteit.	Verworpen	Geen verband
Werkstatus	H12: Hoe lager de werkstatus, hoe groter de kans om slachtoffer te worden van gedigitaliseerde criminaliteit.	Verworpen	Geen verband
Rijkdom	H13: Hoe rijker een individu is, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.	Verworpen	Geen verband
Financiële impulsiviteit	H14: Hoe financieel impulsiever mensen zijn, hoe banger ze zijn om slachtoffer te worden van cybercriminaliteit.	Verworpen	Geen verband
Vaardigheden	H15: Hoe minder computervaardigheden een individu bezit, hoe groter de kans voor dat individu om slachtoffer te worden van cybercriminaliteit.	Verworpen	Geen verband
Tijdsbesteding	H16: Hoe meer tijd mensen besteden op het internet, hoe groter de kans om slachtoffer te worden van cybercriminaliteit.	Aangenomen	Mediatie
Migratie-achtergrond	H17: Mensen met een migratieachtergrond hebben een grotere kans om slachtoffer te worden van cybercriminaliteit dan mensen zonder migratieachtergrond.	Aangenomen (cybercrim.)	Lineair
Woonplaats	H18: Inwoners van Rotterdam-Zuid hebben een grotere kans om te maken te krijgen met cybercriminaliteit dan mensen die niet in Rotterdam-Zuid wonen.	Aangenomen	Lineair

4.2 Beleidssegment

Allereerst is er een overzicht gemaakt van de betrokken partijen en hoe zij zich tot elkaar verhouden. Het overzicht in Figuur 9 is gebaseerd op twee factoren: het type beleid waar een partij zich vooral op richt en de formaliteit van de organisatie. Er zijn tien gesprekken geweest met zeven van deze partijen, namelijk Politie Rotterdam, Openbaar Ministerie, Reclassering, Veiligheidsalliantie Rotterdam, Gemeente Rotterdam, Jongerenwerk op Zuid en Cyberwerkplaats. De positie van de overige partijen bleek uit de gehouden gesprekken.

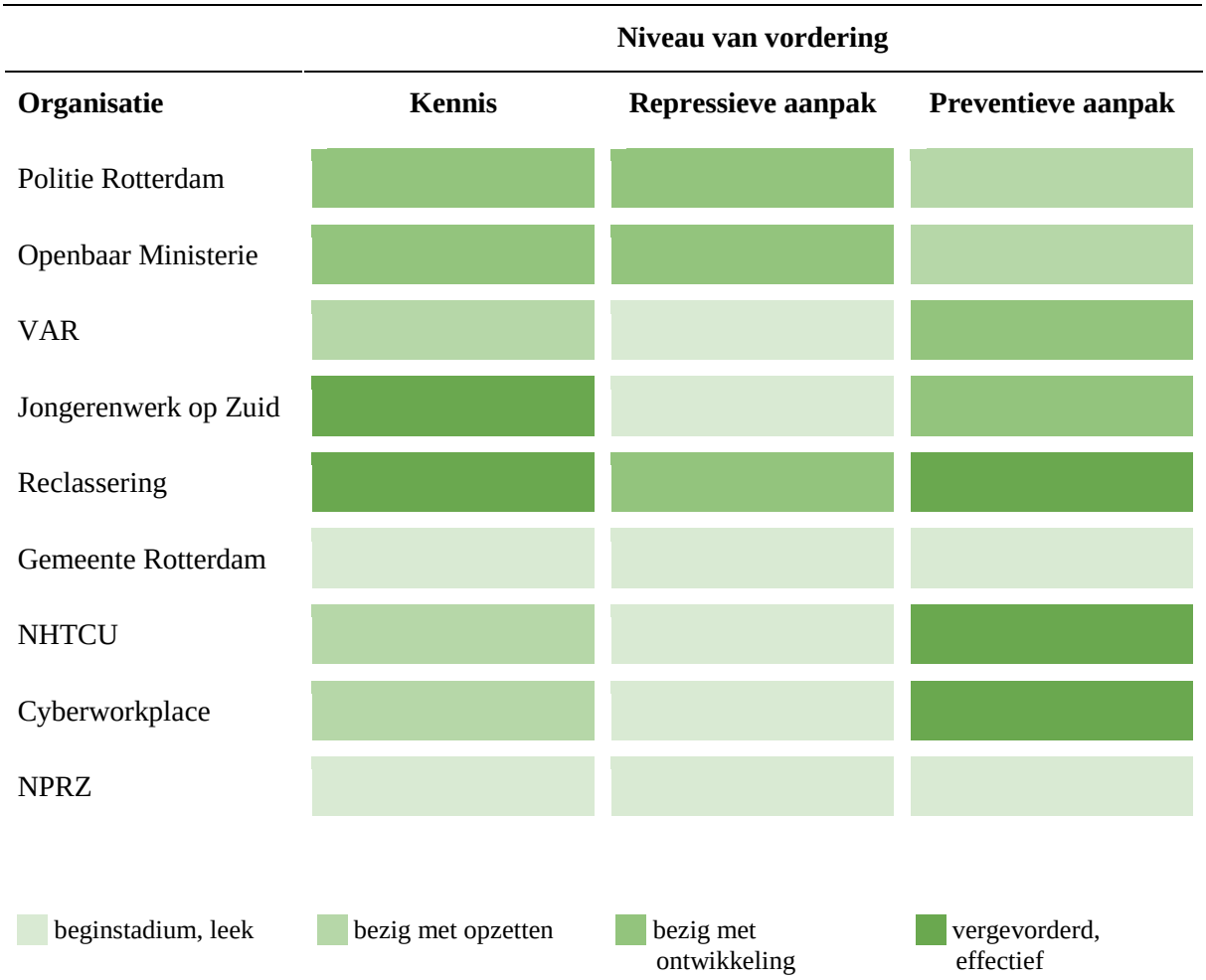
Figuur 9. Overzicht betrokken partijen



Niet alleen variëren deze partijen in aanpak en formaliteit, ze verschillen ook in niveau van kennis en vordering van de preventieve en repressieve aanpak (zie Figuur 10). Dit onderscheid is gemaakt omdat sommige partijen zowel aandacht besteden aan preventie als repressie. De donkerte groen geeft aan in hoeverre de partijen gevorderd zijn in kennis of aanpak.

Het beleidssegment behandelt eerst de mate van kennis onder de betrokken partijen. In dit deel wordt er vooral ingegaan op het vóórkomen van cybercriminaliteit, de verklaringen voor cybercriminaliteit in Rotterdam-Zuid en de urgentie die partijen voelen om daadwerkelijk iets aan cybercriminaliteit in Rotterdam te gaan doen. Daarna volgt een sectie over het daadwerkelijke beleid. Hier zullen vooral het huidige beleid, de knelpunten en het toekomstige beleid behandeld worden. Tenslotte komt de behoefte naar kennis en samenwerking van de partijen naar voren, wat samengevat kan worden als de behoefte aan een Cyber Cirkel Coalitie.

Figuur 10. Overzicht vordering kennis en aanpak onder betrokken partijen



4.2.1 Cybercriminaliteit als het nieuwe fietsendiefstal

Het inzicht in het vóórkomen van cybercriminaliteit is vooral aanwezig bij de politie en het Openbaar Ministerie. De aangiften komen binnen bij de politie en zij hebben daardoor zicht op welke cybermisdaden vooral voorkomen en hoe vaak burgers slachtoffer worden van cybercriminaliteit. Vervolgens achterhalen politie en OM de modus operandi van de dader bij de opsporing. Ook de Reclassering wordt hierbij betrokken, omdat de Reclassering zorg draagt voor terugkeer in de maatschappij van verdachten nadat ze te maken hebben gehad met het strafrecht.

De kennis die er op dit moment over cybercriminaliteit is, is erg beperkt. Een reden hiervoor is dat het aantal aangiften erg laag is. Ondanks het beperkte aantal aangiften krijgen de politie en het OM steeds meer zaken rond cybercriminaliteit binnen. Naar aanleiding van deze zaken stellen deze partijen een daderprofiel op: jongeren met goede technische vaardigheden die financieel gewin voor ogen hebben en jongeren die een IT-opleiding volgen op mbo- of hbo-niveau en met hun kersverse vaardigheden de mogelijkheden van het internet aan het ontdekken zijn. Dit is een interessante bevinding van de betrokken partijen, omdat uit de literatuur en het wetenschappelijk segment blijkt dat er een negatieve relatie is tussen opleidingsniveau en daderschap, wat betekent dat laagopgeleiden vaker

dader zijn van cybercriminaliteit dan hoogopgeleiden, terwijl volgens de betrokken partijen ook hoger opgeleiden steeds vaker dader zijn. De betrokkenheid van IT'ers bij cybercriminaliteit wordt vooral veroorzaakt door de technologische ontwikkeling van de huidige jeugd en de zwakke beveiliging van slachtoffers. Daarnaast biedt het internet nogal wat mogelijkheden voor het plegen van cybercriminaliteit: een lage pakkans, anonimiteit, onduidelijke regels, weinig sociale controle en het ontbreken van een direct slachtoffer. Jongeren proberen ook wel eens wat op de computer omdat ze het leuk vinden of eens willen proberen: "dat het soms onschuldig is…kijken wat ik allemaal kan en dan per ongeluk in een keer, oh, oké, dit is wel heel erg leuk. Maar dat ook duidelijk wordt…dat dat ook gewoon strafbaar is" (Directeur Veiligheidsalliantie Rotterdam). Het gaat hier vaak om intelligente mbo-studenten die goed wegwijs zijn in de IT en betrokken zijn bij cybercriminaliteit. IT'ers zijn vaak intrinsiek gemotiveerd omdat ze zich willen bewijzen door bijvoorbeeld een computervredebreuk op een juiste manier uit te voeren, terwijl anderen minder gefocust zijn op de technische kant, maar uit zijn op financieel gewin.

Ook het feit dat het steeds makkelijker wordt om cybercriminaliteit te plegen zonder dat een dader specifieke technologische kennis heeft, verwijdert een barrière tot het plegen van cybercriminaliteit. Het gaat dan vooral om gedigitaliseerde criminaliteit. Tegenwoordig zien politie en jongerenwerkers een verschuiving in cybercriminaliteit. Er ontstaan hybride cybercriminelen die niet noodzakelijk zelf goed overweg kunnen met digitale middelen, maar simpelweg een pakketje kopen, genaamd plug-and-play malware, waarmee ze gemakkelijk een cyberdelict kunnen plegen. Bovendien zijn sommige jongeren ook bereid om geweld te gebruiken.

> "En je ziet dat jongeren begrijpen dat dat eigenlijk best wel een chille manier is ten opzichte van op straat iemand met een pistool beroven, want je hoeft de deur niet uit, de pakkans is veel lager, je hoeft iemand niet aan te kijken als je het doet…Maar dat zijn wel de jongens die op straat wel bereid zijn tot het gebruiken van geweld, dus je krijgt nu, je wordt niet bedreigd op internet, of afgelegd door een nerd, maar door iemand die ook nog eens bereid is om geweld te gebruiken, dus je hebt een soort van best wel gevaarlijke nieuwe vorm van cybercriminelen die meer angst inboezem[t] dan het klassieke voorbeeld." (Criminoloog Jongerenwerk op Zuid)

Op deze manier komen jongeren niet alleen gemakkelijker in aanraking met cybercriminaliteit, ook raakt digitale ondermijning steeds meer verweven met traditionele ondermijning. Bij traditionele ondermijning is er sprake van legale structuren die verweven raken met illegale structuren, bijvoorbeeld banken die geld van drugshandelaren witwassen. Dat gebeurt ook steeds meer op digitaal gebied. Volgens het 'WODC rapport digitalisering georganiseerde misdaad' (p.15) faciliteren onder andere financiële dienstverleners cybercriminaliteit. Websites worden vaak gebruikt om bijvoorbeeld achter reclames verborgen software te plaatsen of illegale handelingen af te schermen door dekmantalondernemingen.

De meeste betrokken partijen verklaren het vóórkomen van cybercriminaliteit aan de hand van sociale achterstand die samenhangt met de hoge bevolkingsdichtheid en de migratieachtergrond van veel jongeren van Rotterdam-Zuid. Bovendien gaat het vaak om mensen die een laag inkomen hebben, waardoor snel geld verdienen een doel op zich is en bijvoorbeeld het uitlenen van een bankpasje een effectieve manier is om dat doel te bereiken. Belangrijker nog is dat jongeren geld gebruiken om hun straatstatus aan te ontlenen. Hoewel het verlangen naar geld in de maatschappij an sich ook aanwezig is, lijkt de focus op geld er onder jongeren nog sterker te zijn. Een mogelijke verklaring daarvoor is dat jongeren een drang hebben om mee te tellen.

> "Zij gaan nooit een betere baan krijgen dan jij en ik, waarschijnlijk. Maar ze kunnen wel meer geld verdienen door…het op een verkeerde manier te verdienen. En als je dan op een vrij gemakkelijke manier zonder daar heel veel last van te ervaren op straat of op social media, maar in ieder geval via die straatcultuur je geld kunt verdienen, ja, dan is het best moeilijk om die gasten te overtuigen…[G]a ze maar eens uitleggen dat wat zij doen, waar ze heel gemakkelijk geld mee verdienen, dat ze dat eigenlijk niet zouden moeten doen en dat ze eigenlijk een baan moeten aannemen bij de McDonalds of de Albert Heijn, want…in heel veel gevallen is dat hun alternatief. " (Criminoloog Jongerenwerk op Zuid).

