Radboud Universiteit Nijmegen

Faculteit der Managementwetenschappen

Het vermogen om cyberslachtoffer te worden

Een onderzoek naar de relatie tussen iemands financiële positie en diens kans om slachtoffer te worden van cybercriminaliteit

Masterthesis Bestuurskunde - Besturen van Veiligheid

Auteur:
T. Klaassen

Begeleider:
Dr. G.J. Brandsma

Tweede Lezer:
Dr. S.C.H. André

Juli 2022

In opdracht van politiedistrict Gelderland-Midden

Voorwoord

Geachte lezer,

Met deze thesis komt een einde aan een vierjarig studietraject Bestuurskunde aan de Radboud Universiteit te Nijmegen. Na dit laatste masterjaar 'Besturen van Veiligheid' kan ik mij geen passendere afsluiting inbeelden, dan een beleidsadvies te schrijven voor de altijd even hartelijke mensen van politiedistrict Gelderland-Midden; nota bene op basis van eigen onderzoek. Een onderzoek met een heldere bestuurskundige aanleiding en relevantie, maar dat ook een duidelijke (digitaal-)criminologische zijde kent. Derhalve reflecteert het mijn eigen (extracurriculaire) kennisontwikkeling van de afgelopen vier jaar.

Hoewel het afgelopen halfjaar zoals te verwachten de gebruikelijke pieken en dalen heeft gekend, is voor mij de relevantie van - en motivatie voor - deze scriptie altijd onverminderd groot gebleven. Dit heeft van begin tot eind geresulteerd in een sterk gevoel van eigenaarschap, dat in geen kleine mate gefaciliteerd is door de mensen die mij in dit proces hebben begeleid. De geboden ruimte voor zelfstandigheid en het uitgesproken vertrouwen, vanuit zowel de universiteit (de heer Brandsma) als de politie, leidde ertoe dat mij geen strobreed in de weg is gelegd om uiteindelijk een *eigen* thesis te kunnen presenteren.

Mijn dank hiervoor is vanzelfsprekend groot. Evenals mijn dank voor mijn vriendin, met wie ik altijd mijn positieve en negatieve ervaringen kon delen. De gastvrije mensen van het OCP op de afdeling van de districtsrecherche wil ik bedanken voor de geboden werkruimte, de getoonde interesse en de inkijk in hun fascinerende werk. Mijn medestudenten bij de politie wil ik bedanken voor de wederzijds geboden uitlaatklep, en natuurlijk ook de sfeer. Afsluitend wil ik mijn dankbaarheid uitspreken voor de vierhonderd onbekende passanten die wél bereid waren deel te nemen aan dit onderzoek. Hun inzet is hetgeen waar de inhoudelijk toegevoegde waarde van deze scriptie uiteindelijk in de fundatie (mede) op berust.

Ik wens u veel leesplezier.

Tim Klaassen

19-7-2022

INHOUDSOPGAVE

1. INLEIDING

Over de afgelopen tien jaar is een trend in de criminaliteitscijfers zichtbaar geworden: er vindt een verschuiving plaats van 'traditionele' delicten, naar delicten in het digitale domein. Het CBS (2022[a]) meldt namelijk over de afgelopen tien jaar een gestage daling van het traditionele type delicten, terwijl over dezelfde tijdspanne een gestage toename van online criminaliteit zichtbaar is. Vooral de cijfers over 2020 vertonen een scherpe daling van traditionele criminaliteit (CBS, 2021[a]). Hoewel het CBS geen harde uitspraken doet over de destijds voor het eerst geïntroduceerde coronamaatregelen als oorzaak voor deze daling, is dit verband wel aannemelijk gezien het bemoeilijkte klimaat voor traditionele gelegenheidscriminelen.

Het vermogen tot opsporing en afhandeling van digitale criminaliteit raakt echter achter op de groei die de gedigitaliseerde criminaliteit doormaakt. Het Openbaar Ministerie (2021) erkent dat techniek, wetgeving en organisatie achterlopen op de werkelijkheid in de bestrijding van gedigitaliseerde criminaliteit. Ook concluderen Helsloot en Groenendaal (2014) dat de politie in de bestrijding van cybercrime opereert vanuit een beperkte informatiepositie. De politie zou voor de aanpak van cybercrime niet de juiste expertise in de organisatie aanwezig hebben (Schuilenburg, Besseling & Uitendaal, 2017).

Met de achterblijvende ophelderingscijfers voor gedigitaliseerde criminaliteit, wordt het gezegde 'voorkomen is beter dan genezen' daardoor steeds relevanter. Door in te zetten op preventie tracht men dan ook vooraf digitale criminaliteit te dwarsbomen, in plaats van het nastreven van ophelderingsmaximalisatie achteraf (Boekhoorn, 2019). Weerbaarheid van burgers en organisaties tegen gedigitaliseerde criminaliteit is daarmee een nieuw hoofddoel geworden.

Vanuit politiedistrict Gelderland-Midden (en de driehoek) ervaart men echter dat de signalen die zij uitzenden over de gevaren van cybercrime en gedigitaliseerde criminaliteit geen merkbaar preventieve werking hebben. Een verklaring hiervoor is dat het stimuleren van cyberweerbaarheid onder burgers via toespitsing op specifieke doelgroepen met een verhoogd risico op slachtofferschap dient plaats te vinden (Spithoven, Foppen, Van Houten & Misana-Ter Huurne, 2020). Maatwerk per doelgroep dus, in tegenstelling tot de huidige, meer ongerichte communicatie jegens de gehele samenleving (Politie, 2022).

Het identificeren van doelgroepen met een verhoogd risico op slachtofferschap van cybercrime of gedigitaliseerde criminaliteit is echter geen eenvoudige opgave. De wetenschappelijke literatuur over cybercrime-slachtofferschap kent namelijk een hoge mate van ambiguïteit (Van 't Hoff-De Goede, Leukfeldt, Van der Kleij & Van de Weijer, 2021). Gebruikte onderzoeksmethoden en de afbakeningen van de begrippen als cybercrime en gedigitaliseerde criminaliteit spelen daarin een vertroebelende rol. Zo kennen de onderzoeksresultaten van het CBS (2019[a]) en Fawn Ngo & Raymond Paternoster (2011) tegenstrijdige uitslagen wat betreft de relatie tussen leeftijd en cyberslachtofferschap, en

geslacht en cyberslachtofferschap. Daarnaast stellen Spithoven et al. (2020) dat de factor aangiftebereidheid het slachtofferbeeld verder vervaagt, omdat deze aan de lage kant is (Van de Weijer, Leukfeldt & Van der Zee, 2020[a]). Een vignettenstudie die zich specifiek richtte op aangiftebereidheid bij verschillende typen cybercrime kwam zelfs tot de conclusie dat er sprake was van een zogenoemde *intention-behaviour gap*; waarbij respondenten desgevraagd aangaven in bepaalde omstandigheden wel degelijk aangifte te zullen doen van cybercrime, maar dat deze theoretische bereidheid in de praktijk niet terug te zien is (Leukfeldt, Van de Weijer & Van der Zee, 2020[b]).

Een relatie (en bijbehorende doelgroep) die – bij gebrek aan beter weten van de auteur – echter relatief buiten het aandachtsveld van toegewijd internationaal slachtofferonderzoek bij cybercrime blijft, is die tussen de financiële positie (FP) van een individu en diens kans om slachtoffer te worden van cybercrime. Onterecht, aangezien bij traditionele criminaliteit wel degelijk een negatief verband bestaat tussen welvaart en blootstelling aan criminaliteit (Nilsson & Estrada, 2006). Of zoals Thacher (2004, p.89) de situatie in de Verenigde Staten na vergelijkbaar onderzoek betitelt: *"The rich get richer and the poor get robbed"*. Daarnaast is er ook statistische aanleiding om deze relatie nader te onderzoeken, en individuen met een slechte FP als een mogelijke doelgroep te beschouwen. Mensen met een laag inkomen zouden in Nederland namelijk vaker slachtoffer zijn van cybercrime (*hacking* en cyberpesten) dan hogere inkomens, waarvan mensen met een 'langdurig' laag inkomen nóg weer vaker slachtoffer van cybercrime zouden zijn (CBS[b], 2019). Met de verschuiving van traditionele criminaliteitsvormen naar digitale criminaliteitsvormen, lijkt de negatieve relatie tussen financieel welzijn en slachtofferschap zodoende (in ieder geval ten dele) mee te verschuiven.

Bovendien is in termen van objectieve veiligheid, de groep mensen met een relatief moeilijke FP het meest relevant voor veiligheidsbevordering. Persoonlijke welvaart en levensverwachting vertonen immers een sterk positief verband, waardoor enige pogingen tot bevordering van de collectieve objectieve veiligheid (uitgedrukt in gemiddelde levensverwachting) het meest doeltreffend zijn indien de Nederlanders die financieel het slechtst af zijn, de beleidsprioriteit krijgen (Helsloot, Pieterman & Hanekamp, 2010). Omdat verschillende uitingen van cybercrime kunnen leiden tot uiteenlopende emotionele en materiële gevolgen voor de slachtoffers (Leukfeldt, Notté & Malsch, 2018), zouden de consequenties van slachtofferschap voor mensen wiens FP reeds fragiel is, des te omvangrijker kunnen zijn. De combinatie van het mechanisme tussen welvaart, levensverwachting en objectieve veiligheid, tezamen met de mogelijke fragiliteit van individuen die financieel al slechter af zijn, maakt zodoende de groep mensen met een laag financieel welzijn tot een relevante onderzoeksgroep voor dit onderzoek.

Om echter tot wetenschappelijk gefundeerde cyberweerbaarheidsinterventies voor deze doelgroep te kunnen komen; en een bijdrage te leveren aan de wetenschappelijke

literatuur wat betreft de relatie tussen de verhoogde cyberslachtofferschapskans voor mensen met een laag financieel welzijn; dient nader onderzoek te worden verricht. Hierom is voor deze thesis de volgende doelstelling geformuleerd: “Het verifiëren van de relatie tussen iemands financiële positie (FP) en diens kans op slachtofferschap van cybercrime (*hacking* en cyberpesten), evenals welke causale mechanismen hierin een rol spelen; teneinde tot concrete en gefundeerde beleidsmaatregelen te kunnen komen waarmee politiedistrict Gelderland-Midden (en de driehoek) de cyberweerbaarheid van de beoogde doelgroep kan stimuleren”. Om deze doelstelling te bereiken, is de volgende centrale kennisvraag geformuleerd: “Wat is het effect van iemands financiële positie (FP) op de kans op slachtofferschap van cybercrime (*hacking* en cyberpesten) en welke causale mechanismen spelen hierin een rol?”. Dit onderzoek is verricht in het gebied dat politiedistrict Gelderland-Midden behelst.