Geld is één van de doelen die jongeren gemeenschappelijk met de samenleving voor ogen stellen. Jongeren uit Rotterdam-Zuid hebben echter niet dezelfde middelen als jongeren uit andere gebieden of volwassenen uit de bredere samenleving wel hebben om hun doelen te bereiken. Zij zien ook het gebrek aan mogelijkheden als jongere uit Rotterdam-Zuid. Als gevolg van de spanning die zij hierdoor ervaren vinden ze alternatieve manieren om geld te verdienen die vaak niet legaal zijn om daarmee hun doelen te bereiken. Geld verdienen door middel van illegale activiteiten draagt bij aan de status van jongeren binnen de straatcultuur. Dat is belangrijk voor hen omdat de straatcultuur vaak een manier is om geaccepteerd te worden en vervanging te krijgen voor liefde die ontbreekt in gebroken gezinnen waar de jongeren vaak uit afkomstig zijn. Deze straatcultuur en de manieren waarop jongeren geacht worden zich te gedragen worden extra aangemoedigd door groepsdruk. Deze groepsdruk stimuleert jongeren om een bepaalde status te bereiken en macht te verwerven.

> "Iedereen wil op zijn eigen manier een klein beetje belangrijk zijn…En ik heb het gevoel dat dat met jongeren ook een beetje is. Wij kunnen van die straatcultuur vinden wat wij willen… Maar voor die jongeren is dat hun realiteit, hun werkelijkheid en heel belangrijk voor hun persoonlijke identiteit." (Criminoloog Jongerenwerk op Zuid)

Binnen de straatcultuur is dus heel belangrijk om respect te verdienen en dat gebeurt door het gebruik van geweld, het plegen van criminaliteit, een afkeer hebben van de samenleving, 'conspicuous

consumption' en geld verdienen. Jongeren die in de straatcultuur leven hebben dus een intrinsieke motivatie om (cyber-)criminaliteit te plegen, namelijk om status en respect te verwerven, waardoor ze het gevoel hebben dat ze waardevol zijn.

Bovendien komen jongeren binnen die straatcultuur in contact met anderen die criminaliteit heel normaal vinden, waardoor jongeren normen en waarden van crimineel gedrag worden aangeleerd. Niet alleen horen jongeren regelmatig pro-delinquente opvattingen, ze krijgen ook de middelen aangereikt om bepaalde misdaden te plegen. De kans dat die jongeren criminaliteit gaan plegen is dan ook veel groter dan jongeren die niet in deze omstandigheden belanden. Deze invloed van differentiële associatie blijkt ook uit het wetenschappelijk segment. Deelname aan cybercriminaliteit hangt overigens vooral samen met persoonlijkheid en persoonlijke omstandigheden. De fysieke omgeving en de buurt waarin jongeren wonen lijkt een sterke invloed te hebben op het gedrag van jongeren. Sociale media spelen hier ook een belangrijke rol: jongeren delen heel gemakkelijk hun persoonlijke informatie via sociale media en staan er amper bij stil in hoeverre dit invloed kan hebben op de rest van hun leven. Jongeren gebruiken sociale media ook om te laten zien dat ze bij de straatcultuur horen en dus in staat zijn om criminaliteit te plegen.

Slachtofferschap wordt vooral verklaard vanuit veelvuldig internetgebruik, waar vooral sprake van is bij jongeren. Uit onderzoeken van de betrokken organisaties is gebleken dat mensen die veel gebruikmaken van internet eerder slachtoffer zijn van cybercriminaliteit dan mensen die minder gebruikmaken van internet. Ook dit komt overeen met de resultaten van het wetenschappelijk segment. Omdat jongeren over het algemeen meer gebruikmaken van internet, vormen zij een risicogroep. Het is daarom belangrijk om rekening te houden met het gedrag van jongeren in het ontwikkelen van beleid rondom cybercriminaliteit.

4.2.2 Cybercriminaliteitsbeleid in de kinderschoenen

Het huidige beleid van veel overheidsorganisaties is vooral gericht op het voorkómen van slachtofferschap. Het doel van deze strategie is om het bewustzijn en de weerbaarheid van burgers en ondernemers te vergroten. Vooral de organisaties die niet direct betrokken zijn bij het strafrechtelijk proces houden zich bezig met preventie. Zo hebben Gemeente Rotterdam en Veiligheidsalliantie Rotterdam campagnes ontwikkeld die burgers en ondernemers helpen om allereerst het bewustzijn van cybercriminaliteit te vergroten. Daarnaast geven overheidsorganisaties praktische tips om burgers en ondernemers weerbaarder te maken tegen cybercriminaliteit. Deze tips bestaan vooral uit advies voor de beveiliging van computers en data. Veiligheidsalliantie Rotterdam heeft een 'Checklist digitaal veilig' ontwikkeld die gemeenten kunnen verspreiden binnen hun eigen gemeente via bijvoorbeeld voorlichtingsbijeenkomsten. Deze checklist bevat vooral concrete, praktische tips voor privaat internetgebruik, zoals het installeren van een antivirusprogramma, het gebruik van sterke wachtwoorden, het installeren van software-updates en alleen verbinding maken met vertrouwde en geen openbare wifinetwerken.

Politie Eenheid Rotterdam houdt zich meer bezig met de opsporing en vervolging van daders. Traditioneel gezien komt er een aangifte binnen bij een eenheid van de politie van één of meerdere slachtoffers in het gebied van die eenheid en bevindt de dader zich ook in dat gebied. Bij cybercriminaliteit is dat niet zo vanzelfsprekend. Een dader die zich in Groningen bevindt kan slachtoffers maken in heel Nederland, zelfs in heel de wereld. Stel dat dat inderdaad gebeurt en er komen aangiften bij elke eenheid binnen, zou elke eenheid in zijn eigen gebied de dader proberen op te sporen. Dat heeft geen zin bij cybercriminaliteit, omdat alle eenheden dan één dader zoeken die zich op één plek bevindt, wat zonde is van de capaciteit en de moeite. Daarom heeft de politie een systeem ontwikkeld waarbij aangiftes 'gescoord' worden op basis van het type cybercriminaliteit en modus operandi. Door het scoren van de aangiftes kan de politie zien in welke eenheden vergelijkbare aangiftes worden gedaan en aan de hand daarvan wordt beslist welke eenheid of stuurgroep de zaak gaat oppakken.

De landelijke overheid schenkt aandacht aan het voorkomen van daderschap. De Nationale High Tech Crime Unit (NHTCU) heeft een interventie voor beginnende hackers ontwikkeld die kan dienen als voorwaarde van een straf voor het plegen van cybercriminaliteit. De interventie, genaamd HACKRIGHT, is vooral gericht op secundaire preventie: "recidive-preventie gericht op jongeren die voor het eerst kenmerken vertonen van cybercrimineel gedrag" (HACKRIGHT projectplan, p.12). HACKRIGHT beoogt jonge first offenders te helpen met het ontwikkelen van een toekomstperspectief. De invulling van de interventie kan variëren van een gesprek tot een training tot een tijdelijke baan waarbij de jongere leert hoe hij of zij zijn of haar talenten ten goede kan inzetten, bijvoorbeeld als ethisch hacker.

Ook wordt gekeken naar een maatwerkoplossing voor first offenders. In het voorjaar van 2019 heeft er een 'klapweekend' plaatsgevonden, wat zich vooral richtte op katvangers: mensen die hun bankrekening beschikbaar stellen. Op basis van de aangiften die tegen katvangers worden gedaan, stelt het Landelijk Meldpunt Internetoplichting (LMIO) een lijst op met hun namen. Bij de analyse van deze lijst werd een geografische piek in Rotterdam-Zuid zichtbaar, wat zou indiceren dat veel katvangers zich in Rotterdam-Zuid bevinden. Een aantal jongeren dat op de LMIO-lijst staat en in Rotterdam-Zuid woont werd tijdens het klapweekend opgepakt en verhoord. Na hun verhoor bij de politie spraken ze met de betrokken Officier van Justitie en kregen ze direct hun straf te horen. Het is mogelijk om op deze manier te werk te gaan, omdat er alvorens dit weekend uitgebreid financieel onderzoek is gedaan naar de bankrekeningen van de betreffende jongeren, zodat eventuele verweren op de beschuldigingen direct kunnen worden verworpen met behulp van bewijsmateriaal. Op deze manier zit er minder tijd tussen de aanhouding en de straf, wat naar verwachting resulteert in een effectievere aanpak. Het is vooral de bedoeling dat de jongeren niet nog eens in hetzelfde schuitje terecht komen, maar leren van de situatie waar ze in zijn beland. Daarom wordt er vaak in samenwerking met de Reclassering voor gezorgd dat een onderdeel van de straf kan zijn dat katvangers een presentatie geven over wat zij hebben gedaan en welke gevolgen dat heeft. Ook Jongerenwerk op Zuid biedt ook de mogelijkheid om online

aan een gedeelte van de straf te voldoen, aangezien dat vaak het werkveld is van veel first offenders. De achterliggende gedachte is dat jongeren veel meer leren van op maat gemaakte straffen dan een reguliere taakstraf die bestaat uit afval prikken langs de weg. Alle betrokken partijen vinden het klapweekend een erg effectieve aanpak.

Betrokken partijen noemen drie typen knelpunten waar zij tegenaan lopen bij beleid tegen cybercriminaliteit: de aard van cybercriminaliteit, het gebrek aan kennis over cybercriminaliteit en het feit dat de werkwijzen van organisaties nog niet toegespitst zijn op cybercriminaliteit. De aard van cybercriminaliteit heeft vooral betrekking op de permanente nieuwigheid vanwege de snelle ontwikkeling van modus operandi, de grote schaal waarop cybercriminaliteit plaatsvindt en het feit dat er in de ondermijnende criminaliteit ook een verschuiving plaatsvindt naar de digitale wereld. Niet alleen wordt het hierdoor moeilijk om cybercriminaliteit an sich aan te pakken, het is ook onduidelijk wie welke zaken op moet pakken. “We hebben heel vaak gedacht dat er een staat achter zat en dan was het een jongen van vijftien die dat deed vanaf z’n zolderkamertje.” (Beleidsadviseur National High Tech Crime Unit). Op basis van dit vermoeden wordt er dan samengewerkt met staten, terwijl de zaak opgepakt had kunnen worden door een binnenlands politieteam. Ook worden voor het plegen van cybercriminaliteit steeds vaker kant-en-klare pakketjes gebruikt die op zichzelf niet illegaal zijn, maar wel vaak voor illegale handelingen worden gebruikt. Dit geeft juridische moeilijkheden, omdat het middel op zich niet illegaal is, waardoor het ingewikkeld wordt om dit soort illegale handelingen te voorkomen. Ook de ontwikkeling van internetbankieren vergemakkelijkt bankverkeer tussen jongeren, niet alleen op legaal terrein, maar ook op illegaal terrein. De grens tussen legaal en illegaal is daarom vaak vaag. Bovendien is de cyberwereld nog zo ongereguleerd dat het niet duidelijk is wat wel en niet kan en er ook geen sociale controle is. Deze onduidelijkheden zorgen er vaak voor dat cybercriminaliteit als onderwerp naar achteren wordt geschoven en beleidsmakers eerst aandacht besteden aan onderwerpen die concreter zijn vormgegeven.

Het tweede knelpunt waar bijna alle betrokken partijen mee worstelen is dat het onbekend is in welke mate en in welke vormen cybercriminaliteit voorkomt. Er zijn nog veel onbeantwoorde vragen. Natuurlijk weten de politie en het OM wel iets over cybercriminaliteit aan de hand van de zaken die zij behandelen, maar er is geen algemeen beeld van cybercriminaliteit. Het gevolg daarvan is dat partijen er moeite mee hebben om passend en effectief beleid te maken. Een ander probleem waar partijen tegenaan lopen is dat de ontwikkelingen op technologisch gebied erg snel verlopen, waardoor partijen aan de ene kant niet kunnen wachten op het ontwikkelen van een plan om een bepaalde vorm van cybercriminaliteit aan te pakken, maar aan de andere kant ook niet per direct een effectieve aanpak hebben die het probleem onmiddellijk uitroeit.

> “het vervelende is gewoon, met cybercrime:…je loopt altijd achter de feiten aan. Goed, ja, je kan ook niet niks doen, en dat is een beetje het hele probleem met dit…Ja, we kunnen gewoon niet heel gericht dat doen. Ja, moet je dan niks doen? Ik denk het niet.” (Beleidsadviseur Gemeente Rotterdam)

Bovenstaand citaat geeft aan hoe onzeker de ontwikkelingen in beleid zijn rondom cybercriminaliteit. Bovendien wordt de invloed van cybercriminaliteit ook steeds groter. De samenleving wordt steeds digitaler, door onder andere de infrastructuur en de haven die volledig door het internet worden bestuurd. Deze ontwikkelingen maken de huidige maatschappij wel steeds kwetsbaarder voor de invloed van cybercriminaliteit. Deze kwetsbaarheid en het gebrek aan kennis maken het ontwikkelen van kennis en het aan de hand daarvan ontwikkelen van beleid erg urgent. Het gebrek aan kennis wordt onder andere veroorzaakt door een zeer beperkt bewustzijn van zowel publieke organisaties en private organisaties als burgers. Deze drie actoren realiseren zich allemaal niet welke invloed cybercriminaliteit kan hebben. Daarbij is hun risicoperceptie erg laag omdat ze niet beseffen welk risico ze lopen.

> “Je ziet dat er iets raars is met risicoperceptie, mensen hebben het idee, het overkomt mij toch niet, ik ben toch geen doelwit, ik klik niet op een phishing-mail, ik vind het irritant als ik moeilijke wachtwoorden moet gebruiken, want die onthoud ik niet, ik vind tweefactor-authenticatie ook irritant want dat is veel moeite...Enerzijds is er iets met die risicoperceptie, die klopt niet, en anderzijds is het ook een stukje luiheid...En ook wel een stukje, bij een bepaalde groep, onwetendheid… Wat moet ik dan eigenlijk doen?” (Beleidsadviseur Gemeente Rotterdam)

Het feit dat het bewustzijn en de risicoperceptie van mensen laag is draagt eraan bij dat het moeilijk is om te meten in hoeverre cybercriminaliteit voorkomt. Door een beperkt bewustzijn hebben mensen het soms niet door als ze slachtoffer worden van cybercriminaliteit. Sociale media spelen ook een belangrijke rol bij het bewustzijn van slachtoffers, omdat slachtoffers zich vaak niet realiseren dat de gegevens die zij van zichzelf delen misbruikt kunnen worden, wat een vervelende naslag kan hebben. Bovendien onderschatten de daders de schade die ze bij anderen veroorzaken. Een andere factor die het moeilijk maakt om een duidelijk beeld te krijgen van cybercriminaliteit is de lage aangiftebereidheid. Politiestatistieken worden vaak gebruikt als leidraad voor het maken van lokaal beleid, maar het feit dat deze statistieken incompleet zijn op het gebied van cybercriminaliteit, maakt het vrijwel onmogelijk om passend cybercriminaliteitsbeleid te maken. De lage aangiftebereidheid komt voort uit schaamte, het gevoel dat het te veel moeite is om aangifte te doen voor de hoogte van de schade die het slachtoffer heeft ondervonden of wantrouwen in het vermogen van de politie. Ondernemers of grotere organisaties zijn vaak bang voor imagoschade, want als bekend wordt dat een bedrijf slachtoffer is geworden van cybercriminaliteit, daalt het vertrouwen in dat bedrijf en zal de klandizie onvermijdelijk afnemen.

Een derde knelpunt is dat de werkwijze van organisaties nog niet is aangepast op cybercriminaliteit. Ten eerste zijn de verbalisanten die de aangiftes opnemen leken op het gebied van cybercriminaliteit, waardoor ze vaak niet weten wat ze precies moeten vragen en soms zelfs het gevoel hebben dat de politie niets met deze aangifte kan en het slachtoffer daarom wegsturen. Dat leidt tot incomplete aangiftes of tot een genegeerd slachtoffer, beide resulterend in een tekort aan kennis. Ook het OM gaat nog op traditionele wijze om met cybermisdaden, door bijvoorbeeld straffen op te leggen die eigenlijk niet passen bij het gepleegde delict. De maatschappij ziet cybercriminaliteit nog vooral als iets wat de strafrechtketen aan moet pakken en waar de politie dus verantwoordelijk voor is. Als gevolg hiervan wordt gedacht in een aanpak voor de korte termijn in plaats van meer effectieve langetermijnoplossingen. Om cybercriminaliteit te voorkomen is de politie echter ook bezig om met private partijen samen te werken aan preventie. Dat gaat echter wel ten koste van de capaciteit van de politie, waardoor sommige individuele zaken niet opgepakt kunnen worden.

> "hoezee, we hebben vier mensen aangehouden, kost ons heel veel capaciteit en dan, we doen zoveel cybercrime, is ook goed voor de cijfers, stukje in de krant en iedereen weer blij. Terwijl je misschien moet zeggen: nee, we gaan die vier zaken niet doen. En dan gaan we dus tegen de burgers zeggen: ja, we hebben uw zaak niet opgepakt, maar ondertussen hebben we wel met de ABN Amro…gepraat en die hebben ervoor gezorgd dat het helemaal niet meer gebeurt. Dus ik vind het vervelend voor u...Dat zou eigenlijk beter zijn. Maar wat is dan de uitkomst? Dat is: de politie heeft niks aan die driehonderd aangiftes gedaan, want die waren natuurlijk inmiddels al wat opgelopen, en ja, waarom hebben jullie niks gedaan? Waarom hebben wij niks gedaan? We hebben heel veel gedaan, want het komt nu niet meer voor…Zo kijken we natuurlijk niet." (Projectleider Cyberintelligence Politie Rotterdam)

De politie heeft dan weliswaar de taak om daders op te sporen en te straffen, maar ziet ook dat het van een grotere waarde zou zijn om recidive en het plaatsvinden van een cybermisdaad te voorkomen. Dat gebeurt onder andere in samenwerking met banken, zoals weergegeven in het citaat hierboven. Om recidive te voorkomen en jonge first offenders eigenlijk te helpen, worden er in samenwerking met betrokken partijen straffen op maat gemaakt. Dat wordt echter niet altijd geaccepteerd door de maatschappij, omdat de publieke opinie is dat daders gestraft moeten worden en niet afgedaan moeten worden met een presentatie op een school om vervolgens weer vrij rond te lopen.

Deze ontwikkelingen staan nog in de kinderschoenen. De strafrechtketen probeert al veel meer samen te werken met andere partijen, maar nog lang niet alle overheidsorganisaties die te maken hebben met cybercriminaliteit zijn ook al daadwerkelijke acties aan het uitvoeren. Dat is ook een kwestie van prioriteiten stellen. Vooral bij gemeenten is dat een knelpunt. De gemeente heeft eigenlijk nog te weinig informatie over cybercriminaliteit en weet daardoor eigenlijk niet goed wat te doen aan cybercriminaliteit. "Maar bij de meeste gemeenten is mijn algemene gevoel van, die zijn allemaal nog

op zoek van, goh, we moeten er iets mee, maar we hebben eigenlijk geen idee wat." (Directeur Veiligheidsalliantie Rotterdam). Als gevolg hiervan wordt er veel nagedacht over beleid, maar weinig concrete actie ondernomen. Dat heeft niet alleen gevolgen voor preventie, maar ook voor de aanpak van de consequenties die een cyberaanval heeft.

> "als er een grote brand is, dan weet iedereen van, hé, nou, dit is allemaal wat je kan doen. Maar bij een digitale verstoring, dan eh… weten we dat allemaal gewoon nog niet zo goed. [T]wee jaar geleden was die grote hack van die containerterminal op de Maasvlakte. Ja, toen was ook een beetje de vraag van, ja, en nu? Het zat 'm niet zo zeer in dat heel het systeem plat lag, maar meer de mogelijke gevolgen…wat zijn mogelijke consequenties van die verstoringen en wat ga je dan doen? En is er dan ook een partij die je iets kan duiden, van, dit zijn dan de mogelijke consequenties en dit zijn de mogelijke acties die je daar op kan nemen? En dat is gewoon nog voor een groot deel onbekend." (Directeur Veiligheidsalliantie Rotterdam)

Onbekendheid blijkt dus een terugkerend thema te zijn als het gaat om cybercriminaliteit. Ook als wel bekend is wat er moet gebeuren, zoals bij de National High Tech Crime Unit (NHTCU), kan het nog even duren totdat er daadwerkelijke actie plaatsvindt. Vooral als de aanpak samenwerking met andere landen vereist en er een rechtshulpverzoek aangevraagd moet worden, kan de aanpak lang op zich laten wachten, wat de effectiviteit ondermijnt. Jongeren die zich bezighouden met cybercriminaliteit hebben op deze manier vrij spel. Ook de wetgeving kan een barrière opwerpen voor het bestraffen van daders. Het OM is bijvoorbeeld belast met het bewijzen dat bepaalde jongeren schuldig zijn aan internetoplichting. Daarvoor moet bewezen worden dat de jongere oplichtingshandelingen heeft gepleegd, waarbij één oplichtingshandeling volgens jurisprudentie niet volstaat. Als er inderdaad bewijs is van slechts één oplichtingshandeling, is dat niet voldoende om te bewijzen dat de jongere schuldig is aan oplichting en kan strafrechtelijke vervolging niet plaatsvinden, omdat er in dit geval sprake is van een civiele kwestie tussen de verdachte en het slachtoffer.

Tenslotte kan de samenwerking met private partijen een knelpunt zijn. Het opvragen van bijvoorbeeld bankgegevens door de politie kan zes tot acht weken duren, waardoor een financieel onderzoek veel tijd in beslag neemt. Het feit dat dit bij sommige banken meer gebeurt dan bij andere banken is afhankelijk van de voorwaarden die een bank stelt. Een mogelijke oplossing om witwassen via deze banken te voorkomen is het daglimiet voor het opnemen van geld te verlagen, maar de bank weigert dit omdat de bank bang is dat de klanten dan reden zien om naar een andere bank te gaan. Het feit dat deze belangen zo botsen baart zorgen, omdat ook banken witwassen voor internetoplichting op deze manier faciliteren.

Veel van deze knelpunten zullen worden aangepakt in toekomstig beleid. Een belangrijk element in het ontwikkelen van toekomstig beleid is het vergroten van kennis en bewustzijn. Veel organisaties hebben voor ogen dit te bewerkstelligen door middel van voorlichting van burgers en

bijvoorbeeld op scholen. Ook is de gemeente bezig met het ontwikkelen van trainingen voor senioren en conferenties voor MKB-ondernemers. Daarnaast kunnen er praktische tips worden gegeven aan jongeren over de risico's van internetgebruik.

De stap naar de politie moet ook kleiner worden en het vertrouwen in de politie moet worden bijgeschaafd. Als burgers het gevoel hebben dat de politie ook daadwerkelijk iets kan doen met de aangifte die zij aanleveren, zullen ze ook sneller naar de politie stappen om hun verhaal te doen. Succesverhalen van de politie zouden hierbij een belangrijke rol kunnen spelen. Ook zijn de Veiligheidsalliantie Rotterdam en Gemeente Rotterdam in samenwerking met de politie bezig met het ontwikkelen van een meldpunt voor cybercriminaliteit. Burgers kunnen bij dit meldpunt terecht om aan te geven dat ze slachtoffer zijn geworden van cybercriminaliteit. Het is de bedoeling dat slachtoffers niet direct aangifte hoeven te doen, maar wel die mogelijkheid hebben. Daarnaast krijgen slachtoffers hulp en slachtofferzorg aangeboden en kunnen ze terecht bij een fraudehelpdesk. Op deze manier krijgen de politie en andere betrokken organisaties ook inzicht in het vóórkomen van cybercriminaliteit en worden burgers tegelijkertijd geholpen. Indien het meldpunt voor burgers de gewenste resultaten oplevert, is het ook de bedoeling dat het meldpunt op een zodanige manier wordt uitgebreid dat het ook toegankelijk is voor ondernemers.

Daarnaast moet er een integrale aanpak worden ontwikkeld door betrokken partijen. De afgelopen jaren hebben de betrokken partijen allemaal een eigen strategie bedacht om cybercriminaliteit aan te pakken. De partijen realiseerden zich dat ze allemaal ongeveer hetzelfde aan het doen waren en zien mogelijkheden om die strategieën samen te voegen. Concreet betekent dat dat de betrokken partijen een nauw samenwerkingsverband aan moeten gaan om cybercriminaliteit op een effectieve manier het hoofd te kunnen bieden. Grote gemeenten in Nederland werken al samen voor het ontwikkelen van beleid rondom de omgang met cybercriminaliteit. De vraagstukken die deze gemeenten samen in kaart proberen te brengen hebben nu vooral betrekking op cybergevolgbestrijding. De gemeente is in principe verantwoordelijk voor de veiligheidsdriehoek (politie, brandweer en ambulance) en stuurt deze partijen ook aan in een crisissituatie. Het is nog onduidelijk hoe een gemeente zou moeten handelen in het geval van een crisissituatie rondom cybercriminaliteit en daarom werken gemeenten aan een concrete strategie om te handelen in een dergelijke crisissituatie.

Bovendien zijn er ontwikkelingen in het denken van overheidsorganisaties over de opsporing en aanpak van daders. Om niet alleen de politie en het OM te belasten met het opsporen van cybercriminelen, kunnen publiek-private samenwerkingsverbanden worden aangegaan. Private partijen hebben misschien de technische middelen om een bijdrage te leveren aan de aanpak van cybercriminaliteit. Een publiek-private samenwerking zou dan een zeer effectieve manier zijn om cybercriminaliteit te bestrijden. Ook is er behoefte aan personeel dat gespecialiseerd is in IT of cybercriminaliteit. Met hulp van deze mensen kunnen de politie en het OM sneller en effectiever achterhalen vanuit welke plek een bepaalde cybermisdaad is gepleegd en kunnen ze daar sneller een

mogelijke verdachte aan koppelen. Het ministerie van Veiligheid en Justitie heeft al budget vrijgemaakt om dit in het gehele land te bewerkstelligen.

Misschien belangrijker nog dan de huidige ontwikkelingen is de insteek waarmee betrokken partijen cybercriminaliteit benaderen. Er zijn veel knelpunten met het huidige beleid en bovendien blijkt het niet altijd effectief. Het kan waardevol zijn om te denken in alternatieven en vooral om in de huid te kruipen van een cybercrimineel. De meeste verdachten hebben niet eens altijd een crimineel motief, ze zoeken simpelweg manieren om snel geld te verdienen. Daarom is het verstandig om te bedenken wat betrokken partijen als alternatief kunnen aanbieden om cybercriminelen af te laten wijken van hun huidige activiteiten. Bovendien is het belangrijk om ervoor te zorgen dat organisaties die cybercriminaliteit faciliteren aan te pakken.