Om tot een antwoord op deze centrale vraagstelling te komen, is deze thesis als volgt opgebouwd. Om te beginnen presenteert het theoretische kader de verbanden die dit onderzoek verwacht aan te treffen op basis van een verkenning van de literatuur. Het theoretisch kader verschaft ook enkele bijbehorende definities. Vervolgens gaat het methodologisch kader in op de operationalisatie van de beoogde concepten uit het conceptueel model; omschrijft het de details rondom de methoden van dataverzameling en -analyse die voor dit onderzoek gehanteerd zullen worden; en wordt de keuze voor deze methoden onderbouwd. Daarna worden in het hoofdstuk ‘analyse’ de resultaten van de dataverzameling gepresenteerd, evenals wat deze resultaten impliceren voor de opgestelde hypothesen. Afsluitend volgt een concluderend hoofdstuk, waarin niet alleen de centrale vraagstelling ter sprake komt, maar ook een discussie wordt gepresenteerd waarin de beperking van dit onderzoek staan vermeld, tezamen met aanbevelingen voor toekomstig onderzoek binnen dit thema.

2. THEORETISCH KADER

Om tot inhoudelijk gedegen en samenhangend preventief beleid op het gebied van cybercriminaliteit te komen, passeert dit hoofdstuk eerst in relatieve vogelvlucht de relevante literatuur uit de traditionele en modernere (deels gedigitaliseerde) criminologie. Zodoende komt dit hoofdstuk tot een conceptueel model, passend bij de centrale vraagstelling. Het traditionele criminologisch perspectief biedt ter fundatie een aantal risicofactoren die bijdragen aan de relatie tussen iemands FP enerzijds en slachtofferschap van inbraak en geweld anderzijds. Vervolgens biedt de moderne empirie inzichten over welke aspecten van traditioneel slachtofferschap in relatie met iemands FP zich laten vertalen naar slachtofferschap van *hacking* en cyberpesten in het digitale domein. Waar deze vertaalslag mogelijk blijkt, zullen bijbehorende hypothesen worden geformuleerd. Het hoofdstuk mondt uit in een samenvattende figuur waarin het conceptueel model met alle hypothesen is uitgebeeld.

2.1 De oorsprong van de relatie tussen FP en slachtofferschap van (cyber)criminaliteit

In de wetenschappelijke literatuur over slachtofferschap van traditionele criminaliteit is de relatie tussen iemands FP en diens kans om slachtoffer te worden reeds extensiever belicht dan bij cybercriminaliteit. Hoewel dat tot gevolg heeft dat er geen directe theoretische onderbouwing voor de relatie tussen iemands FP en kans op slachtofferschap van cybercriminaliteit in de literatuur bestaat, is er wel aanleiding om via een indirecte weg – de literatuur over traditionele criminaliteit – tot een theoretische afbakening te komen. Er zijn namelijk opvallende hypothetische paralellen te trekken tussen bepaalde typen traditionele criminaliteit, waarbij iemands FP negatief verband houdt met diens kans op slachtofferschap, en bepaalde hedendaagse typen cybercriminaliteit die eenzelfde verband lijken te vertonen. Ofwel, hoe beperkter iemands FP is, hoe groter diens kans is om slachtoffer te worden van bepaalde vormen van traditionele criminaliteit. De wetenschappelijke literatuur wijst hierbij in het bijzonder op het verband tussen iemands FP en diens kans op slachtofferschap van inbraak, diefstal, geweld en bedreiging (Kingston & Webster, 2015; Levitt, 1999; Nilsson & Estrada, 2006).

Door deze verbanden binnen de traditionele criminaliteit te vergelijken met cijfers over cybercriminaliteit in Nederland, ontstaat een interessante parallel: in 2019[b] presenteerde het CBS namelijk data waaruit blijkt dat mensen met een laag inkomen vaker slachtoffer zijn van *hacking* en cyberpesten. Voor mensen met een langdurig laag inkomen is dit effect nog sterker. Een opvallende statistiek, gegeven de aard van deze typen cybercriminaliteit in vergelijking met de traditionele criminaliteitsvormen inbraak, diefstal, geweld en bedreiging waar mensen

met een slechte FP bewezen vaker slachtoffer van worden. Het CBS (2019[c]) definieert *hacking* namelijk als "Bij hacken is er met kwade bedoelingen ingebroken of ingelogd op iemands computer, mobiele telefoon, e-mailaccount, socialenetwerksite of een ander online account"; en definieert cyberpesten (2016) als "Roddel, getreiter, pesten, stalken, chantage of bedreiging via internet". Ofwel, traditionele inbraak en *hacking* (digitale inbraak) kennen beiden een verband met iemands FP, evenals traditionele bedreigingen en geweld, en cyberpesten.

Toegegeven zijn traditionele bedreigingen en geweld enerzijds, en cyberpesten anderzijds in hun aard enigszins minder conceptueel overeenkomstig dan inbraak en *hacking* dat zijn. Fysieke vormen van mishandeling zijn in het digitale domein immers uitgesloten, waardoor cyberpesten nooit de exacte aard, eigenschappen en gevolgen van daadwerkelijk traditioneel fysiek geweld zal kennen. Desondanks dient niet te worden vergeten dat de delicten die het CBS (2016) schaart onder cyberpesten, in het digitale domein het maximaal haalbare zijn om een ander individu in enige vorm (emotioneel) te mishandelen. De term 'pesten' in het woord 'cyberpesten' acht deze thesis dan ook als een bagatellisering van de realiteit, zeker gezien de ernst van de eerdergenoemde definitie die het CBS ervoor hanteert.

Bovendien is in deze definitie de term 'pesten' opgenomen als een van de uitingen van cyberpesten, wat leidt tot circulariteit tussen het begrip en de bijbehorende definitie. Wall (2001) gebruikt voor vergelijkbare digitale vergrijpen die het CBS in haar definitie van cyberpesten heeft opgenomen dan ook de term *cyberviolence*. Dus hoewel deze thesis zijn bestaansrecht mede ontleent aan de data van het CBS, en daarmee ook de door het CBS gehanteerde definities van *hacking* en cyberpesten dienen te worden toegepast, zal vanaf dit punt de term 'cyberagressie' worden gebruikt om de CBS-definitie van cyberpesten te omvatten. Daarmee is de parallel die deze thesis trekt tussen traditioneel geweld en bedreigingen enerzijds, en cyberpesten (cyberagressie) anderzijds ook op een tekstueel niveau helderder. De herbenoeming van cyberpesten tot cyberagressie gebeurt echter enkel binnen de redeneer- en analysekaders van deze thesis; indien een bron spreekt over cyberpesten, zal dit vanzelfsprekend ook als zodanig worden geparafraseerd.

Hypothese 1: Er bestaat een negatief verband tussen iemands financiële positie (FP) en diens kans om slachtoffer te worden van cybercriminaliteit (*hacking* en cyberagressie).

2.2 Het mechanisme achter de relatie tussen FP en slachtofferschap van (cyber)criminaliteit

Hoewel eerder aangehaalde papers de statistische relatie tussen FP en slachtofferschap van inbraak, geweld en bedreiging bevestigen, blijft er gegeven de kwantitatieve aard van deze onderzoeken onzekerheid over het mechanisme achter deze statistische relatie. De relatie

tussen armoede en slachtofferschap is niet altijd een directe; maar tegelijkertijd verhoogt het leven in armoede de kans op slachtofferschap wel aanzienlijk, blijkt uit literatuuronderzoek van Kingston en Webster (2015).

De paralellen in slachtofferdata tussen traditionele criminaliteit en cybercriminaliteit bieden echter aanleiding om perspectieven op slachtofferschap van traditionele criminaliteit uit de criminologische literatuur nader te bekijken. Hierin zijn *opportunity*-theorieën prominent als het aankomt op de positie en rol van potentiële slachtoffers als verklaring voor criminaliteit, wat tevens een fundatie biedt voor preventieve maatregelen die de burger zelf kan nemen. Hoewel *opportunity*-theorieën (*rational choice theory* & *routine activity theory*) onderling enigszins variëren van visie, is de hoofdgedachte van dit type criminologische theorieën dat een samenkomst van omstandigheden leidt tot een misdrijf, en daarmee gepaard slachtofferschap (Lanier, Henry & Anastasia, 2015). Criminaliteit-preveniërend beleid dat wordt gebaseerd op dit type theorieën berust dan ook in de gedachte dat de opportuniteitsstructuur in een bepaalde omgeving gemanipuleerd kan worden, waardoor de omstandigheden voor het plegen van een delict minder gunstig worden (Lanier et al., 2015). Dit proces heet ook wel *target hardening* (Gooch & Williams, 2007).

De connectie tussen dit soort *opportunity theories* en sociale ongelijkheid is reeds onderzocht. Lawrence Cohen, James Kluegel en Kenneth Land (1981) bieden een framework van mediërende risicofactoren die verband houden met enerzijds enkele dimensies van sociale stratificatie: inkomen, ras en leeftijd; en anderzijds de kans op slachtofferschap van inbraak, diefstal en geweld. De betreffende mediërende factoren die zij presenteren zijn *exposure, guardianship, proximity to potential offenders, attractiveness of potential targets* en *definitional properties of specific crimes*. Cohen et al. (1981) tonen het verband tussen inkomen en deze mediërende factoren aan, in het nadeel van de minderbedeelden, waardoor ook een potentieel mechanisme achter het slachtofferschap van deze groep in beeld komt.

Bovendien wordt met de toenemende hegemonie van het internet door criminologen ondertussen een vertaalslag gemaakt tussen deze traditionele *opportunity*-theorieën naar moderne cybercrime. Hoewel het bewijs niet geheel eenduidig is, en het debat over de toepasbaarheid van *opportunity*-theorieën in het cyberdomein zeker leeft, zouden criteria voor misdaaduitingen die *opportunity*-theorieën presenteren wel degelijk toepasbaar zijn in het digitale domein (Henson, 2020). Referend naar de drie pijlers van de *routine activity theory*, stelt Grabosky (2001, p.248) dan ook: "*One of the basic tenets of criminology holds that crime can be explained by three factors: motivation, opportunity, and the absence of a capable guardian. This explanation can apply to an individual incident as well as to long-term trends. Derived initially to explain conventional 'street' crime, it is equally applicable to crime in cyberspace*".