> "[W]e hebben eigenlijk te maken met een soort van ijsberg. Criminaliteit is een ijsberg en je ziet eigenlijk maar een heel klein deel zichtbaar. En we hebben de neiging om daar heel erg in te hakken, dat is fijn, maar als je alleen maar dat doet, dan drijft die ijsberg weer naar boven en ben je weer terug bij af. Dus het is verstandig om niet alleen te hakken, maar ook het water te verwarmen. Rondom die ijsberg. Om het heel onplezierig te maken voor mensen die zich bezig houden met criminaliteit. En dan de vormen van cybercrime die daar ook een rol spelen, die dat ook makkelijk faciliteren, die dat gunstig maken. En daar zou je als eerste mee aan de slag moeten gaan." (Stadsmarinier Rotterdam-Zuid, Gemeente Rotterdam)

Uit bovenstaand citaat blijkt het belang van de publiek-private samenwerkingen. Als iedereen ervan overtuigd is dat cybercriminaliteit verminderd moet worden en het duidelijk is dat private organisaties soms onbewust illegale activiteiten faciliteren, is er een grond om een integrale aanpak op te bouwen.

4.2.3 Kennis en samenwerking

Waar de partijen vooral behoefte aan lijken te hebben zijn kennis en samenwerking. Kennis heeft vooral betrekking op gegevens over het vóórkomen van cybercriminaliteit, het handelingsperspectief voor wanneer er een cybercrisis plaatsvindt en kennis over het bewustzijn van burgers en ondernemers. De meeste elementen van kennis worden al opgepakt in het toekomstig beleid, maar dat wil niet zeggen dat de behoefte aan deze kennis op korte termijn wordt vervuld. Een handelingsperspectief voor cybergevolgbestrijding kan in principe binnen een redelijk korte termijn worden ontwikkeld, maar daarbij hebben betrokken partijen nog steeds te maken met andere partijen en beleidsprocessen die de ontwikkeling hiervan kunnen vertragen. Gegevens over het vóórkomen van cybercriminaliteit worden gedurende 2019 in Rotterdam verzameld door middel van een enquête. Op deze manier krijgt de gemeente al een beter beeld van cybercriminaliteit in Rotterdam. Het meldpunt dat de gemeente en de Veiligheidsalliantie Rotterdam aan het ontwikkelen zijn zal hier ook een belangrijke rol bij kunnen

spelen. Deze projecten zijn echter nog in ontwikkeling, waardoor de kennis over het vóórkomen van cybercriminaliteit op dit moment nog achterblijft.

Een tweede behoefte van de betrokken partijen is samenwerking. Er is niet alleen behoefte aan samenwerking met overheidsorganisaties, maar ook met private organisaties. De huidige samenwerking tussen overheidsorganisaties kan verbeterd worden om zo samen een integrale aanpak van cybercriminaliteit te ontwikkelen, zonder dat elke partij afzonderlijk een strategie gaat bedenken. Daarnaast zien de partijen in dat publiek-private samenwerkingen vruchtbaar kunnen zijn in de aanpak van cybercriminaliteit omdat zij op een andere manier kijken naar cybercriminaliteit en daarbij ook andere inzichten en bevoegdheden hebben. Daarom is er behoefte aan de connectie tussen overheidsorganisaties en private ondernemingen die bij voorkeur gevormd wordt door hoogopgeleiden die een voet hebben in het bedrijfsleven en tegelijkertijd betrokken zijn bij publieke organisaties.

5. Discussie

Tot dusver was het onduidelijk in hoeverre cybercriminaliteit voorkomt in Rotterdam-Zuid en welke partijen over welke kennis over cybercriminaliteit beschikken. In opdracht van het OM en het NPRZ heeft deze scriptie getracht een beeld te schetsen van de aard en omvang van cybercriminaliteit in Rotterdam-Zuid en welke partijen hierbij betrokken zijn. Dit onderzoek is uitgevoerd aan de hand van een tweetal segmenten: een wetenschappelijk segment en een beleidssegment. In het wetenschappelijk segment is vooral de nadruk gelegd op de mate waarin cybercriminaliteit voorkomt onder jongeren in Rotterdam-Zuid en hoe dit verklaard kan worden. Deze informatie is verzameld door middel van het afnemen van een enquête. In het beleidssegment is aandacht besteed aan de partijen die betrokken zijn bij beleid rondom cybercriminaliteit en het huidig en toekomstig beleid rondom dit onderwerp. Om deze informatie helder te krijgen, zijn er open interviews gehouden met de betrokken partijen.

De eerste onderzoeksvraag die centraal stond had een beschrijvende aard en luidde als volgt: Welke vormen van cybercriminaliteit komen vooral voor in Rotterdam-Zuid? Allereerst moet opgemerkt worden dat inwoners van Rotterdam-Zuid niet vaker slachtoffer zijn dan mensen die niet woonachtig zijn in Rotterdam-Zuid. De meest voorkomende vormen van cybercriminaliteit waar inwoners van Rotterdam-Zuid slachtoffer van worden zijn virussen, phishing, internetoplichting en hacking. Inwoners van Rotterdam-Zuid zijn wél vaker dader van cybercriminaliteit. De meest voorkomende vormen van cybercriminaliteit waar inwoners van Rotterdam-Zuid zich schuldig aan hebben gemaakt zijn virussen, cyberpesten, password cracking, internetoplichting en hacking.

De tweede onderzoeksvraag die centraal stond richtte zich op het verklaren van deze patronen: Hoe kan cybercriminaliteit in Rotterdam-Zuid verklaard worden? De eerste en meest noemenswaardige bevinding is dat ‘Woonachtig in Rotterdam-Zuid’ steeds als een verklarende factor terugkomt in de resultaten, wat aantoont dat het lokale component een rol speelt. Er is overigens geen sprake van multicollineariteit, wat betekent dat ‘Woonachtig in Rotterdam-Zuid’ niet overlapt met andere factoren zoals leeftijd, migratieachtergrond, leeftijd, sociale kwetsbaarheid of sociaaleconomische status die meegenomen zijn in de analyse.

Ten tweede heeft dit onderzoek gevonden dat er een positief verband is tussen sociale kwetsbaarheid en daderschap van cybercriminaliteit. Sociale kwetsbaarheid bestaat uit armoede, scholingsgraad, gezinsstructuur en etnische afkomst en zorgt voor een beperkter vermogen om om te gaan met gebeurtenissen die een negatieve invloed kunnen hebben op hun emotionele, fysieke of financiële welzijn (Van Damme & Pauwels, 2010; Fisher et al., 2016). De verwachting was dat sociale kwetsbaarheid de kans op slachtofferschap zou vergroten, maar uit de resultaten blijkt dat er juist een relatie is tussen sociale kwetsbaarheid en daderschap (Riesig et al., 2009). Impulsiviteit en social learning hebben invloed op dit verband. Zelfcontrole, hier geoperationaliseerd als impulsiviteit, is volgens de General Theory of Crime een verklaring voor de bevinding dat individuen vatbaarder zijn

voor deelname aan criminele activiteiten, omdat ze impulsiever en egoïstischer zijn (Gottfredson & Hirshi, 1990, zoals beschreven in Maimon & Louderback, 2019; Donner et al., 2014, zoals beschreven in Jahankhani, 2018; Marcum et al., 2014; Holt & Kilger, 2008; Bossler & Burruss, 2011). De Social Learning Theory vult dit aan met de bewering dat imitatie en deviante associatie ervoor zorgen dat crimineel gedrag wordt aangeleerd door te testen op welke gedragingen beloningen volgen. De ontdekking dat cybercriminaliteit hoge beloningen en lage risico's kent, kan leiden tot online crimineel gedrag (Jahankhani, 2018; Maimon & Louderback, 2019). De bevindingen van dit onderzoek tonen aan dat deviante associatie inderdaad een rol speelt bij cybercriminalitiet, wat de Social Learning Theory bevestigt.

Een derde belangrijke bevinding is dat sociale kwetsbaarheid een positieve invloed heeft op strain en dat strain een positieve invloed heeft op daderschap van cybercriminaliteit. Volgens de General Strain Theory kunnen individuen strain ervaren als zij spanningen ervaren als onjuist en onproportioneel, als ze druk creëren en er weinig sociale controle is. Sociale kwetsbaarheid kan bijvoorbeeld leiden tot gevoelens van strain en als gevolg daarvan nemen de vaardigheden om hier op een legale manier mee om te gaan af, dientengevolge dat individuen vervallen in cybercriminaliteit (Agnew, 2001; Baron, 2004). Dit onderzoek heeft gronden gevonden om de General Strain Theory aan te nemen.

Ten vierde heeft dit onderzoek gevonden dat sociale kwetsbaarheid een negatieve invloed heeft op tijdsbesteding en tijdsbesteding een positieve invloed op slachtofferschap van cybercriminaliteit heeft. Dat betekent dat hoe sociaal kwetsbaarder iemand is, hoe minder tijd deze persoon op het internet besteedt, hoe kleiner de kans dat diegene slachtoffer wordt van cybercriminaliteit. In de theorie kwam niet naar voren dat sociale kwetsbaarheid invloed heeft op tijdsbesteding. Uit het onderzoek van Leukfeldt (2015) bleek echter wel dat veel tijd besteden op het internet een risicoverhogende factor is, wat overeenkomt met de resultaten van dit onderzoek. Op basis hiervan kan de Routine Activity Theory worden aangenomen.

Tenslotte hebben differentiële associatie en migratieachtergrond een directe positieve invloed op slachtofferschap van cybercriminaliteit. Differentiële associatie houdt in dat de kans om slachtoffer te worden groter is wanneer individuen kennissen hebben die zich bezighouden met cybercriminaliteit (Bossler & Holt, 2009; Maimon et al., 2013). Uit dit onderzoek blijkt dat differentiële associatie inderdaad de kans op slachtofferschap van cybercriminaliteit vergroot. Ook migratieachtergrond vergroot deze kans, omdat individuen wiens ouders allebei uit het buitenland komen de digitale connectie met familie in het buitenland in stand houden (Näsi et al., 2015).

De derde centrale onderzoeksvraag heeft betrekking op het huidige beleid rondom cybercriminaliteit in Rotterdam-Zuid: Welke maatregelen zijn er tot nu toe genomen om cybercriminaliteit te verminderen in Rotterdam-Zuid? Het huidige beleid van veel overheidsorganisaties is vooral gericht op het voorkómen van slachtofferschap met als doel om het bewustzijn en de weerbaarheid van burgers en ondernemers te vergroten. Gemeente Rotterdam en

Veiligheidsalliantie Rotterdam proberen het bewustzijn van cybercriminaliteit te vergroten door praktische tips te geven om burgers en ondernemers weerbaarder te maken tegen cybercriminaliteit. Deze tips bestaan vooral uit advies voor de beveiliging van computers en data. De politie en het OM proberen ook first offenders te helpen door een maatwerkoplossing te bieden. Voor jonge hackers is er HACKRIGHT, waarbij ze stage gaan lopen bij een IT-bedrijf en leren hoe ze hun vaardigheden ten goede kunnen gebruiken. Katvangers geven een presentatie op scholen zodat ze zelf inzien dat wat ze hebben gedaan zeer schadelijk is en voorkomen dat andere jongeren op hetzelfde pad terecht komen. Daarnaast kunnen online daders hun straf ook online voldoen, omdat dit tenslotte hun werkgebied is. Deze maatregelen zullen kritisch worden geanalyseerd in Hoofdstuk 6: Beleidsaanbevelingen. Hierop zullen ze beleidsaanbevelingen volgen, waarmee de vierde onderzoeksvraag wordt beantwoord.

Hoewel dit onderzoek erg informatief is geweest en antwoord geeft op al haar onderzoeksvragen, kent dit onderzoek enkele limitaties. Het feit dat dit onderzoek een verkennend onderzoek was, maakte het erg moeilijk om een goede afbakening te maken. De patronen die zichtbaar werden tijdens het onderzoek konden niet verder worden uitgediept wegens de brede oriëntatie van het onderzoek. Als gevolg hiervan zouden andere voorkomende vormen van cybercriminaliteit over het hoofd kunnen worden gezien, terwijl het doel van het onderzoek was om een breed beeld te schetsen van cybercriminaliteit in Rotterdam-Zuid. De brede oriëntatie van het onderzoek heeft echter de behoefte om de zichtbare patronen en het beleid verder uit te diepen aangewakkerd.

Een tweede limitatie is dat het onderzoek een relatief kleine steekproef in de analyse heeft kunnen opnemen. Dat is onder andere te wijten aan het feit dat een groot aantal scholen niet de moeite heeft genomen om antwoord te geven op de vraag of ze mee wilden werken aan het onderzoek, waardoor veel leerlingen en studenten niet konden worden bereikt. Bovendien zijn jongeren die voldoen aan de criteria van de doelgroep moeilijk bereikbaar. Een bijkomende beperking is dat de dataverzameling plaatsvond tijdens de examenperiode, waardoor veel scholen en leerlingen deelname aan een onderzoek kunnen zien als tijdrovend.

Ondanks deze limitaties heeft dit onderzoek een beeld kunnen schetsen van cybercriminaliteit onder jongeren in Rotterdam-Zuid. Daarnaast is duidelijk geworden welke partijen een rol spelen bij cybercriminaliteit en wat het huidige beleid is rondom dit onderwerp. Dit onderzoek heeft kunnen aantonen dat het online domein en jongeren regelmatig te maken hebben met cybercriminaliteit dat cybercriminaliteit weldegelijk een lokale component in zich heeft, wat eerder onderzoek tegenspreekt (Van de Pavert, 2018). Hoewel er verschillende sociaaleconomische factoren zijn die een rol spelen bij cybercriminaliteit, is er een factor die een grote invloed heeft, maar waar dit onderzoek nog niet de vinger op heeft kunnen leggen: Rotterdam-Zuid. Dit gegeven toont aan dat niet alleen sociaaleconomische factoren cybercriminaliteit in Rotterdam-Zuid kunnen verklaren. Ook Rotterdam-Zuid zelf is klaarblijkelijk een manifestatie van de lokaliteit van cybercriminaliteit, wat reden geeft om lokaal aandacht te besteden aan cybercriminaliteit.

6. Beleidsaanbevelingen

Dit hoofdstuk behandelt het huidige beleid en het toekomstig beleid. Het doel van dit hoofdstuk is om antwoord te geven op de vierde onderzoeksvraag: Op welke manier(en) kunnen betrokken partijen cybercriminaliteit in Rotterdam-Zuid verminderen? Allereerst wordt het huidige beleid kritisch geanalyseerd door de knelpunten in ogenschouw te nemen. Daarna zullen er suggesties worden gedaan voor toekomstig beleid en vervolgonderzoek.

Wat betreft huidig beleid is er een verschuiving zichtbaar in de focus van betrokken partijen. Voorheen richtten OM en politie zich vooral op de vervolging en bestraffing van daders, waar andere betrokken partijen zich alleen bezig hielden met preventie van slachtofferschap. Tegenwoordig is preventie ook gericht op potentiële daders en houden OM en politie zich daar ook steeds meer mee bezig. Bovendien is preventie een haalbare manier om cybercriminaliteit aan te pakken, omdat opsporing van cyberdaders moeilijk is. Het feit dat OM en politie steeds meer preventieve maatregelen nemen, betekent dat ze ook steeds meer samenwerken met organisaties die zich al langer bezig houden met preventie. Ook hebben partijen die zich richten op preventie zo meer contact met de strafrechtelijke kant en worden zij ook betrokken bij een deel van de straf, bijvoorbeeld dat jongeren een presentatie geven op een school of dat jongeren hun straf online voldoen via jongerenwerkers.

Toch blijkt dat het huidige beleid nog geen vergevorderde aanpak van cybercriminaliteit betreft. Hoewel sommige interventies zeker het gewenste effect bereiken, zijn de meeste betrokken partijen nog zoekende naar een effectieve manier om de cybercriminaliteitsproblematiek het hoofd te bieden. Niet alleen weten betrokken partijen niet goed waar ze moeten beginnen, ze lopen ook tegen een aantal knelpunten aan. Een knelpunt dat vaak als eerst ter sprake komt is capaciteit. Het feit dat de aanpak van cybercriminaliteit nog in de kinderschoenen staat, zorgt ervoor dat er nog weinig aandacht voor de aanpak is en er nog niet veel concrete actie wordt ondernomen. Daarnaast lijkt het erop dat er een beperkt bewustzijn is van de schade die cybercriminaliteit kan toebrengen, vooral bij preventie-georiënteerde partijen. Het is daarom van groot belang dat de urgentie van de aanpak van cybercriminaliteit duidelijk wordt. Het OM werkt daar hard aan, maar kan dat niet zonder de erkenning van het gevaar van cybercriminaliteit door andere partijen. Er is daarom een grote noodzaak om samen te werken met andere partijen en samen deze urgentie bij te brengen aan betrokken partijen. Dat kan plaatsvinden door middel van een regelmatig overleg in een samenwerkingsverband tussen de betrokken partijen.

Daarnaast vormt cybercriminaliteit een *wicked problem.* Wicked problems zijn maatschappelijke problemen waarbij er kennis ontbreekt en er onenigheid is over waarden (Klijn & Koppenjan, 2016). Dat betekent dat partijen aan de ene kant moeilijkheden ervaren bij het interpreteren van de aard van het probleem, de oplossingen en wie de problematiek aan moet pakken. Dat is mede te wijten aan de verschillende prioriteiten en belangen die betrokken partijen hebben. Dat is precies wat het geval is met cybercriminaliteit. De aard van cybercriminaliteit is zodanig onbekend bij betrokken

partijen dat ze moeite heben met het verzamelen van informatie over het probleem en het maken van beleid maar moeilijk van de grond komt. Bovendien worstelen partijen met wie verantwoordelijk is voor de oplossing van het probleem. Daarnaast botsen de belangen, vooral tussen publieke en private partijen. Aan de andere kant is er een tekort aan kennis over de aard van het probleem, de verklaringen en de gevolgen ervan (Klijn & Koppenjan, 2016). Het is problematisch om aan kennis over het probleem te komen voor betrokken partijen, omdat de kennis die er is afkomstig is uit politiestatistieken en deze niet representatief zijn. Dit tekort is ook een oorzaak van het gebrek aan kennis over de verklaringen, omdat er als gevolg van de beperkte politiestatistieken ook beperkte verklaringen kunnen worden ondervonden. Bij kleinere cybercrimezaken zijn de gevolgen bekend, maar het is de vraag wat de consequenties zijn als er een grote cyberaanval plaatsvindt op een grote organisatie of infrastructuur. Op basis van deze informatie kan gesteld worden dat er sprake is van substantieve complexiteit (Klijn & Koppenjan, 2016).

Mijns inziens is het het best om deze substantieve complexiteit te verminderen door middel van een netwerkbenadering. Deze benadering benadrukt het belang van het erkennen dat er meerdere percepties en voorkeuren zijn, maar dat de betrokken partijen tegelijkertijd moeten zoeken naar gemeenschappelijke gronden om hun aanpak op te funderen (Klijn & Koppenjan, 2016). De partijen zijn het tot nu toe in ieder geval over één punt eens: cybercriminaliteit moet aangepakt worden. Dat is een goed uitgangspunt. Bij het vinden van een oplossing blijft het belangrijk om het bestaan van verschillende percepties te erkennen, maar partijen kunnen het ook zien als een kans om van elkaar te leren. Ook de substantieve complexiteit kan worden verminderd door middel van een samenwerkingsverband.

Tenslotte is er ook sprake van institutionele complexiteit. Er is sprake van institutionele complexiteit wanneer de regels van een netwerk of organisatie onduidelijk, tegenstrijdig of dubbelzinnig zijn. Ook kan een gebrek aan vertrouwen bijdragen aan institutionele complexiteit (Klijn & Koppenjan, 2016). In het netwerk van de aanpak van cybercriminaliteit in Rotterdam-Zuid is er sprake van de tegenstrijdigheid van regels binnen organisaties. Het gaat dan vooral om de manier waarop bepaalde organisaties te werk gaan. De politie en het OM gaan op een traditionele manier om met cybercriminaliteit, omdat zij afhankelijk zijn van wetgeving en deze nog niet volledig is aangepast op de huidige cybercriminaliteitsproblematiek. Op deze manier krijgen daders niet altijd een passende straf. Aan de andere kant proberen deze en andere organisaties op een innovatieve manier om te gaan met cybercriminaliteit, maar de bureaucratie van hun organisatie beperkt hen daarin. Ook de werkwijze van private partijen, zoals bijvoorbeeld banken, maken het moeilijk om een efficiënte aanpak van cybercriminaliteit te bewerkstelligen. De procedure om bijvoorbeeld bankgegevens aan de politie te leveren duurt een aantal weken. Dat is problematisch, omdat de politie lang op deze gegevens moet wachten. De zaak heeft echter niet de prioriteit van de bank, waardoor het proces niet versneld kan worden. Ook dit toont de prioriteiten van de bank, waaruit substantieve complexiteit blijkt.

Het verminderen van institutionele complexiteit is veel ingewikkelder dan het verminderen van substatieve complexiteit. Institutionele complexiteit behelst professionele codes waaraan professionals zich houden en aan de hand waarvan ze functioneren (Klijn & Koppenjan, 2016). Ze kunnen de ontwikkeling van nieuw beleid echter beperken. Om gezamenlijke doelen te bereiken, zoals het verminderen van cybercriminaliteit, moeten professionals hun professionele codes anders vormgeven in de samenwerking met andere organisaties, maar wel behouden in hun eigen professionele netwerk. Dat betekent dat professionals hun rol moeten herdefiniëren op eigen initiatief om het gewenste doel te bereiken (ibid). Concreet betekent dat dat de betrokken partijen open moeten staan voor andere perspectieven en bereid moeten zijn hun regels te buigen om zo een integrale aanpak te bewerkstelligen.

De aanbevelingen voor de oplossing van knelpunten kunnen samen worden gevoegd in een Cyber Cirkel Coalitie. Daarbij komen betrokken en geïnteresseerde partijen, genaamd coalitiegenoten, samen om kennis te delen, van elkaar te leren en mogelijke ideeën te bespreken om cybercriminaliteit aan te pakken. Een dergelijke cirkelcoalitie zou niet alleen een mooie manier zijn om ervoor te zorgen dat er één geheel beeld is van cybercriminaliteit in Rotterdam-Zuid waar alle betrokken partijen toegang tot hebben, maar ook een samenwerkingsverband waaruit een integrale aanpak van cybercriminaliteit kan ontstaan. Door regelmatig bijeenkomsten te houden met verschillende sprekers houden de partijen elkaar op de hoogte van ontwikkelingen op het gebied van cybercriminaliteitsbeleid en informatie over daders en slachtoffers.

Om beter inzicht te krijgen in de belevingswereld van jongeren kunnen betrokken partijen zich verdiepen in het perspectief en de activiteiten van jongeren. Op deze manier krijgen betrokken partijen niet alleen een beeld van de belevingswereld van jongeren, ook is dit een manier om de verklaringen voor cybercriminaliteit onder jongeren te achterhalen. Als partijen weten wat er speelt onder jongeren, kunnen zij wellicht inspelen op de sociaaleconomische factoren die een rol spelen bij cybercriminaliteit onder jongeren. Gedeeltelijk ligt deze rol bij vervolgonderzoek.

Het beeld dat deze scriptie heeft geschetst zal verder moeten worden onderzocht om een completer en verdiepender beeld van de cybercriminaliteitsproblematiek in Rotterdam-Zuid te bewerkstelligen. Vervolgonderzoek zal gebruik moeten maken van een grotere en meer representatieve steekproef om zo de betrouwbaarheid van het onderzoek te vergroten. Ook kan vervolgonderzoek kijken naar het achterliggende mechanisme van de verklarende factor ‘Rotterdam-Zuid’. Daarnaast kan vervolgonderzoek ook een verdiepingsslag maken door te onderzoeken waarom bepaalde typen cybercriminaliteit meer voorkomen dan andere typen, welke modus operandi er worden gebruikt en welk type daders vooral schuldig is aan bepaalde typen cybercriminaliteit. Op basis van dit onderzoek zou er specifieker beleid ontwikkeld kunnen worden om bepaalde typen cybercriminaliteit tegen te gaan. Tenslotte kan vervolgonderzoek aandacht besteden aan de interventies die nu al plaatsvinden en de effectiviteit van deze interventies over een aantal jaren meten.

Literatuur

Agnew, R. (2001). Building on the foundation of general strain theory: specifying the types of strain most likely to lead to crime and delinquency. *Journal of research in crime and delinquency, 38* (4). 319-361.

Andersson, R., & Bråmå, Å. (2004). Selective migration in Swedish distressed neighbourhoods: can area-based urban policies counteract segregation processes? *Housing Studies, 19* (4), 517-539.

Baron, S.W. (2004). General strain, street youth and crime: A test of Agnew's revised theory. *Criminology, 42* (2). 457-483.

Bastiaanssen, J., Martens, C.J.C.M.., Polhuijs, G.J. (2013). Geen rijbewijs, geen fiets, geen ov-aansluiting, geen baan' : Vervoersarmoede in Rotterdam-Zuid. *Verkeerskunde, 63* (5).

Bossler, A.M., Burruss, G.W. (2011). The general theory of crime and computer hacking: low self-control hackers. In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* ed. TJ Holt, BH Schell, pp. 38–67. Hershey, PA: IGI Glob.

Bossler, A. M. & Holt, T. J. (2009), 'On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory', *International Journal of Cyber Criminology, 3,* 400–20.

Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum, 15,* 1-8. doi: 10.1007/s12027-014-0333-4.

Cárdenas, A.A., Radosavac, S., Grossklags, J., Chuang, J. & Hoofnagle, C. (2009). An economic map of cybercrime. *TPRC.* Verkregen via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997795.

CBS. (2019a). Criminaliteit. Verkregen via https://www.cbs.nl/nl-nl/achtergrond/2018/47/criminaliteit.

CBS. (2019b). Arbeidsdeelname; migratieachtergrond. Verkregen via https://opendata.cbs.nl/statline/#/CBS/nl/dataset/82809NED/table?dl=19CF1.

CBS. (2019c). Geregistreerde criminaliteit; soort misdrijf, regio. Verkregen via https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1551703707117.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2* (1), 308-333.

D'Hont, N. (2009). *De rol van individuele verschilvariabelen* (Masterthesis). Universiteit Gent, Gent.