Deze thesis volgt deze lijn, en neemt zodoende primair aan dat elementen van *opportunity theories* toepasbaar zijn in het digitale domein. Of deze aanname ook verdere theoretische en empirische steun kent, zal dadelijk uitgebreid uiteen worden gezet. De reeds geïntroduceerde mediërende risicofactoren tussen inkomen en slachtofferschap van Cohen et al. (1981) dienen hiervoor als basis. Elk van deze factoren wordt beknopt uiteengezet, beoordeeld op de mate waarin deze zich over laat hevelen naar het digitale domein en daarmee getoetst op geschiktheid voor gebruik in deze thesis; beginnend met *exposure*.

De risicofactor *Exposure* (Cohen et al., 1981) gaat uit van de gedachte dat een gemotiveerde dader in contact moet komen met (de eigendommen van) een potentieel slachtoffer om een misdrijf te laten plaatsvinden. Hoe vaker dit gebeurt, hoe meer gelegenheden er zijn voor een dader om een misdrijf te begaan. Hoewel in het cyberdomein niet langer per se het kruisen van tijd en plaats tussen dader en slachtoffer hoeft plaats te vinden zoals dat in de theorie van Cohen et al. (1981) wordt gesteld (Henson, 2020), valt te beredeneren dat een hogere mate van online aanwezigheid leidt tot een hogere *exposure* aan cybercrime. Recent onderzoek naar slachtofferschap in het digitale domein toont echter aan dat variaties in de hoeveelheid tijd die men online spendeert geen significant verschil maken in de kans op slachtofferschap, afgezien van een uitzondering voor 'ongewenste blootstelling aan pornografie' (Ngo, Piquero, LaPrade & Duong, 2020). Daarnaast zou beredeneerd kunnen worden dat zodra iemand een apparaat verbindt met het internet, deze persoon automatisch in de basis al een minimum hoeveelheid *exposure* kent, waardoor vrijwel elke gebruiker van moderne techniek ongeacht FP om deze reden slachtoffer kan worden. Om deze redenen zal deze factor dan ook niet worden meegenomen in het huidige onderzoek.

De tweede factor, *guardianship*, is daarentegen een belangrijke. *Guardianship* als factor is gebaseerd op de gedachte dat – in de traditionele criminologie – de aanwezigheid van personen (zoals huisgenoten) of veiligheidsbevorderende objecten zoals sloten, dichte ramen en alarmsystemen de kans op het voordoen van een misdrijf verlaagt (Miró, 2014). Dit soort maatregelen gaan echter vaak gepaard met kosten, wat als verklaring voor de negatieve relatie tussen inkomen en slachtofferschap die Cohen et al. (1981; Levitt, 1999) vaststellen wordt gegeven.

Zoals de toepassing van *opportunity theories* in het digitale domein met enige discussie gepaard gaat, benoemen Leukfeldt en Yar (2016) dan ook dat *guardianship* gemengde resultaten oplevert in het daadwerkelijk voorkomen van slachtofferschap van cybercrime. Hoewel in ieder geval *hacking* profiteert van *guardianship*; lijkt het erop dat deze preventieve werking vooral afhangt van de menselijke omgang met digitale risico's en in mindere mate van de (vaak geld kostende) technische voorzorgsmaatregelen. Zodoende spreekt de huidige thesis dan ook van 'digitaal *guardianship*': als combinatie van de menselijke omgang met digitale veiligheidsrisico's en het nemen van technische maatregelen in het digitale domein.

Dat het kostenelement van *guardianship* daarmee wellicht ontkracht is, betekent echter dat niet dat de mediërende functie van *guardianship* tussen FP en kans op slachtofferschap van *hacking* en cyberagressie daarmee niet meer het toetsen waard is. De psychologische wetenschappelijke literatuur stelt namelijk dat sociaaleconomische ongelijkheid gepaard kan gaan met verminderde tevredenheid met het leven, riskanter gedrag, en mede daardoor een verhoogde kans op slachtofferschap van criminaliteit (Wolfarth, Winkel, Ybema & Van den Brink, 2001). Ofwel, een verslechterde sociaaleconomische positie kan leiden tot verslechtering van juist dat risico-averse (online) gedrag waar Leukfeldt en Yar (2016) over stellen dat het juist zou moeten bijdragen aan digitaal *guardianship*. Het onderzoek van Leukfeldt en Yar (2016) gaat niet voldoende in op de verschillende elementen van cyberagressie, maar benoemt nog wel dat wederom risicobewust gedrag remmend werkt op de kans op slachtofferschap van *cyberstalking*.

Hypothese 2: er bestaat een positief verband tussen iemands financiële positie (FP) en diens digitale *guardianship*.
Hypothese 3: er bestaat een negatief verband tussen iemands digitale *guardianship* en diens kans op slachtofferschap van *hacking*.
Hypothese 4: iemands digitale *guardianship* vertoont een negatief mediërend verband tussen iemands financiële positie (FP) en diens kans op slachtofferschap van *hacking*.

De derde factor volgens Cohen et al. (1981), *proximity to potential offenders*, behelst de afstand tussen potentiële slachtoffers en gemotiveerde daders, waarbij er een negatief verband zou moeten bestaan tussen de afstand tussen een groep potentiële gemotiveerde daders en slachtoffers enerzijds, en de kans op slachtofferschap anderzijds. Deze risicofactor zie je bijvoorbeeld in de traditionele criminaliteit terug doordat in criminele (vaak armere) buurten de kans op slachtofferschap groter wordt. Deze factor laat zich echter niet eenvoudig overhevelen vanuit de traditionele criminologie naar het digitale domein.

Cybercrime kan, op voorwaarde van een internetverbinding, immers over grote afstanden plaatsvinden. Dat maakt mede dat opsporingsdiensten grote moeite hebben met het traceren en vervolgen van daders. Een individu in Nieuw-Zeeland kan iemand in Arnhem hacken, of zelfs vormen van cyberagressie op die persoon uiten. Een deel van de participanten in de discussie over de ruimtelijkheid in het digitale domein noemt het internet dan ook *'anti-spatial'* (Yar, 2005), een soort virtueel vacuüm waarin 'afstand' eigenlijk geen concept meer is. Yar (2005) zelf zet hiertegenover dat vanwege de fysieke afstanden tussen servers, en de afhankelijkheid van de kwaliteit van de digitale infrastructuur in geografische gebieden er technisch gezien alsnog verschillen ontstaan wat betreft de relatieve *proximity* tussen mensen. Ervan uitgaande dat de welvaart van een land in zijn totaliteit bijdraagt aan de algehele

kwaliteit van de interne digitale infrastructuur; en dat afstanden tussen servers eigenlijk pas op continentaal niveau een beperkende rol qua *proximity* beginnen te spelen; kan deze risicofactor op individueel slachtofferniveau worden losgelaten. Een cybercrimineel kan zich immers alsnog op een ongrijpbaar grote afstand bevinden binnen het welvarende (en kwalitatief sterk gedigitaliseerde) Europa; en de individuele FP van een potentieel slachtoffer brengt geen verandering in de *proximity* tot die crimineel teweeg, wonend in een welvarend land als Nederland. *Proximity to potential offenders* is zodoende geen onderdeel van de analyse in dit onderzoek.

De vierde risicofactor, *attractiveness of potential targets,* van Cohen et al. (1981), omvat het principe dat de mate waarin een persoon of diens eigendommen een aantrekkelijk doelwit zijn, ofwel vanwege materiele waarde, ofwel vanwege de expressieve waarde (criminaliteit omwille van bijvoorbeeld status), medebepalend is voor diens kans op slachtofferschap. Hoe hoger die aantrekkelijkheid is, hoe groter de kans dat die persoon slachtoffer wordt. Cohen et al. (1981) stellen dan ook logischerwijs, dat *target attractiveness* bij mensen met een beperkte FP zodoende geen risicoverhogende rol speelt, uitgaande van instrumentele motieven bij inbraak.

Attractiveness of potential targets bestaat echter niet alleen uit de waarde van een potentieel slachtoffer of diens eigendommen, maar ook de *inertia* of inertie van die eigendommen (Cohen et al., 1981). Ter illustratie, een gouden standbeeld kent wellicht een grote geldwaarde en is daardoor in de basis een aantrekkelijk doel, maar door de grote massa van goud is een volledig gouden standbeeld direct ook weer een onaantrekkelijk doel omdat het onpraktisch is. Daardoor wordt het gelegenheidselement waar deze theorie op berust bemoeilijkt in het nadeel van de potentiële crimineel. Gewicht is zodoende een belangrijke indicator van inertie, maar omvang, aangesloten of vastgezette onderdelen en andere factoren die het proces van diefstal bij inbraak bemoeilijken spelen ook een rol. Uit deze tegenstelling tussen geldwaarde en inertie blijkt de rationele kosten-batenachtergrond die deze criminologische theorie kent. Een arm huishouden kan zodoende alsnog een aantrekkelijk doelwit zijn, wanneer de 'kosten' van een inbraakpoging dusdanig laag zijn dat de relatief lage opbrengsten het alsnog tot een aantrekkelijk doelwit maken. Inertie heeft zodoende een effect dat kenmerken vertoont van de materiële objecten die bijdragen aan *guardianship*.

Vervolgens resteert echter de kwestie van de vertaling naar het digitale domein. In de basis kennen computerbestanden geen gewicht, en daarmee dus geen inertie. Dat maakt dat het stelen, kopiëren, aanpassen of vernietigen van digitale 'goederen' geen 'kosten' heeft en zodoende in de basis erg aantrekkelijk is (Yucedal, 2010). Yar (2005) stipt nog enige digitale inertie aan in het feit dat de grootte van databestanden en de snelheid waarmee data door computers verwerkt kan worden, evenals de snelheid van het internet waarmee het verplaatst moet worden, 'kosten' kunnen opleveren. Sinds dat artikel in 2005 is gepubliceerd is de opslag-

en geheugentechniek echter sterk verbeterd, evenals de toegang tot hoge internetsnelheden. Hoewel het stelen van vele terabytes aan bedrijfsdata over (continentaal) grote afstanden inderdaad in die zin inertie kent, is dat niet de focus van deze thesis, die zich richt op het niveau van de individu. Dit zijn vergelijkbare argumenten als bij de factor *proximity* zijn gegeven.