Ellis, L. & McDonald, J.N. (2001). Crime, Delinquency, and Social Status. *Journal of Offender Rehabilitation, 32* (3), 23-52. doi: 10.1300/J076v32n03_03.

Epps, C. (2017). Best practices to deal with top cybercrime activities. *Computer Fraud &*

Security, 4, 13-15.

Fisher, M.H., Baird, J.V., Currey, A.D. & Hodapp, R.M. (2016). Victimisation and Social Vulnerability of Adults with Intellectual Disability: A review of Research extending beyond Wilson and Brewer. *Australian Psychologist, 41,* 114-127. doi: 10.1111/ap.12180.

Gemeente Rotterdam. (2017). Feitenkaart Opleidingsniveau Rotterdam op gebieds- en buurtniveau 2017. Verkregen via https://rotterdam.buurtmonitor.nl/handlers/ballroom.ashx?function=download&id=443&rnd=0.7711963653236316.

Gemeente Rotterdam. (2019). Rotterdam Onderzocht: Werkloosheid, 15 t/m 26 jaar. Verkregen via https://rotterdam.buurtmonitor.nl/dashboard/Werk--cgd8cjfXxCgg1/werkloosheid--15-t-m-26-jaar--425.

Gijsberts, M. & Dagevos, J. (2007). *Interventies voor integratie - Het tegengaan van etnische concentratie en bevorderen van interetnisch contact.* Den Haag: Sociaal Cultureel Planbureau.

Hirschi, T. (1969). *Causes of Delinquency*. Piscataway, NJ: Transaction Publ.

Holt, T.J. & Kilger, M. (2008). Techcrafters and makecrafters: a comparison of two populations of hackers. In IEEE Information Security Threats Data Collection and Sharing Workshop, pp. 67–78. New York: IEEE.

Jahankhani, H. (2018). *Cyber Criminology.* Cham, Zwitserland: Springer.

Jennings, W.J., Gibson, C. & Lanza-Kaduce, L. (2009). Why not let kids be kids? An exploratory analysis of the relationship between alternative rationales for managing status offending and youths' self-concepts. *Annual Journal of Criminal Justice, 34,* 198-212. doi: 10.1007/s12103-008-9054-y.

Klijn, E.H. & Koppenjan, J. (2016). *Governance Networks in the Public Sector.* Leiden, Nederland: Taylor & Francis Ltd.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* New York, NY: Springer. doi: 10.1007/978-3-642-11522-6.

Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention, presented at the International Conference on Cybersecurity, Redlands, 2015. California, CA.

Leukfeldt, E.R. & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37* (3), 263-280. doi: 10.1080/01639625.2015.1012409.

Lusthaus, J. & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing,* 1-11. doi:10.1093/police/pax042.

Maimon, D., Kamerdze, A., Cukier, M. & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network. *British Journal of Criminology, 53,* 319-343. doi: 10.1093/bjc/azs067.

Maimon, D. & Louderback, E.R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology, 2,* 191-216.

Marcum, C.D., Higgins, G.E., Ricketts, M.L. & Wolfe, S.E. (2014). Hacking in High School: Cybercrime Perpetration by Juveniles. *Deviant Behavior, 35*(7), 581-591. doi: 10.1080/01639625.2013.867721.

Martin, N. & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security, 30,* 803-814.

Näsi, M., Oksanen, A., Keipi, T. & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16* (2), 203–210.

NPRZ. (2019). Verkregen via https://nprz.nl.

nu.nl. (2019). Bende Marktplaats-oplichters opgepakt in Rotterdam en Schiedam. Verkregen via https://www.nu.nl/internet/5702750/bende-marktplaats-oplichters-opgepakt-in-rotterdam-en-schiedam.html.

Oosterwijk, K. & Fisher, T.F.C. (2017). Interventies jeugdige daders cybercrime. Verkregen via https://www.wodc.nl/onderzoeksdatabase/2779-interventies-jeugdige-daders-cybercrime.aspx.

Putnam, R. D. (2007). E Pluribus Unum: Diversity and community in the twenty-first century The 2006 Johan Skytte Prize Lecture. *Scandinavian Political Studies, 30* (2).

Reyns, B.W. (2015). A routine activity perspective on online victimisation: results from the Canadian General Social Survey. *Journal of Financial Crime, 22*:396–411.

Riesig, M.D., Pratt, T.C. & Holtfreter, K. (2009). Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminal Justice & Behavior, 36* (4), 369-384. doi: 10.1177/0093854808329405.

Schram, J., Scherpenisse, J. & Van Twist, M. (2018). *Zweven en zwoegen op Zuid: Een kroniek over de integrale ondermijningsaanpak op Rotterdam Zuid.* Verkregen via https://nsob.nl/wp-content/uploads/2018/10/NSOB-2018-Zweven-en-zwoegen-op-Zuid.pdf.

Tan, S. & Spies, H. (2014). Rotterdamse jongeren over sociale ongelijkheid en werkloosheid. Plusconfidence. Verkregen via http://www.plusconfidence.nl/sites/default/files/Rotterdamse%20jongeren%20over%20sociale%20ongelijkheid%20en%20werkloosheid.pdf.

Tolsma, J., Van der Meer, T., & Gesthuizen, M. (2009). The impact of neighbourhood and municipality characteristics on social cohesion in the Netherlands. *Acta Politica, 44* (3), 286-313.

Van Damme, A. & Pauwels, L. (2010). Onveiligheidsbeleving van jonge adolescenten op school: de rol van de schoolcontext, kwetsbaarheid en individuele slachtofferervaringen op school. *Panopticon, 31* (6), 17-36.

Van Deursen, A. & Van Dijk, J. (2010). Internet skills and the digital divide. *New Media & Society, 13* (6), 893-911. doi: 10.1177/1461444810386774.

Van de Pavert, D. (2018). *Ondermijnende criminaliteit in een digitaal tijdperk.* (master thesis).

Volksgezondheidenzorg.info. (2017). Sociaaleconomische status 2017. Verkregen via https://www.volksgezondheidenzorg.info/onderwerp/sociaaleconomische-status/regionaal-internationaal/regionaal#node-sociaaleconomische-status/.

Wang, J., Gupta, M., Rao, H.R. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. *MIS Q, 39*:91–112.

Wittebrood, K. (z.d.). *Sociale cohesie als bouwsteen voor veilige buurten.* SCP. Verkregen via https://www.scp.nl/dsresource?objectid=94eb5eb7-6a65-4c91-b6ce-f7ff36da0de5/.

WODC. (2019). Omvang en aard van de niet-geregistreerde criminaliteit: cybercriminaliteit, horizontale fraude en georganiseerde criminaliteit. Verkregen via https://www.wodc.nl/onderzoeksdatabase/2830b-omvang-en-aard-van-de-niet-geregistreerde-criminaliteit-cybercriminaliteit-horizontale-fraude-en-georganiseerde-criminaliteit.aspx.

Yar, M. (2016). The novelty of 'cybercrime': An Assessment in light of Routine Activity Theory. *European Journal of Criminology, 2* (4), 407-427. doi: 101177/147737080556056.

[#Online daders]. (z.d.). Geraadpleegd van http://cirkelcoalitie.nl/coalitie-dossiers/online-daders/hacker-in-opleiding/.

Bijlagen

Bijlage 1: Enquête

Enquête onderzoek online veiligheid in Rotterdam-Zuid

Dit onderzoek gaat over online veiligheid in Rotterdam-Zuid. Het doel van het onderzoek is om te achterhalen in hoeverre cybercriminaliteit voorkomt in Rotterdam-Zuid, hoe sociaaleconomische omstandigheden deze mate van online onveiligheid kunnen verklaren en op welke manieren betrokken partijen online veiligheid in dit gebied kunnen verbeteren. Het onderzoek is vooral gericht op Rotterdam-Zuid. Woon je niet in Rotterdam-Zuid, mag je de enquête wel invullen, maar is dit minder relevant voor het onderzoek dan respondenten uit Rotterdam (Zuid). Dit onderzoek is onderdeel van mijn masterscriptie voor de opleiding Sociologie van de Universiteit Utrecht en wordt uitgevoerd in samenwerking met het OM en het NPRZ, waar ik stage loop. Ik waardeer je bijdrage aan het onderzoek zeer en beloof zorgvuldig om te gaan met je tijd en informatie. Ik vraag daarom in deze enquête niet om je naam, maar wel om demografische gegevens, zoals leeftijd, geslacht, werk en opleidingsniveau. Ook de school waar je naartoe gaat blijft buiten beschouwing. De gegevens zullen anoniem blijven en alleen gebruikt worden voor dit onderzoek. Ik wil je daarom vragen om de enquête zo veel mogelijk naar waarheid in te vullen en alle vragen te beantwoorden. De enquête bestaat uit 74 vragen waaronder 54 stellingen. Het duurt ongeveer 15 tot 20 minuten om de enquête in te vullen.

Deel 1: Demografische gegevens

1. Wat is je leeftijd?
    - O Jonger dan 14 jaar
    - O 14 tot 16 jaar
    - O 17 tot 20 jaar
    - O 21 tot 23 jaar
    - O Ouder dan 23 jaar

2. Wat is je geslacht?
    - O Man
    - O Vrouw
    - O Anders

3. Wat is je etnische afkomst?
    _____

4. Wat is je opleidingsniveau (huidige opleiding of hoogst afgeronde opleiding)?
    - O Geen
    - O Basisschool
    - O VMBO/mavo
    - O Havo
    - O Vwo
    - O MBO
    - O HBO
    - O WO

5. Wat is je arbeidsstatus?
    - O Student/leerling (voltijd)
    - O Werkloos
    - O Verzorger
    - O Deeltijd werkzaam (12 tot 32 uur)
    - O Voltijd werkzaam (meer dan 32 uur)
    - O Anders, namelijk: _____

6. Indien je student bent: heb je een bijbaantje?
    - O Ja
    - O Nee
    - O Niet van toepassing

7. Wat is de arbeidsstatus van je vader?
    - O Student
    - O Werkloos
    - O Verzorger
    - O Deeltijd werkzaam
    - O Voltijd werkzaam
    - O Anders, namelijk: _____

8. Wat is de arbeidsstatus van je moeder?
    - O Student
    - O Werkloos
    - O Verzorger
    - O Deeltijd werkzaam
    - O Voltijd werkzaam
    - O Anders, namelijk: _____

9. In welke gezinssamenstelling woon je nu?
    - O Een gezin met twee ouders die samen zijn, ik ben het enige kind
    - O Een gezin met twee ouders die samen zijn, ik heb broertje(s) en/of zusje(s)
    - O Een gezin met twee ouders die gescheiden zijn, ik ben het enige kind
    - O Een gezin met twee ouders die gescheiden zijn, ik heb broertje(s) en/of zusje(s)
    - O Een gezin met één ouder, ik ben het enige kind
    - O Een gezin met één ouder, ik heb broertje(s) en/of zusje(s)
    - O Mijn ouders kunnen niet voor mij zorgen, ik woon in een opvang
    - O Ik woon zelfstandig

O Anders, namelijk: _____

10. Wat is je inkomensklasse (inkomen aangeduid per jaar)?
    O Ik krijg een uitkering
    O Ik heb geen inkomen
    O €0 tot €10.000
    O €10.001 tot €20.000
    O €20.001 tot €30.000
    O €30.001 tot €40.000
    O €40.001 tot €50.000
    O €50.001 tot €75.000
    O Meer dan €75.000

11. Waar woon je? Graag woonplaats en wijk invullen.
    _____

Deel 2: Internetvaardigheden

12. Geef aan in hoeverre je het eens bent met de volgende stellingen over internetvaardigheden.

12a. Ik kan goed omgaan met de hardware en software van een computer en begrijp hoe deze in elkaar zitten.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

12b. Ik kan begrijpen hoe de structuur van bestanden en hyperlinks in elkaar zit.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

12c. Ik kan goed omgaan met de structuur van bestanden en hyperlinks.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

12d. Ik kan specifieke informatiebronnen in computers en online netwerken vinden, selecteren, verwerken en evalueren.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

12e. Ik kan informatie die ik heb gevonden op het internet gebruiken voor specifieke doelen.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

Deel 3: Computergebruik

13. Geef aan waar je vooral het internet voor gebruikt op de volgende apparaten. Kies het antwoord
dat het meest op jou van toepassing is.

	Ik gebruik dit apparaat nooit om het internet te gebruiken	Ik gebruik dit apparaat nooit	Downloaden van het internet	Online gamen	Informatie opzoeken via Google, Google Chrome, Yahoo!, Firefox, Internet Explorer, Microsoft Edge of Safari (Apple)	Informatie opzoeken via andere webbrowsers	Werken met Microsoft Office (Word, Excel, PowerPoint, etc.)	Sociale media (Facebook, Instagram, Pinterest, LinkedIn, Twitter, Skype, Tumblr, etc.)	Online shoppen	Anders
Schoolcomputer	O	O	O	O	O	O	O	O	O	O
Vaste PC thuis	O	O	O	O	O	O	O	O	O	O
Eigen laptop	O	O	O	O	O	O	O	O	O	O
Tablet	O	O	O	O	O	O	O	O	O	O
Mobiele telefoon	O	O	O	O	O	O	O	O	O	O

14. Geef aan van welke apparaten jij weet dat ze voorzien zijn van één soort virusbeveiliging (bijv. McAfee, Norton).
    - O Vaste PC
    - O Eigen laptop
    - O Tablet
    - O Mobiele telefoon
    - O Geen van allen

15. Geef aan van welke apparaten jij weet dat ze voorzien zijn van meerdere soorten beveiliging, niet alleen virusbeveiliging (McAfee, Norton), maar ook een malwarescanner of een firewall.
    - O Vaste PC
    - O Eigen laptop
    - O Tablet
    - O Mobiele telefoon
    - O Geen van allen

16. Hoe veel tijd besteed je wekelijks op het internet, de tijd op de computer en mobiele apparaten (tablet en mobiele telefoon) bij elkaar opgeteld?
    - O 0 tot 5 uur
    - O 6 tot 10 uur
    - O 11 tot 15 uur
    - O 16 tot 20 uur
    - O 21 tot 25 uur
    - O Meer dan 25 uur

Deel 4: Cybercriminaliteit

17. Wat zijn de risico's van internetgebruik?

    _____
    _____
    _____
    _____

18. Geef hieronder aan met welke vormen van cybercriminaliteit je op welke manier te maken hebt gehad. Je kunt meerdere antwoorden aankruisen.

18a. Virus (*Een virus is een klein programma dat de werking van je computer verstoort. Een virus kan gegevens op je computer beschadigen of verwijderen, je e-mailprogramma gebruiken om zichzelf te verspreiden of zelfs je hele harde schijf wissen. Veel virussen worden per e-mail verspreid en zijn vermomd als onschuldige bijlage, zoals een foto of geluidsbestand*)

- O Ik heb hier niet mee te maken gehad
- O Ik heb een virus op mijn computer gehad en heb daar schade aan ondervonden
- O Ik heb een virus op mijn computer gehad, maar kwam er op tijd achter en heb het verwijderd voordat het schade kon veroorzaken
- O Ik heb wel eens geprobeerd een virus op iemands computer te plaatsen
- O Ik plaats vaker virussen op iemands computer
- O Anders, namelijk: _____

18b. Malware (*Malware (malicious software) is een verzamelnaam voor alle software met een opzettelijk kwaadaardige werking, vaak wordt dit ook een virus genoemd.*)

- O Ik heb hier niet mee te maken gehad
- O Ik heb malware op mijn computer gehad en heb daar schade aan ondervonden
- O Ik heb malware op mijn computer gehad, maar kwam er op tijd achter en heb het verwijderd voordat het schade kon veroorzaken
- O Ik heb wel eens geprobeerd malware op iemands computer te plaatsen
- O Ik plaats vaker malware op iemands computer
- O Anders, namelijk: _____

18c. Phishing (*Het per mail hengelen naar informatie door criminelen wordt phishing genoemd. Via de mail (maar ook via de telefoon) lijken betrouwbare instanties zoals een bank of creditcardmaatschappij te vragen om bijvoorbeeld inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie.*)

- O Ik heb hier niet mee te maken gehad
- O Ik heb wel eens een phishing mailtje of telefoontje gehad en ben daar op ingegaan
- O Ik heb wel eens een phishing mailtje of telefoontje gehad, maar ik heb het verwijderd of opgehangen
- O Ik heb wel eens geprobeerd om te phishen
- O Ik phish regelmatig
- O Anders, namelijk: _____

18d. Ransomware (*Ransomware is een computervirus dat probeert je geld te laten betalen om van het virus af te komen. Ransomware kaapt je computer door bijvoorbeeld documenten en foto's te blokkeren waardoor ze niet meer toegankelijk zijn. Het virus meldt dat je een geldbedrag moet betalen om van de blokkade af te komen.*)

- O Ik heb hier niet mee te maken gehad
- O Ik heb wel eens ransomware op mijn computer gehad en heb hier schade aan ondervonden
- O Ik heb wel eens ransomware op mijn computer gehad, maar ik heb niet betaald en het virus verwijderd
- O Ik heb wel eens geprobeerd om ransomware op iemands computer te plaatsen
- O Ik plaats vaker ransomware op iemands computer
- O Anders, namelijk: _____

18e. Botnet (*Botnets zijn netwerken van computers die zonder medeweten van hun eigenaar besmet zijn met een virus of andere software en door derden worden misbruikt. Botnets worden gebruikt voor het versturen van spam en het uitvoeren van cyberaanvallen.)*

- O Ik heb hier niet mee te maken gehad
- O Mijn computer is onderdeel geweest van een botnet en ik heb hier schade aan ondervonden
- O Mijn computer is onderdeel geweest van een botnet, maar ik kwam hier op tijd achter en heb hier geen schade aan ondervonden
- O Ik heb wel eens geprobeerd om computers aan een botnet toe te voegen
- O Ik beheer een botnet en verstuur regelmatig spam of voer een cyberaanval uit
- O Anders, namelijk: _____

18f. Cryptojacking (*Cryptojacking is een vorm van cybercrime waarbij cybercriminelen geld willen verdienen door cryptogeld (bijvoorbeeld Bitcoin) in handen te krijgen. Dit doen ze in te breken op zoveel mogelijk wifi-netwerken, computers en websites, ook van mensen die niet in cryptogeld handelen. Ze besmetten de netwerken en apparaten dan bijvoorbeeld met malware om ze onderdeel te maken van een botnet voor cryptomining (handelen in cryptogeld))*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens gecryptojackt en heb hier schade aan ondervonden
- O Ik ben wel eens gecryptojackt, maar ik heb ervoor gezorgd dat het geen schade meer zou kunnen aanrichten bij mij
- O Ik heb wel eens geprobeerd om iemand te cryptojacken
- O Ik cryptojack vaker
- O Anders, namelijk: _____

18g. Pinpasfraude (*Criminelen kunnen je bijvoorbeeld via sociale media benaderen met de vraag of ze geld op je rekening mogen laten storten. Ze nemen het geld daarna van je rekening op door te pinnen met jouw bankpas en pincode. Hiervoor bedenken ze een misleidend verhaal en stellen ze een beloning in het vooruitzicht in de hoop dat je meewerkt. De beloning krijg je alleen niet en het gaat om illegaal verkregen geld dat ze willen wegsluizen. Omdat het via jouw rekening loopt, werk jij mee aan de criminele activiteit en ben jij ook strafbaar.)*

- O Ik heb hier niet mee te maken gehad
- O Ik heb wel eens pinpasfraude meegemaakt en heb hier schade aan ondervonden
- O Ik heb wel eens pinpasfraude meegemaakt, maar ik ben er niet ingetrapt
- O Ik heb wel eens geprobeerd om pinpasfraude te plegen
- O Ik pleeg regelmatig pinpasfraude
- O Anders, namelijk: _____

18h. Helpdeskfraude (*Helpdeskfraude is een vorm van oplichting waarbij fraudeurs vaak vanuit landen als India bellen en doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn, zoals Microsoft, Google en Ziggo. Ze zeggen je dat je computer besmet is met virussen of dat je gehackt bent. Als je hier aan meewerkt, krijgen ze op slinkse wijze toegang tot je computer en maken ze je geld naar zichzelf over.)*

- O Ik heb hier niet mee te maken gehad
- O Ik heb wel eens helpdeskfraude meegemaakt en heb hier schade aan ondervonden
- O Ik heb wel eens helpdeskfraude meegemaakt, maar ik ben er niet ingetrapt
- O Ik heb wel eens geprobeerd om helpdeskfraude te plegen
- O Ik pleeg regelmatig helpdeskfraude
- O Anders, namelijk: _____

18i. Identiteitsfraude (*Bij identiteitsfraude maakt iemand misbruik van je persoonlijke gegevens. Onder je naam worden er producten of diensten besteld, uitkeringen of creditcards aangevraagd, betalingen gedaan of bankrekeningen geopend.)*

- O Ik heb hier niet mee te maken gehad
- O Ik heb wel eens identiteitsfraude meegemaakt en heb hier schade aan ondervonden
- O Ik heb wel eens identiteitsfraude meegemaakt, maar ik heb mijn persoonlijke gegevens niet verstrekt
- O Ik heb wel eens geprobeerd om identiteitsfraude te plegen
- O Ik pleeg regelmatig identiteitsfraude
- O Anders, namelijk: _____

18j. Terrorisme (*Terroristen en andere radicale personen en groeperingen maken in groten getale gebruik van internet, bijvoorbeeld voor propaganda, het oproepen tot haat en geweld en het bedreigen van personen of instanties. Ook wordt internet ingezet bij het rekruteren en mobiliseren van personen bij het plannen van aanslagen.*)

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van terroristisch geweld
- O Ik heb wel eens propaganda of oproepen tot haat en geweld langs zien komen, maar heb hier niets mee gedaan
- O Ik heb wel eens propaganda of oproepen tot haat en geweld verspreid, of geholpen met rekruteren en mobiliseren van personen bij het plannen van aanslagen
- O Ik verspreid regelmatig propaganda of oproepen tot geweld en rekruteer en mobiliseer personen bij het plannen van aanslagen
- O Anders, namelijk: _____

18k. DDoS-aanval (*Distributed denial-of-service (DDoS)-aanvallen hebben als doel een website of internetdienst onbruikbaar te maken door middel van overbelasting van de server. Vaak gaat het om websites van grote commerciële bedrijven, diensten van banken en creditcardmaatschappijen of e-maildiensten. De criminelen achter de aanvallen kunnen veel geld verdienen door hun diensten te verhuren of door bedrijven te chanteren. Particuliere websites zullen niet snel worden aangevallen, omdat er geen commercieel belang is.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van een DDoS-aanval en heb hier schade aan ondervonden
- O Ik heb wel eens een DDoS-aanval meegemaakt, maar het is niet gelukt en er is dus ook geen schade gemaakt
- O Ik heb wel eens geprobeerd een DDoS-aanval te plegen
- O Ik pleeg regelmatig DDoS-aanvallen
- O Anders, namelijk: _____

18l. Hacking (*In het dagelijks taalgebruik verstaan we onder hacken het inbreken in een computersysteem of netwerk. De inbrekers, hackers genoemd, kunnen hiervoor onder meer gebruikmaken van virussen, spyware, phishing en poortscans.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens gehackt en heb hier schade aan ondervonden

- O Ik ben wel eens gehackt, maar heb kunnen voorkomen dat er schade gemaakt kon worden
- O Ik heb wel eens geprobeerd te hacken
- O Ik hack regelmatig
- O Anders, namelijk: _____

18m. Internetoplichting (*Bekende vormen van oplichting zijn: phishing, scam, marktplaatsfraude en malafide ticketsites.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens opgelicht via het internet en heb hier schade aan ondervonden
- O Ik ben wel eens opgelicht via het internet, maar ben er niet ingetrapt
- O Ik heb wel eens geprobeerd om iemand op te lichten via het internet
- O Ik licht regelmatig mensen op via het internet
- O Anders, namelijk: _____

18n. Defacing *(Bij defacing veranderen cybercriminelen de content: bijvoorbeeld door de homepage van je website aan te passen.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van defacing en heb hier schade aan ondervonden
- O Ik heb wel eens met defacing te maken gehad, maar heb kunnen voorkomen dat er schade gemaakt kon worden
- O Ik heb wel eens geprobeerd om iemand te defacen
- O Ik doe regelmatig aan defacing
- O Anders, namelijk: _____

18o. Password cracking (*Criminelen achterhalen je wachtwoorden om vervolgens in te breken op je computer, telefoon en/of netwerk.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van password cracking en heb hier schade aan ondervonden
- O Ik ben wel eens slachtoffer geweest van password cracking, maar heb kunnen voorkomen dat er schade gemaakt kon worden
- O Ik heb wel eens geprobeerd om te password cracken
- O Ik doe regelmatig aan password cracking
- O Anders, namelijk: _____

18p. Cyberafpersing (*Zodra hackers toegang hebben tot het digitale netwerk starten zij met het afpersen van de organisatie of een persoon. Je krijgt pas weer toegang tot de computer(s) of telefoon(s) zodra er geld betaald is.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van cyberafpersing en heb hier schade aan ondervonden
- O Ik ben wel eens slachtoffer geweest van cyberafpersing, maar heb kunnen voorkomen dat er schade gemaakt kon worden
- O Ik heb wel eens iemand afgeperst via het internet
- O Ik doe regelmatig aan cyberafpersing
- O Anders, namelijk: _____

18q. Cyberstalking (*Deze vorm van cybercrime komt vaak voor bij individuen: via digitale kanalen word je stelselmatig lastiggevallen.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van cyberstalking en heb hier schade aan ondervonden

- O Ik ben wel eens slachtoffer geweest van cyberstalking, maar heb kunnen voorkomen dat er schade gemaakt kon worden
- O Ik heb wel eens iemand gestalkt via het internet
- O Ik doe regelmatig aan cyberstalking
- O Anders, namelijk: _____

18r. Cyberpesten *(Pesten via het internet of een mobiele telefoon.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geweest van cyberpesten en heb hier schade aan ondervonden
- O Ik ben wel eens slachtoffer geweest van cyberpesten, maar heb de pesters geblokkeerd en heb hier geen schade aan ondervonden
- O Ik heb wel eens iemand gepest via het internet of de mobiele telefoon
- O Ik doe regelmatig aan cyberpesten
- O Anders, namelijk: _____

18s. Kinderporno *(Het gaat hierbij om mensen die foto's en video's op internet zetten van kinderen jonger dan 18 jaar die seksuele handelingen verrichten, seksueel poseren of zich in een seksueel getinte omgeving bevinden.)*

- O Ik heb hier niet mee te maken gehad
- O Ik ben wel eens slachtoffer geworden van kinderporno en heb hier schade aan ondervonden
- O Ik ben wel eens benaderd voor kinderporno, maar ben hier niet op ingegaan
- O Ik kijk wel eens naar kinderporno
- O Ik kijk regelmatig naar kinderporno en werk mee aan de productie van kinderporno
- O Anders, namelijk: _____

19. Ben je bang om (nog een keer) slachtoffer te worden van cybercriminaliteit? Waarom?

_____

20. Hebben kennissen van jou wel eens geprobeerd om een cybercrime te plegen? Zo ja, om welke cybercrime ging het?

_____

21. Hebben leeftijdsgenoten of vrienden van jou wel eens geprobeerd om een cybercrime te plegen? Zo ja, om welke cybercrime ging het?