Gegeven dat de inertie van inbraak op persoonlijke gegevensdragers zodoende dusdanig laag is dat de 'kosten' van deze criminele activiteit vrijwel nihil zijn, zorgt dat ervoor dat iedere individu een basisniveau van aantrekkelijkheid kent. Cybercriminelen maken hier dan ook gebruik van door relatief grootschalig te werk te gaan (Yucedal, 2010). Bijvoorbeeld door na het bekend worden van een veiligheidslek in een veelgebruikte applicatie, direct te proberen bij zoveel mogelijk gebruikers tegelijk in te breken (*zero-day attack*) (Kaspersky, 2022). Eenmaal binnen zal de waarde moeten worden vastgesteld van de gegevens die toegankelijk zijn geworden. De 'kosten' en inertie van *hacking* zijn daarmee dusdanig laag dat de baten vooraf niet eens in kaart hoeven te worden gebracht. Met enkel een paar persoonsgegevens is het daarnaast voor een hacker overigens vooraf niet eens altijd eenvoudig om daadwerkelijk te weten wat een doelwit waard is. Verder vond recent panelonderzoek, hoewel wederom de literatuur niet altijd eenduidig is, geen significante relatie tussen *target attractiveness* en het risico om slachtoffer te worden van *hacking* of *malware* (Guarra & Ingram, 2022). Het geheel overziend kan daarom beredeneerd worden dat in het licht en perspectief van deze thesis, de risicofactor *attractiveness* geneutraliseerd is voor iedereen; en dat daarmee het bestaan van deze mediërende risicofactor tussen de kans op slachtofferschap van *hacking* en inkomen niet hoeft te worden verwacht.

De laatste factor die Cohen et al. (1981) benoemen is die van *definitional properties of specific crimes*. De mate waarin de kenmerken van een specifiek misdrijf beperkend werken (*constrain*) op strikt instrumentele actie, is bepalend voor de kracht van de vier eerder behandelde risicofactoren. Hoe meer deze instrumentele actie door bepaalde misdrijfkenmerken beperkt wordt, hoe sterker de effecten van *exposure, guardianship* en *proximity* in verhouding tot het effect van *target attractiveness*. Deze abstracte omschrijving illustreren Cohen et al. (1981) middels een vergelijking tussen enerzijds inbraak en anderzijds diefstal buiten het huishouden: diefstal zou daarbij meer strikt instrumenteel gedrag faciliteren vanuit het perspectief van de delinquent, omdat de goederen die gestolen kunnen worden een stuk zichtbaarder zijn (en daarmee beter op waarde te schatten zijn) dan dat bij inbraak het geval is. Bij inbraak daarentegen, is vaak alsnog sprake van een gecalculeerde gok. Hierdoor krijgen veel inbraken een niet-instrumentele kwaliteit. Daarnaast vereist inbraak ook meer kennis van de aanwezigheid van het slachtoffer of andere potentiële menselijke *guardians*. Al met al staat het risico om slachtoffer te worden van diefstal buiten het huishouden daarmee sterker onder invloed van *target attractiveness* dan het risico om slachtoffer te worden van inbraak dat staat. De effecten van *exposure, guardianship* en

proximity zijn daarmee bij inbraak automatisch ook weer relatief sterk in verhouding tot het effect van *target attractiveness*, vergeleken met diefstal buiten het huishouden.
De risicofactor *definitional properties of specific crimes* is daarmee vooral een vergelijkende factor tussen verschillende typen misdrijven, die iets zegt over hoe de verdeling van de vier andere risicofactoren – die wél betrekking hebben op inkomen – is gesteld. Hoewel inbraak en *hacking* enige paralellen kennen die in deze thesis reeds zijn uitgelicht, laten de meeste risicofactoren zich niet vertalen naar het digitale domein, waardoor een waardevolle redeneerlijn en werking van ook deze specifieke risicofactor teniet wordt gedaan. Ook een relevante vergelijking tussen *hacking* en cyberagressie via deze risicofactor blijkt niet mogelijk. Cyberagressie, als parallel van (fysiek) geweld (*assault*), is wat Cohen et al. (1981) betreft namelijk een misdrijf uit 'expressie', in plaats van uit instrumentele overwegingen zoals bij *hacking* (Holt & Bossler, 2014). Het denken in kosten en baten (instrumenteel) is bij misdrijven uit expressie niet langer aan de orde, waardoor cyberagressie in de basis al buiten de focus van de risicofactor *definitional properties of specific crimes* valt.

Hoewel theoretisch gezien een jammerlijke constatering, wijst dit wel op de theoretische onderbelichting van cyberagressie in dit theoretisch kader. Veel van de factoren die worden behandeld zijn namelijk geformuleerd vanuit een eenduidig kosten-batenperspectief (*guardianship, target attractiveness*). Dit leent zich goed voor analogieën over inbraak en *hacking*, maar is niet overtuigend bij cyberagressie. Om slachtofferschap van cyberagressie (en de relatie met FP) beter te verklaren, zal in de volgende paragraaf dan ook een tweede criminologisch perspectief worden aangehaald, de *strain theory*, welke net als de theorie van Cohen et al. (2018) op eenzelfde kritische wijze naar het digitale domein zal worden vertaald.

2.3 De relatie tussen inkomen en cyberagressie nader belicht

Hoewel het CBS (2018) aangeeft dat individuen met een (al dan niet langdurig) laag inkomen vaker slachtoffer zijn van cyberagressie, is een theoretische benadering van deze relatie door de emotionele grondslag minder evident dan bij de instrumenteel gemotiveerde cybermisdrijven. Hoewel criminologisch gezien de *strain theory* van Robert Merton een emotionele basis kent, waarbij ontevredenheid over sociaaleconomische status (*strain*) als aanleiding dient voor crimineel gedrag, betreft dit wederom een verklaring voor instrumenteel-gemotiveerde criminaliteit (Lanier et al, 2015). De *strain* voortkomend uit deze financiële ontevredenheid, zou immers leiden tot delinquent gedrag dat deze ontevredenheid wegneemt.

Een latere herziening van de *strain theory,* de zogenoemde *General Strain Theory* (GST) (Agnew, 1992)*,* die meer gefocust is op sociaal-emotionele factoren als aanleiding voor *strain,* toont daarentegen wel degelijk een positief verband aan tussen de hoeveelheid *strain*

en de kans op (cyber)pestgedrag (Hay & Ray, 2020; Patchin & Hinduja, 2011; Eden, Heiman & Olenik-Shemesh, 2014). Het probleem met de GST is dat de door Merton gemaakte oorspronkelijke connectie met inkomen, FP of sociaaleconomische status niet langer centraal staat. Daarnaast heeft deze theorie bovenal oog voor de voorspelbaarheid van daderschap, terwijl deze thesis echter de voorspelbaarheid van slachtofferschap onderzoekt. Een beredenering vanuit een daderschapstheorie, die zou moeten hypothetiseren over slachtofferschap, leidt hooguit tot zwakke indirecte relaties.

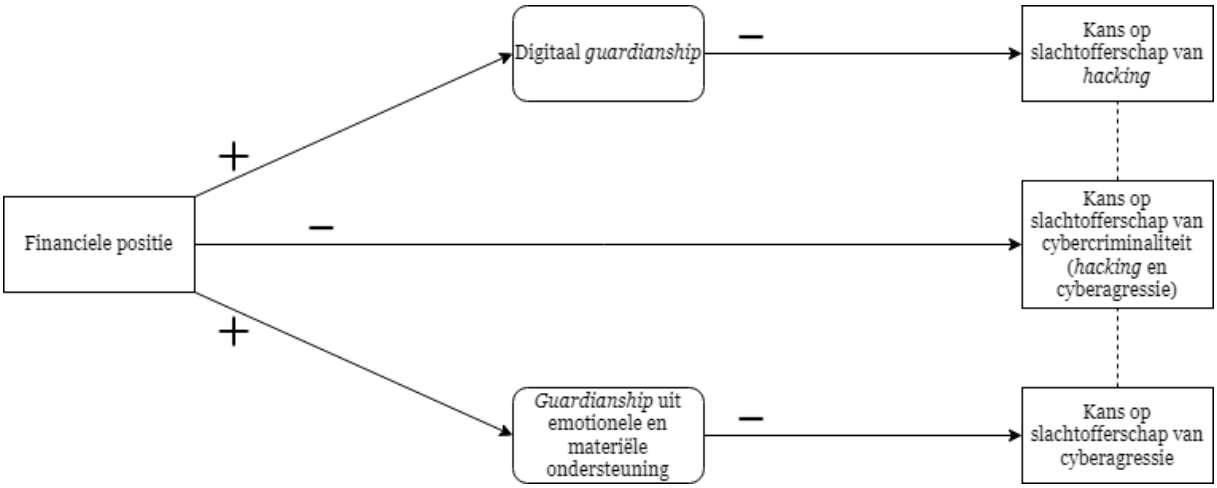
Daar staat tegenover dat er wel degelijk wetenschappelijke papers zijn geschreven over de relatie tussen (familiaire) contextfactoren, waaronder inkomen, en de gerelateerde kans op slachtofferschap van cyberagressie. Deze literatuur over slachtofferschap van cyberagressie is, zoals ondertussen gebruikelijk lijkt bij academisch onderzoek naar cybercrime, niet eenduidig; ook al lijkt er een overwicht te bestaan van onderzoeken die de negatieve relatie met inkomen bevestigen (López-Castro & Priegue, 2019). Zo zijn scholieren uit gezinnen waarbij sprake is van relatieve financiële deprivatie vaker zowel slachtoffer van 'traditioneel' pestgedrag (Shaheen, Hammad, Haourani, & Nassar, 2017; Gardella, Fisher, Teurbe-Tolon, Ketner & Nation, 2019; Hye-Jin, Young-Eun, Moon-Doo, Won-Myong, 2017), als slachtoffer van cyberpesten (Chen et al., 2018; Jansen et al., 2012), als dader van cyberpesten (Bevilacqua et al., 2017). Mogelijk is hierbij sprake van een cyclus; omdat het slachtofferschap van cyberagressie nieuwe *strain* veroorzaakt, wat weer leidt tot een verhoogde kans op daderschap van cyberagressie (Hay & Ray, 2020).

Hoewel de kanttekening gemaakt dient te worden dat de onderzoeken in de bovenstaande literatuur georiënteerd zijn op (cyber)pestgedrag en –slachtofferschap onder specifiek adolescenten, bieden ze wel theoretisch inzicht in een mogelijk mechanisme achter cyberagressie. Zo blijkt, het geheel overziend, de dader van cyberagressie gemotiveerd te worden door *strain*, voortkomend uit factoren die de GST van Agnew aanwijst (Hay & Ray, 2020; Patchin & Hinduja, 2011); terwijl het slachtoffer door diens economisch zwakke positie een kwetsbaarheid kent door een gebrek aan emotionele en materiële ondersteuning in diens directe context (Chen et al., 2014; Hye-Jin, Young-Eun, Moon-Doo, Won-Myong, 2017).

Voornamelijk het laatstgenoemde is daardoor te interpreteren als een vorm van gebrekkig '*guardianship* uit emotionele en materiële steun'; wat in samenspel werkt met het eerstgenoemde, een mate van *exposure* aan door *strain* gemotiveerde daders. Een synthese van *general strain theory* en elementen van *opportunity theories* lijkt hier gaande. Hierbij zou een gegeven mate van door *strain* gemotiveerde daders in iemands omgeving, leiden tot diens slachtofferschap van cyberagressie, wanneer diens '*guardianship* uit emotionele en materiële steun' door diens bemoeilijkte FP relatief laag is.

Hypothese 5: er bestaat een positief verband tussen iemands financiële positie (FP) en diens *guardianship* uit emotionele en materiële ondersteuning.
Hypothese 6: er bestaat een negatief verband tussen iemands *guardianship* uit emotionele en materiële ondersteuning, en diens kans om slachtoffer te worden van cyberagressie.
Hypothese 7: iemands *guardianship* uit emotionele en materiële ondersteuning vertoont een negatief mediërend verband tussen iemands financiële positie (FP) en diens kans op slachtofferschap van cyberagressie.

Het geheel overziend is de theoretische verwachting dat naarmate iemands FP verslechtert, twee typen *guardianship* daaronder komen te lijden, wat naar verwachting leidt tot een verhoogde kans op slachtofferschap van *hacking* en *cyberagressie*. In figuur 1 wordt het conceptueel model op basis van de geformuleerde hypothesen gepresenteerd. In het volgende hoofdstuk, het methodologisch kader, zullen de concepten uit dit model meetbaar worden gemaakt.



Figuur 1: *Conceptueel model*

3. METHODOLOGISCH KADER

Dit hoofdstuk gaat in op de methodologische dimensie van dit onderzoek. Hiertoe zal eerst een algemene introductie worden gegeven over de methodologische aanpak van dit onderzoek. Daarna volgt de operationalisatie van de verschillende theoretische concepten, waarbij wordt gekeken naar andere onderzoeken die in het verleden dezelfde of vergelijkbare concepten onderzochten. De operationalisatie eindigt met een operationalisatietabel waarin een overzicht van indicatoren is opgenomen, evenals de bijbehorende interviewvragen. Vervolgens komen de dataverzamelings- en -analysemethoden in groter detail aan bod, alvorens wordt afgesloten met een uiteenzetting van (voor zover vooraf bekend) betrouwbaarheids- en validiteitskwesties die gepaard gaan met dit onderzoek.

3.1 Introductie

Om vast te stellen hoe en in welke mate iemands FP daadwerkelijk gerelateerd is aan diens kans op slachtofferschap van *hacking* en cyberagressie, zijn in het gebied dat politiedistrict Gelderland-Midden behelst flitsinterviews afgenomen met willekeurige voorbijgangers (N=400). Op basis van inwonersaantallen en de allocatie van politieteams in de regio zijn vijf plaatsen in Gelderland-Midden aangewezen waar de data verzameld zou worden (zie paragraaf 'dataverzameling'). Met de benodigde data over de FP van de respondenten, de twee typen *guardianship* en het ervaren slachtofferschap van *hacking* en cyberagressie onder deze populatie verzameld, is middels enkele verschillende typen regressieanalyse het mogelijke verband tussen iemands FP en diens kans op slachtofferschap bij de data-analyse blootgelegd.

Deze regressievarianten betreffen in IBM SPSS Statistics uitgevoerde lineaire regressieanalyses (hypothesen 2 en 5) en multinomiale logistische regressieanalyses (hypothesen 1, 3 en 6). Deze laatstgenoemde vorm van logistische regressieanalyse kan worden beschouwd als een verlengstuk van een binomiale logistische regressieanalyse (Field, 2018). Waar bij binomiale analyses sprake is van een (dichotome) Y-variabele die slechts twee uitingen kent ('wel' of 'niet' gehackt) (Hagle, 2011), kent een multinomiale analyse de mogelijkheid om meerdere categoriale uitingen toe te wijzen aan de Y-variabele ('nooit', 'een enkele keer' of 'vaker' gehackt). Daarmee kan ook een mate van gewicht worden toegekend aan deze uitingen. Zo vergelijkt SPSS de categorieën 'een enkele keer gehackt' en 'vaker gehackt' met de groep respondenten die 'nooit gehackt' is. Dit heeft genuanceerdere (informatie-rijkere) voorspelbaarheidsresultaten tot gevolg. Bij lineaire regressie ligt dit wat eenvoudiger. Lineaire regressie spiegelt twee continue variabelen tegen elkaar af en beoordeelt in hoeverre deze vergelijking in een lineair model past (Field, 2018).

Met elke 'enkelvoudige' hypothese getest, waarbij duidelijk is geworden welke indicatoren voor de twee typen *guardianship* daadwerkelijk significant blijken, dienen de

hypothesen die een mediërend verband voorspellen te worden getoetst. Hiertoe is eerst voor *hacking* en daarna voor cyberagressie een multinomiaal logistisch regressiemodel opgezet met FP als onafhankelijke variabele, waaraan de resterende mediërende indicatoren in tweede instantie zijn toegevoegd. Als robuustheidstoets is parallel via PROCESS nog een binomiale regressieanalyse gedraaid waarin de mediërende factoren nogmaals zijn getoetst. Een gedetailleerdere omschrijving van het analyseproces is te vinden in de paragraaf 'data-analyse'.

De keuze voor regressiemodellen als methode van data-analyse is gebaseerd op de gedachte dat deze modellen passend zijn wanneer men met statistische zekerheid uitspraken wil doen over de voorspelbaarheid van een uiting van de y-variabele, middels de geformuleerde x-variabelen (Gallo, 2015). De externe validiteit van deze methode is dan ook hoog. Belangrijk hierbij is dat er geen sprake is van causaliteit. Er wordt niet gemeten of X tot Y leidt, maar in hoeverre X een voorspeller is van Y. Voor dit onderzoek geldt dan ook dat getracht werd te achterhalen hoe de variabelen van FP, in combinatie met de mediërende variabelen, een voorspeller kunnen zijn van de kans op slachtofferschap van *hacking* of cyberagressie.

3.2 Operationalisatie

Hieronder worden opeenvolgend de verschillende concepten uit het conceptueel model meetbaar gemaakt, ofwel geoperationaliseerd. Elk concept krijgt een aantal indicatoren toegewezen op basis van de wetenschappelijke literatuur. Voor enkele concepten is een groot aantal indicatoren gebruikt; hierom eindigt de operationalisatie in een operationalisatietabel (tabel 1), zodat de tekst schematisch ondersteund wordt en daarmee de overzichtelijkheid gewaarborgd blijft. In de uiteindelijke analyse worden ook de controlevariabelen leeftijd, geslacht en opleidingsniveau meegenomen.

3.2.1 Operationalisatie – FP (X-variabele)

Het valide en betrouwbaar meten van financiële persoonskenmerken is een lastige opgave. Vragen hierover beschouwt men namelijk vaak als ongewenst en/of ongemakkelijk (Duncan & Peters, 2001). Om die reden vermijdt dit onderzoek een rechtstreekse vraag naar een geldbedrag of inkomenscategorie aan bereidwillige respondenten. Daarom is gebruik gemaakt van de *Financial Well-Being Scale* (FWS) van het Amerikaanse *Consumer Financial Protection Bureau* (CFPB, 2022), de FP van elke respondent in kaart te brengen. Bij elke indicator op de FWS zal ter illustratie een toelichting worden gegeven over waar een respondent zoal aan zou kunnen denken bij elke indicator.

De FWS onderscheidt een aantal indicatoren (CFPB, 2022). Ten eerste kijkt het naar *'having control over one's finances'*. Dit houdt in dat een individu bijvoorbeeld zijn of haar rekeningen kan betalen en geen onoverkomelijke schuld heeft.

Ten tweede is er *'the capacity to absorb a financial shock'*, als onderdeel van de FWS. Dit behelst het hebben van reserves om onverwachte uitgaven te kunnen doen, op basis van eigen middelen of middelen die beschikbaar worden gesteld door iemands directe omgeving. Deze benadering voor het bepalen van iemands FP komt ook terug in vergelijkbaar onderzoek naar de relatie tussen sociale ongelijkheid en slachtofferschap van criminaliteit. Zo stellen Nilsson & Estrada (2006) dat het verzamelen van informatie over de *'cash safety margin'* die men al dan niet heeft bijdraagt aan een meer valide beeld van individuele welvaart dan enkel een statistiek over inkomenshoogte. Het levert namelijk een statistisch onderscheid op tussen mensen met een laag inkomen die wél een reserve hebben, en mensen met een laag inkomen die dat niet hebben. Evenals dat het een statistisch onderscheid oplevert tussen mensen met een hoog inkomen die tevens een reserve achter de hand hebben, en mensen met een hoog inkomen die dat niet hebben. Wat de categorisering van FP betreft, is dit een belangrijk onderscheid. Lage inkomens mét reserves kennen namelijk een stuk gunstiger FP dan de lage inkomens zonder reserves. Evenals dat de hoge inkomens mét reserves een gunstiger FP kennen dat de hoge inkomens zonder reserves. Door dergelijke nuances aan te brengen in de vragenlijst ontstaat een meer valide beeld dan enkel een inkomensstatistiek.