_____

22. Heeft een kennis of vriend jou wel eens gevraagd of geprobeerd over te halen om mee te doen met (activiteiten die kunnen leiden tot) cybercrime? Zo ja, welke? En waarom heb je hieraan wel of niet meegedaan?

_____

23. Geef aan in hoeverre je het eens bent met de volgende stellingen:

23a. Ik maak mij weinig zorgen over de toekomst

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23b. Ik leef bij de dag

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23c. Ik kan moeilijk verleidingen weerstaan

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23d. Ik geef meer geld uit dan ik eigenlijk zou moeten doen

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23e. Ik stel een budget op voor een bepaalde periode

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23f. Ik houd bij mijn aankopen rekening met mijn budget

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

23g. Ik kan mijzelf vertrouwen als het gaat om mijn uitgaven

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24. Geef aan in hoeverre je het eens bent met de volgende stellingen:

24a. Slechte gewoontes leer ik moeilijk af.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24b. Ik ben eerder lui.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24c. Ik zeg soms ongepaste dingen.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24d. Ik doe soms dingen die slecht voor me zijn, gewoon omdat ik ze leuk vind.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24e. Ik weiger dingen die slecht voor me zijn.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24f. Ik zou willen dat ik meer zelfdiscipline had.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

18g. Ik kan gemakkelijk verleidingen weerstaan.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24h. Mensen vinden dat ik veel zelfdiscipline heb.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24i. Plezier en amusement zorgen er soms voor dat ik niet aan werken toekom.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24j. Ik kan me moeilijk concentreren.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24k. Ik kan effectief toewerken naar lange termijn doelstellingen.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24l. Soms kan ik het niet laten bepaalde dingen te doen, ook al weet ik dat ze verkeerd zijn.

o	o	o	o	o	o	o
helemaal niet mee eens						helemaal mee eens

24m. Ik doe vaak dingen zonder eerst alle alternatieven te overwegen.

o	o	o	o	o	o	o
helemaal						helemaal

niet mee eens mee eens

25. Geef aan in hoeverre je het eens bent met de volgende stellingen.

25a. Ik voel mij verbonden met de buurt waarin ik woon.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25b. In mijn buurt zijn er gedeelde waarden en normen (dingen die we allemaal belangrijk vinden en regels waar we ons allemaal aan houden).

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25c. In mijn buurt wijzen we elkaar erop als we iets verkeerd doen.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25d. In mijn buurt letten we op elkaar en houden we elkaar veilig.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25e. In mijn buurt kent bijna iedereen elkaar.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25f. In mijn buurt zeggen we gedag als we een buurman of buurvrouw tegenkomen.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25g. In mijn buurt praten we veel met de mensen die in de buurt wonen.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25h. Ik voel me thuis in mijn buurt.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

25i. In mijn buurt wonen veel mensen zoals ik.

o o o o o o o

helemaal helemaal

niet mee eens mee eens

25j. In mijn buurt wonen mensen met dezelfde interesses als ik.

o o o o o o o

helemaal helemaal
niet mee eens mee eens

Bedankt voor het invullen van de enquête!

Ik wil je graag bedanken voor het invullen van de enquête door je de kans te bieden om een Bol.com cadeaubon t.w.v. €25,- te winnen! Als je kans wil maken, wil ik je vragen om je e-mailadres in te vullen via de volgende link. Dit is een aparte link om te zorgen dat jouw antwoorden op geen enkele manier te herleiden zijn tot jouw e-mailadres.
https://docs.google.com/forms/d/e/1FAIpQLSeTpqcpGyo33EVPV-EFQ8e8FG_99wZjYfuEadOnnLCsH017cQ/viewform?usp=sf_link.

Mocht je nog vragen of opmerkingen hebben naar aanleiding van de enquête, kun je contact opnemen.
T 06-39237201
E l.tuk@students.uu.nl

Als je slachtoffer bent geweest van cybercriminaliteit en je wilt aangifte doen, kan dat via het algemene nummer van de politie. Als je aangifte doet, krijg je slachtofferhulp aangeboden.
Politie: 0800 8844

Bijlage 2: Resultaten regressieanalyse interactievariabelen en mediatievariabelen

Tabel 8. Resultaten meervoudige regressie met interactievariabelen (slachtofferschap).

	Algeheel slachtofferschap				Slachtofferschap gedigitaliseerde criminaliteit				Slachtofferschap cybercriminaliteit			
Variabele	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**
			.043	1.757			.108	3.027			.214	5.564
Sociale kwetsbaarheid	-.227*	-2.916			.128	-.787			.122	.556		
Impulsiviteit (tegenover zelfcontrole)	-.246	-1.042			-.015	-.040			.938	1.888		
Sociale kwetsbaarheid * impulsiviteit	.051	1.827			.020	.458			-.061	-1.033		
Rotterdam-Zuid	.377	1.338			1.464***	3.333			2.416***	4.084		
			.068	1.151 (n.s.)			.126	3.411			.189	4.902
Sociale kwetsbaarheid	-.029	-.289			.084	.549			-.331	-1.565		
Sociale cohesie	.047	.283			.408	1.595			-.326	-.924		
Sociale kwetsbaarheid * sociale cohesie	-.006	-.249			-.030	-.877			.051	1.080		
Rotterdam-Zuid	.574*	2.082			1.626***	3.883			2.328***	4.022		
			.034	1.588			.107	2.993			.189	4.911
Sociale kwetsbaarheid	-.022	-.233			-.119	-.813			-.316	-1.584		
Internetvaardigheden	.168	1.156			-.011	-.049			-.251	-.814		
Sociale kwetsbaarheid * Internetvaardigheden	-.005	-.271			.013	.429			.044	1.076		
Rotterdam-Zuid	.639*	2.341			1.592***	3.744			2.389***	4.110		
			.009	1.147 (n.s.)			.104	2.994			.202	5.251
Sociale kwetsbaarheid	-.058	-.621			-.042	-.291			.206	1.057		
Financiële impulsiviteit	.011	.053			-.030	-.089			.851	1.882		
Sociale kwetsbaarheid * Financiële impulsiviteit	.001	.051			-.006	-.166			-.090	-1.761		
Rotterdam-Zuid	.552*	1.974			1.610***	3.727			2.432***	4.174		
			.015	1.256 (n.s.)			.158	4.134			.197	5.125
Sociale kwetsbaarheid	-.046	-1.343			-.045	-.861			-.078	-1.086		
Differentiële associatie	.610	.871			2.316*	2.202			2.413	1.640		

door kennissen												
Sociale kwetsbaarheid * Differentiële associatie	-.038	-.490			-.085	-.721			-.241	-1.466		
Rotterdam-Zuid	.495	1.743			1.217***	2.873			2.263***	3.814		
			.018	1.306 (n.s)			.132	2.541			.215	5.582
Sociale kwetsbaarheid	-.045	-1.271			-.044	-.809			-.056	-.754		
Differentiële associatie door leeftijdsgenoten	.481	.845			1.152	1.340			2.653*	2.266		
Sociale kwetsbaarheid * Differentiële associatie	-.022	-.307			-.027	-.256			-.218	-1.496		
Rotterdam-Zuid	.473	1.655			1.274***	2.921			2.095***	3.520		

Noot: N=161, *p <.05, **p <.02, ***p <.01

Tabel 9. Resultaten meervoudige regressie met interactievariabelen (daderschap).

	Algeheel daderschap				Daderschap gedigitaliseerde criminaliteit				Daderschap cybercriminaliteit			
Variabele	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**	**B**	**t**	**R^2**	**F**
			.150	3.956			.190	4.938			.066	2.185
Sociale kwetsbaarheid	-.101	-1.537			.-.061	-1.608			-.090	-1.056		
Impulsiviteit (tegenover zelfcontrole)	-.047	-.316			-.112	-1.295			-.076	-.392		
Sociale kwetsbaarheid * impulsiviteit	.032	1.785			.027***	2.642			.020	.864		
Opleidingsniveau	-.135***	-2.648			-.031	-1.032			-.217***	-3.269		
Migratieachtergrond	.367*	2.251			.189*	1.989			.129	.604		
Leeftijd	.121	1.231			.015	.254			.289*	2.244		
			.085	2.559			.122	3.329			.062	2.113
Sociale kwetsbaarheid	.050	.779			.060	1.583			.034	.412		
Sociale cohesie	.081	.750			.055	.871			.060	.444		
Sociale kwetsbaarheid * sociale cohesie	-.012	-.798			-.007	-.811			-.014	-.790		
Opleidingsniveau	-.150***	-2.829			-.039	-1.260			-.231***	-3.446		
Migratieachtergrond	.403**	2.370			.199*	2.006			.117	-.790		
Leeftijd	.134	1.318			.018	.306			.288*	2.239		
			.144	2.662			.122	3.341			.070	2.265
Sociale kwetsbaarheid	.047	.764			.022	.613			-.028	-.362		
Internetvaardigheden	.104	1.112			.010	.185			.071	.599		
Sociale kwetsbaarheid * Internetvaardigheden	-.009	-.754			.002	.276			.002	.117		
Leeftijd	.128	1.207			.031	.494			.320**	2.396		
Opleidingsniveau	-.147***	-2.782			-.040	-1.286			-.229***	-3.450		
Migratieachtergrond	.420**	2.514			.218*	2.226			.156	.743		
			.173	4.510			.202	5.240			.077	2.390
Sociale kwetsbaarheid	-.092	-1.607			-.050	-1.494			-.087	-1.153		
Financiële impulsiviteit	.015	.110			-.070	-.910			-.015	-.088		
Sociale kwetsbaarheid * Financiële impulsiviteit	.026	1.753			.023**	2.560			.018	.900		

Opleidingsniveau	-.133***	-2.643			-.029	-.976			-.214***	-3.239		
Leeftijd	.133	1.369			.018	.316			.291*	2.281		
Migratieachtergrond	.402**	2.257			.196*	2.105			.133	.636		
			.098	2.828			.121	3.299			.099	2.848
Sociale kwetsbaarheid	.012	.553			.033**	2.525			-.002	-.059		
Differentiële associatie door kennissen	.741	1.653			.194	.737			1.455***	2.605		
Sociale kwetsbaarheid * Differentiële associatie	-.068	-1.363			-.018	-.594			-.138*	-2.215		
Migratieachtergrond	.420**	2.503			.211*	-.594			.137	.655		
Opleidingsniveau	-.147***	-2.806			-.037	-1.217			-.223***	-3.426		
Leeftijd	.120	1.179			.015	-1.685			.259*	2.042		
			.092	2.692			.119	3.257			.085	2.552
Sociale kwetsbaarheid	.012	.534			.033**	.573			-.005	-.172		
Differentiële associatie door leeftijdsgenoten	.458	1.265			.103	.484			.850	1.877		
Sociale kwetsbaarheid * Differentiële associatie	-.042	-.942			-.012	-.435			-.063	-1.121		
Migratieachtergrond	.418**	2.498			.213*	2.171			.119	.569		
Opleidingsniveau	-.140***	-2.667			-.036	-1.169			-.211***	-3.196		
			.056	3.980			.126	8.287			.008	1.384
Sociale kwetsbaarheid	-.161	-1.726			-.085	-1.602			-.172	-1.447		
Strain	-.038	-.838			-.033	-1.263			-.043	-.734		
Sociale kwetsbaarheid * Strain	.009	1.934			.006*	2.254			.009	1.453		

Noot: N=161, *p <.05, **p <.02, ***p <.0

Tabel 10. Resultaten meervoudige regressie mediatievariabelen.

Afhankelijke variabele:	**Strain**				**Differentiële associatie**				**Tijdsbesteding**				**Migratieachtergrond**			
			.747	64.812			.176	5.610			.049	2.107			.284	10.978
Sociale kwetsbaarheid	.468***	9.370			-.003	-.459			-.121***	-2.986			.020	1.912		
Opleidings-niveau	-.917***	-7.252			.000	.983			-.056	-.548			-.020	-.751		
Arbeidsstatus	-1.354***	-12.357			.036*	2.275			.034	.386			-.046*	-2.074		
Rotterdam-Zuid	.761	1.806			.201***	3.338			.580	1.693			.471***	6.030		
Leeftijd	-.044	-.182			.019	.544			.204	1.025			.100*	1.990		

Noot: N=161, *p <.05, **p <.02, ***p <.01

Bijlage 3: Topiclijst interviews

Topiclijst interviews Masterscriptie Cybercrime

1. Belang van cybercrime voor organisatie
2. Cybercrime in Zuid
3. Achterstanden als verklaringen voor cybercrime
4. Perspectief cybercrime
5. Huidig beleid
6. Toekomstig beleid
7. Kennisbehoefte
8. Interesse cirkelcoalitie cybercrime in Rotterdam
9. Andere belangrijke partijen die een interessant perspectief zouden kunnen bieden

Bijlage 4: Codeboom