Ten derde dient volgens het FWS een individu idealiter *'on track to meet financial goals'* te zijn. Dit behelst de vraag of een individu bijvoorbeeld naar tevredenheid verwacht om over een aantal jaar zijn of haar (studie)schuld af te lossen, of bijvoorbeeld succesvol op termijn kan sparen voor een grotere uitgave.

Afsluitend behelst de vierde indicator op de FWS de kwestie of een individu in staat is om *'choices that allow to enjoy life'* te maken. Vakanties, recreatie, het volgen van cursussen, of het spenderen van extra tijd met familie vallen hier allen onder. Het zijn keuzes die het leven aangenamer moeten maken, maar ook kosten ze elk op hun eigen manier geld. Het vermogen om (gerust) dergelijke keuzes te maken, valt onder deze laatste indicator.

Om de FWS naar behoren in te zetten, geeft het CFPB (2022[a]) een aantal instructies over het gebruik van de schaal. Zo leiden, per respondent, de vier indicatoren tot vier scores op een tienpuntsschaal. De som van deze scores wordt onder invloed van de leeftijd van de respondent en het al dan niet zelfstandig beantwoorden van de scores tijdens het interview, getransformeerd tot een door het CFPB gerangschikte eindscore. Bij deze transformaties is de leeftijd '62' voor het CFPB de grens om een tweedeling in de groep respondenten aan te brengen. Bij een gelijke somscore, eindigt een respondent jonger dan 62 zodoende met een andere getransformeerde eindscore dan een respondent ouder dan 62. Wat betreft de zelfstandigheid van de respondenten bij het beantwoorden van de vragen over hun FP vallen alle respondenten in dezelfde categorie. In dit onderzoek hebben namelijk alle respondenten de vragen over hun FP zelfstandig en in anonimiteit op een tablet ingevuld. Via SPSS zijn gedurende de datapreparatie de transformaties op de FP-scores doorgevoerd, wat terug te

vinden is in de syntax (bijlage 1). Tabel 1 geeft een overzicht van de vier gebruikte indicatoren (exact gefomuleerd) en interviewvragen, horende bij dit concept.

3.2.2 Operationalisatie - slachtofferschap van *hacking* en/of cyberagressie (Y-variabele)

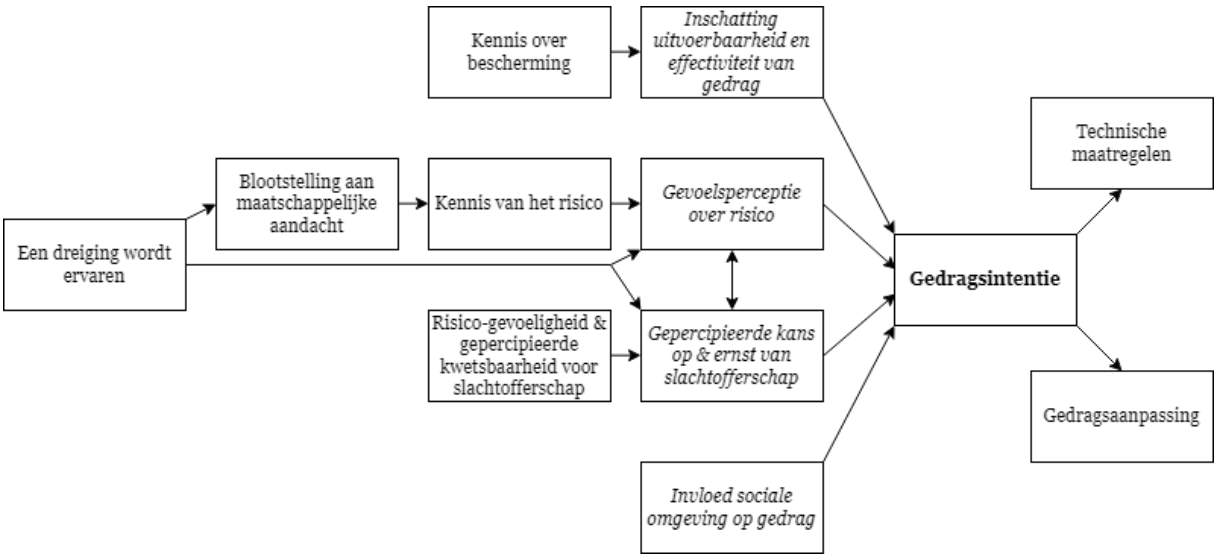
Bij het vaststellen of een respondent al dan niet slachtoffer is geweest van *hacking* en/of cyberagressie, worden de in eerder CBS-onderzoek (2019[c]; 2016) gehanteerde definities van deze twee begrippen uit het theoretisch kader gevolgd. Dit onderzoek beschouwt een respondent dan ook als slachtoffer van *hacking,* indien dit individu in de veronderstelling is dat bij hem of haar "in het verleden met kwade bedoelingen ingebroken of ingelogd op diens computer, mobiele telefoon, e-mailaccount, socialenetwerksite of een ander online account". Verder beschouwt dit onderzoek een respondent als slachtoffer van cyberagressie indien dit individu in de veronderstelling is dat hij of zij "in het verleden slachtoffer is geweest van roddel, getreiter, pesten, stalken, chantage of bedreiging via internet". Tabel 1 geeft een overzicht van de twee gebruikte indicatoren (exact geformuleerd) en interviewvragen, horende bij dit concept. Deze indicatoren worden strikt gescheiden behandeld, zijnde twee verschillende variabelen.

Toegegeven berust deze operationalisatie sterk op de perceptie en het beoordelingsvermogen van de respondenten. Indien een respondent bijvoorbeeld in volledige overtuiging een incorrect wachtwoord blijft invoeren voor een account, en hieraan de conclusie verbindt dat hij of zij dan wel gehackt moet zijn, kan dit tot een onjuist antwoord op de vraag leiden. Tegelijkertijd kunnen mensen gehackt zijn zonder dat zij zich hiervan bewust zijn, en zodoende onterecht aangeven dat zij nooit gehackt zijn. Daar staat tegenover dat, zoals eerder aangegeven, de aangiftebereidheid voor cybercriminaliteit erg laag ligt; waardoor politiecijfers als alternatieve informatiebron naar alle waarschijnlijkheid een nog verder vertekend beeld vertonen. Tevens maken Spithoven et al. (2020) in panelonderzoek naar slachtofferschap van cybercriminaliteit op eenzelfde wijze gebruik van de ervaringen van respondenten zelf.

3.2.3 Operationalisatie - digitaal *guardianship* (mediërende variabele)

Ter belichaming van digitaal *guardianship*, maakt dit onderzoek gebruik van de wetenschappelijke literatuur over 'cyberweerbaarheid'. De aanleiding hiertoe berust in de gelijkenis tussen de reeds uitgekristalliseerde aspecten van digitaal *guardianship* enerzijds, namelijk de menselijke omgang met digitale risico's en de technische voorzorgsmaatregelen die men neemt; en anderzijds de definitie van cyberweerbaarheid: "het samenvallen van risicobewustzijn en zelfbeschermend gedrag tegen cybercriminaliteit" (Spithoven et al., 2020, p.5). De conceptuele aard van digitaal *guardianship* en die van cyberweerbaarheid vertonen zodoende sterke overeenkomsten.

Cyberweerbaarheid vertaalt zich in de praktijk idealiter in “De individuele doelstelling om zelfbeschermend gedrag te vertonen [(gedragsintentie)] in het nemen van maatregelen of het aanpassen van het eigen gedrag” (Spithoven et al., 2020, p.8). Voor de totstandkoming van deze individuele doelstelling is volgens de auteurs sprake van een veertiental contribuerende factoren, welke in dit onderzoek worden overgenomen als indicatoren voor cyberweerbaarheid. Figuur 2 geeft op basis van het *cyber resilience model* uit Spithoven et al. (2021) een schematische weergave van deze veertien indicatoren. Tabel 1 geeft opnieuw een overzicht van deze indicatoren (exact geformuleerd), inclusief interviewvragen, horende bij dit concept. Deze indicatoren worden zowel gescheiden geanalyseerd, als samengevoegd tot het concept dat zij tezamen vormen (digitaal *guardianship*). Daarmee kan zowel vanuit praktisch oogpunt (als inhoud van risicocommunicatie), als vanuit wetenschappelijk oogpunt (samenhang van theoretische concepten) naar de onderzoeksresultaten worden gekeken, respectievelijk.



Figuur 2: *Indicatoren voor cyberweerbaarheid, op basis van het “cyber resilience model” uit Spithoven et al. (2021).*

Deze indicatoren worden in dit onderzoek overgenomen voor het concept ‘digitaal guardianship’.

3.2.4 Operationalisatie - *Guardianship* uit emotionele en materiële ondersteuning (mediërende variabele)

Uit het theoretisch kader is gebleken dat de relatie tussen slachtofferschap van (cyber)pestgedrag en inkomen-gerelateerde persoonskenmerken, vaak is geverifieerd. In zoverre in de literatuur over causale mechanismen wordt gesproken, zou *Guardianship* uit emotionele en materiële ondersteuning hierin theoretisch gezien (een van) de causale schakel(s) omvatten (Chen et al., 2014; Hye-Jin, Young-Eun, Moon-Doo, Won-Myong, 2017). Concrete indicatoren over emotionele en materiële ondersteuning ontbreken echter in de literatuur.

Een artikel van Cathleen Lewandowski en Twyla Hill (2009) wijst op het gebrek aan wetenschappelijke literatuur over de combinatie van emotionele en materiële ondersteuning in iemands directe sociale omgeving. Desondanks maken zij zelf gebruik van een variëteit van indicatoren om het effect van emotionele en materiële ondersteuning op de succeskans van vrouwen in drugsverslavingstrajecten te meten. Ironischerwijs ontbreekt in het artikel een duidelijk overzicht van de getoetste indicatoren. Afgaand op de definities die Lewandowski en Hill (2009) hanteren van emotionele steun en materiële steun, kan alsnog tot een op literatuur gebaseerde operationalisatie gekomen worden, hoewel deze minder uitgebreid is dan bij 'digitaal *guardianship*'.

Zodoende maakt dit onderzoek gebruik van de volgende indicator voor emotionele steun: "de mate waarin de respondent zich emotioneel gesteund voelt door diens sociale omgeving". Tevens maakt het gebruik van de volgende indicator voor materiële steun: "de mate waarin de respondent zich financieel gesteund voelt door diens sociale omgeving".

Tabel 1 geeft een overzicht van de twee gebruikte indicatoren en interviewvragen, horende bij dit concept. Deze indicatoren worden zowel gescheiden geanalyseerd, als samengevoegd tot het concept dat zij tezamen vormen (*guardianship* uit emotionele en materiële steun). Daarmee kan zowel vanuit praktisch oogpunt (als inhoud van risicocommunicatie), als vanuit wetenschappelijk oogpunt (samenhang van theoretische concepten) naar de onderzoeksresultaten worden gekeken, respectievelijk.

3.2.5 Operationalisatietabel

Met alle concepten geoperationaliseerd, is in tabel 1 een overzicht opgenomen van alle indicatoren, inclusief de bijbehorende interviewvragen. Steeds staat in de eerste kolom het concept aangegeven, met in de tweede kolom de bijbehorende indicatoren

Concept	**Indicator**	**Interviewvraag**
Financiële positie	De mate waarin een respondent controle heeft over diens financiën.	Op een schaal van één tot tien, in hoeverre ervaart u controle te hebben over uw financiën?
	De mate waarin een respondent en financiële tegenvaller kan opvangen.	Op een schaal van één tot tien, in hoeverre acht u uzelf in staat om een financiële tegenvaller op te vangen?
	De mate waarin een respondent afstevent op het bereiken van financiële doelen.	Op een schaal van één tot tien, in hoeverre stevent u af op het bereiken van uw financiële doelen?
	De mate waarin een respondent in staat is om keuzes te maken die het levensgeluk te vergroten.	Op een schaal van één tot tien, in hoeverre bent u financieel in staat om keuzes te maken die uw levensgeluk vergroten?

Digitaal *guardianship*	De mate waarin een respondent hacking als dreiging ervaart.	Op een schaal van één tot tien, in hoeverre ervaart u hacking als bedreiging voor uzelf?
	De mate waarin een respondent maatschappelijke aandacht voor hacking ervaart.	Op een schaal van één tot tien, in hoeverre ervaart u dat er maatschappelijke aandacht is voor hacking?
	De mate waarin een respondent aangeeft kennis te hebben over hacking als risico.	Op een schaal van één tot tien, in hoeverre heeft u kennis over hacking als risico?
	De mate waarin een respondent aangeeft risico-gevoeligheid te ervaren.	Op een schaal van één tot tien, in hoeverre bent u in het algemeen prikkelbaar voor gevaren?
	De mate waarin een respondent aangeeft persoonlijke kwetsbaarheid voor hacking te ervaren.	Op een schaal van één tot tien, in hoeverre voelt u zich kwetsbaar voor hacking?
	De mate waarin een respondent aangeeft kennis te hebben over beschermende maatregelen tegen hacking.	Op een schaal van één tot tien, in hoeverre heeft u kennis over beschermende maatregelen die men kan nemen tegen hacking?
	De mate waarin een respondent aangeeft dat mogelijk zelfbeschermend gedrag tegen hacking uitvoerbaar is.	Op een schaal van één tot tien, in hoeverre denkt u dat het uitvoerbaar is om uzelf te beschermen tegen hacking?
	De mate waarin een respondent De mate waarin geeft dat mogelijk zelfbeschermend gedrag tegen hacking effectief is.	Op een schaal van één tot tien, in hoeverre denkt u dat bescherming tegen hacking effectief is?
	De mate waarin een respondent aangeeft negatieve gevoelens te ervaren bij hacking als risico.	Op een schaal van één tot tien, in hoeverre ervaart u negatieve gevoelens bij hacking als risico?
	De grootte van de kans die een respondent aangeeft op het risico gehackt te worden.	Op een schaal van één tot tien, hoe groot acht u de kans dat u zelf gehackt wordt?
	De mate van ernst van slachtofferschap van hacking die een respondent inschat.	Op een schaal van één tot tien, hoe ernstig schat u de gevolgen, mocht u gehackt worden?
	De mate waarin een respondent ervaart door diens sociale omgeving te worden beïnvloed om online zelfbeschermend gedrag te vertonen.	Op een schaal van één tot tien, in hoeverre ervaart u dat uw sociale omgeving u beïnvloedt om uzelf online te beschermen tegen hacking?

	De mate waarin een respondent aangeeft technische maatregelen te nemen om te voorkomen dat men slachtoffer wordt van hacking.	Op een schaal van één tot tien, in hoeverre neemt u technische maatregelen om te voorkomen dat u slachtoffer wordt van hacking?
	De mate waarin een respondent aangeeft diens online gedrag aan te passen om te voorkomen dat men slachtoffer wordt van hacking.	Op een schaal van één tot tien, in hoeverre past u uw online gedrag aan om te voorkomen dat u gehackt wordt?
Guardianship uit materiële en emotionele ondersteuning	De mate waarin de respondent zich emotioneel gesteund voelt door diens sociale omgeving.	Op een schaal van één tot tien, in hoeverre ervaart u (op de momenten dat het nodig is) emotionele steun uit uw sociale omgeving?
	De mate waarin de respondent zich financieel gesteund voelt door diens sociale omgeving.	Op een schaal van één tot tien, in hoeverre ervaart u (op de momenten dat het nodig is) financiële steun uit uw sociale omgeving?
Slachtofferschap van hacking	Hoe vaak een respondent veronderstelt te zijn gehackt.	Hoe vaak heeft in het verleden iemand met kwade bedoelingen ingebroken of ingelogd op uw computer, mobiele telefoon, e-mailaccount, socialenetwerksite of een ander online account? Nooit, een enkele keer, een paar keer, vaak, heel vaak.
Slachtofferschap van cyberagressie	Hoe vaak een respondent veronderstelt slachtoffer te zijn geworden van cyberagressie.	Hoe vaak bent u in het verleden slachtoffer geweest van roddel, getreiter, pesten, stalken, chantage of bedreiging via internet. Nooit, een enkele keer, een paar keer, vaak, heel vaak.

Tabel 1: *Indicatoren volledig uitgeschreven en koppeling aan interviewvragen.*

3.3 Dataverzameling

Nu de verschillende theoretische concepten meetbaar zijn gemaakt, is een repliceerbare uiteenzetting van het dataverzamelingsplan op zijn plaats. De basis voor deze dataverzameling is het afnemen van vierhonderd flitsinterviews ('gestructureerd interview' in Vennix (2016)) in het gebied dat politiedistrict Gelderland-Midden dekt, gedurende de gehele maand mei en de eerste week van juni, op werkdagen. Het voordeel van flitsinterviews ten opzichte van een digitale enquête is dat het de onderzoeker in staat stelt om onduidelijkheden voor de

respondenten te verhelderen en eventueel door te vragen wanneer een antwoord of redenering van een respondent onvolledig is (Izmeth, 2015). De interviews zijn afgenomen bij toevallige passanten, in een poging de willekeur van de steekproef te vergroten. Hierin schuilt nog een voordeel van fysieke flitsinterviews ten opzichte van een digitale enquête: bij een digitale enquête is sprake van afhankelijkheid van het digitale netwerk van de onderzoeker(s), tenzij men geld zou betalen aan een organisatie die een groot respondentenpanel onderhoudt en een enquête onder dit panel uit zou zetten. Voor deze thesis zijn dergelijke middelen echter niet beschikbaar; dus om te voorkomen dat de respondenten grotendeels uit de digitale bubbel van de onderzoeker komen, wat gepaard gaat met gebrekkige representativiteit, is gekozen voor zo willekeurig mogelijke flitsinterviews. De positionering van de onderzoeker in het veld om flitsinterviews af te nemen, en daarbij bovenstaande methodologische voordelen te optimaliseren, is gebaseerd op de volgende overwegingen.

Ten eerste dient een diverse steekproef te worden genomen, waarin individuen met verschillende FP's in de analyse later tegen elkaar af kunnen worden gezet. Hiertoe zijn winkelcentra die centraal tussen buurten in liggen, met een breed aanbod van duurdere en goedkopere winkels, geschikt om een zo divers mogelijke groep respondenten te spreken. De individuen in deze groep passeren vrijwel allemaal een centrale ingang, of een parkeerplaats, wat deze locaties tot een geschikte plek voor flitsinterviews maakt.

Ten tweede is het nodig geweest om keuzes te maken wat betreft de verdeling van interviewlocaties binnen de regio. Een aantal zaken zijn hierin doorslaggevend geweest: grotere gemeenten krijgen de prioriteit omwille van de diversiteit in populatie die deze gemeenten te bieden hebben ten opzichte van kleinere gemeenten. Ook dient het aantal respondenten dat in elke gemeente wordt benaderd naar proportie van het inwoneraantal te worden verdeeld. Zo blijven de onderlinge populatieverhoudingen tussen de gemeenten relatief bewaard.

Afsluitend is de allocatie van politieteams medebepalend geweest. Hoewel de opdracht voor dit onderzoek vanuit Arnhem komt, wenst deze organisatie dat basisteams die zijn gekoppeld aan andere gemeenten in Gelderland-Midden zo veel mogelijk betrokken worden bij dit onderzoek. Zodoende zouden de onderzoeksresultaten een wijdverbreidere validiteit kennen dan enkel tot de grenzen van de gemeente Arnhem. Uiteindelijk is gekozen voor Arnhem, Ede, Wageningen, Zevenaar en Barneveld. Binnen de verdeling van de vierhonderd flitsinterviews over deze steden, is naar inwoneraantal een proportionele verhouding bepaald. Deze verhouding is terug te zien in tabel 2 op de volgende pagina.

Gemeente	Inwoneraantal	%	N
Arnhem	162.424	~38	200
Ede	118.530	~28	91
Wageningen	39.635	~9	29
Zevenaar	44.096	~10	32
Barneveld	59.995	~14	45
Totaal	424.680	100	400

Tabel 2: *Inwoneraantallen per gemeente, op basis van het CBS (2021[b])*

Wat betreft de allocatie van steekproefposities binnen de verschillende gemeenten, zijn positioneringskeuzes gemaakt met het streven om een steekproef met een zo groot mogelijke inkomensdiversiteit te doen. Zo heeft de onderzoeker zich in Arnhem voorbij de hoofdingang in winkelcentrum Kronenburg gepositioneerd. Hoewel deze wijk (Vredenburg/Kronenburg) zelf een lichtelijk beneden-modaal inkomen kent, is het winkelcentrum op een kruispunt tussen vier wijken met verschillende gemiddelde inkomenshoogten gelegen. De aangelegen wijk met het laagste gemiddeld inkomen is Malburgen-Oost (€29.500) en de aangelegen wijk met het hoogste gemiddeld inkomen is Elden (€48.400), een gemiddeld verschil van bijna €20.000 (Gemeente Arnhem, 2022).

Daarnaast zijn er in Arnhem Centrum (straat: Bovenbeekstraat) en in winkelcentrum Presikhaaf interviews afgenomen, om een zo divers mogelijke groep Arnhemse respondenten te kunnen interviewen. Hiermee is het aantal respondenten uit Arnhem op 200 komen te staan, wat de verhoudingen naar populatieaantal lichtelijk scheef trekt (tabel 2). Daar staat tegenover dat inkomensgegevens uit Arnhem gearticuleerder waren dan bij de rest van de gemeenten, waardoor tactischere positionering van de onderzoeker bewerkstelligd kon worden, en daarmee de kans op het treffen van een grotere inkomensdiversiteit groter werd. Bovendien is de exacte woonplaats van de respondenten geen onderzochte variabele, waardoor het voor de inhoud van het onderzoek weinig gevolgen heeft.

In Ede heeft de onderzoeker zich bij Winkelcentrum Spindop gepositioneerd, en later ook in de dorpskern van Ede (straat: Maandereind). De Spindop is wederom een winkelcentrum dat in de relatieve nabijheid van drie verschillende woonwijken met een brede inkomensdiversiteit ligt. Van deze drie wijken heeft Ede-Zuid het laagste gemiddeld inkomen (€40.300) en Veluwse Poort het hoogste gemiddeld inkomen (€59.900), wederom een verschil van nagenoeg €20.000 (EdeInCijfers, 2022).

Over Wageningen, Zevenaar en Barneveld geldt dat geen of slechts beperkt data beschikbaar is over inkomen. Over de gemeente Zevenaar zijn sowieso weinig statistieken beschikbaar, naar alle waarschijnlijkheid komt dit door de beperkte omvang van Zevenaar. Om die reden heeft de onderzoeker zich centraal opgesteld, bij het Raadhuisplein (straat:

Grietsestraat). Voor Barneveld is wat meer data beschikbaar, maar is door de grote oppervlakte van de gemeente, en de grove indeling van statistische gebieden, geen bruikbare nuance aan te brengen qua positionering van de onderzoeker. Hierom zal wederom het stadshart worden aangehouden als steekproeflocatie (straat: Langstraat). Voor Wageningen geldt dat hoewel er wel enkele gegevens over inkomenshoogte op wijk- en buurtniveau beschikbaar waren (CBS-InUwBuurt, 2018), dit onvolledige informatie betrof. Hierom is wederom voor een centrale positie gekozen (straat: Hoogstraat).

Met de overwegingen omtrent plaatsing afgehandeld, is de benadering van potentiële respondenten een aandachtspunt. Om presumpties over commerciële doeleinden van de onderzoeker zo snel mogelijk teniet te doen, dient in de openingsvraag te worden benadrukt dat het een hulpvraag betreft voor een afstudeeronderzoek. Daarnaast stelt de onderzoeker de vragen, maar voert de onderzoeker de antwoorden in op een tablet waar via Qualtrics een enquêteversie van de interviewvragen openstaat. Er is daarmee sprake van gesloten antwoordcategorieën. Zodoende kunnen zo valide mogelijke antwoorden worden nagestreefd door het feit dat de methode van dataverzameling een fysiek gesprek is met ruimte voor verheldering en doorvragen, maar kunnen ingevoerde antwoorden alsnog direct worden gekwantificeerd.

Zoals bij de operationalisatie reeds aangegeven is, zijn mensen bij bijvoorbeeld vragen over hun FP begrijpelijkerwijs niet snel bereid om hierover te praten met een onbekend persoon. Naast de keuze voor een toegankelijker meetinstrument (de *CFPB*-schaal), zullen de vragen die hieruit voortkomen door de respondenten zelf op de tablet worden ingevoerd, zodat door de ontstane anonimiteit een zo hoog mogelijke responsebereidheid wordt gestimuleerd, evenals een zo eerlijk mogelijk antwoord. Deze lijn wordt in de opzet van de flitsinterviews gevolgd: de vragen die naar alle waarschijnlijkheid met minder taboe gepaard gaan (digitale weerbaarheid) komen als eerst aan bod in een gespreksvorm, waarna de vragen die men mogelijk als ongemakkelijk percipieert (slachtofferschap, emotionele en financiele steun, FP) op het tablet kunnen worden ingevoerd door de respondenten. Voordat respondenten de tablet overhandigd krijgen, wordt hen gewezen op de lolly die zij kunnen bemachtigen bij het volledig afronden van het interview. Niet alleen wordt hiermee de bereidheid om deel te nemen vergroot (CBS, 2022[b]), maar wordt ook getracht middels de onschuld van een lolly de gepercipieerde betrouwbaarheid van de onderzoeker door de respondenten (alvorens zij informatie over hun FP delen) te verhogen.

3.4 Data-analyse

Het doel van deze paragraaf is om in een drietal stappen uiteen te zetten hoe de data-analyse tot stand is gekomen. Deze stappen betreffen de datapreparatie, het toetsen van assumpties en het uitvoeren van de juiste analysevormen. Een volledig en repliceerbaar totaaloverzicht van de stappen die zijn gezet om vanuit de ruwe dataset tot een eindanalyse te komen zijn vastgelegd in de syntax, welke terug te vinden is in de bijlagen. Het analyseren van de data heeft plaatsgevonden middels het programma *IBM Statistics SPSS 28*.

3.4.1 Datapreparatie

Voorafgaand aan het uitvoeren van de analyse of het toetsen van assumpties, dienen een aantal voorbereidende stappen te worden gezet. Zo worden eerst alle onnodige variabelen die Qualtrics zelf toevoegt aan de dataset verwijderd. Tevens dienen de scores op de tienpuntsschalen voor FP te worden gecumuleerd naar totaalscores, alvorens deze totaalscores worden gecorrigeerd voor leeftijd en het zelfstandig beantwoorden van de FP-vragen, conform de instructies voor de toepassing van de CFPB-schaal (CFPB, 2022[a]). Ook is de vijfpuntsschaal van de Y-variabelen omgezet naar 3 antwoordcategorieën (0=nooit, 1=een enkele keer, 2=vaker). De categorieën 4 en 5 op de vijfpuntsschaal zijn namelijk te klein gebleken om bruikbaar in een analyse opgenomen te kunnen worden. Om die reden zijn ze samengevoegd met de derde categorie onder de noemer 'vaker' [slachtoffer geweest van hacking/cyberagressie]. Daarnaast zijn dummyvariabelen aangemaakt voor zowel slachtofferschap van *hacking* als van cyberagressie ('wel of geen slachtoffer van …'), zodat ook binomiale toetsen uitgevoerd kunnen worden.

3.4.2 Toetsing van statistische assumpties

Het toetsen van assumpties is van belang voor het waarborgen van de bruikbaarheid van de uitkomsten van de data-analyse. Om de resultaten van dit onderzoek echter leesbaar en overzichtelijk te houden, zijn uitkomsten van assumptietoetsen enkel in het resultatenhoofdstuk vermeld indien ze geschonden zijn. Indien dit het geval is, staat dit vermeld bij de uitkomsten van de bijbehorende regressieanalyse. Om de transparantie omtrent dit onderzoek te bewaren, is een volledig overzicht van de uitkomsten van de assumptie-toetsen in bijlage 2 opgenomen.

De eerste assumpties die zijn getoetst betreffen de nominaliteit van de afhankelijke variabele (Y); de continuïteit, ordinaliteit of nominaliteit van de onafhankelijke variabele en mediërende variabelen (X & M); evenals de onafhankelijkheid van observaties en wederzijds uitsluitende en uitputtende antwoordcategorieën. Hoewel de wijze van vraagformulering en dataverzamelingsmethode binnen dit onderzoek al tot naleving van deze assumpties leidt, is

voor de onafhankelijkheid van observaties een extra Durbin-Watson test uitgevoerd, waarbij uitkomsten buiten de range van 1-3 ongunstig zijn (Field, 2018).

Vervolgens is op meerdere wijzen getest op multicollineariteit, op basis van grenswaarden uit werk van Belsley, Kuh & Welsch (1980). Ten eerste via *Pearson correlation*, welke niet boven .80 mag uitkomen voor getoetste variabelen. Ten tweede via *correlation statistics*, waarbij de *VIF-value* niet boven 3.0 mag uitkomen. Ten derde via *condition index*, waarbij waarden niet boven 30.0 mogen uitkomen. Ten vierde via *variance proportions*, waarbij per dimensie geen twee of meer variabelen boven .50 mogen uitkomen.

Voor de logistische toetsen dient de assumptie 'lineariteit van de logit' te worden getoetst. Hiervoor is een Box-Tidwell procedure uitgevoerd. Bij deze procedure worden nieuwe variabelen gegenereerd via een zogenoemde log transformatie. De te toetsen variabelen, inclusief de getransformeerde versies, worden in één binomiale logistische regressie getoetst, waarbij de getransformeerde variabelen niet-significant dienen uit te slaan om lineariteit van de logit aan te tonen. De grenswaarde voor significantie is daarbij $\alpha=.05$.

Enkele resterende assumpties zijn als volgt getoetst. Wat betreft de normaalverdeeldheid van de data mag op basis van de centrale limiet stelling worden aangenomen dat bij $N>30$ sprake is van normaalverdeeldheid (Field, 2018). Een controletoets middels een Shapiro-Wilk test of Kolmogorov-Smirnov test is dan ook niet nodig, en kan zelfs onwenselijk zijn. Niet alleen omdat bij omvangrijkere steekproeven de normaalverdeeldheid van data minder relevant wordt, maar ook omdat grotere steekproeven sneller onterecht significant uit dergelijke tests komen (Field, 2018).

Afsluitend is de betrouwbaarheid en interne consistentie van de *guardianship*-constructen gemeten via Cronbach's Alpha. Hoewel Field (2013) ook hier aangeeft voorzichtig te zijn met harde grenswaarden, zou een Cronbach's Alpha van tussen .7 en .8 voor de hele schaal een waarschijnlijke indicatie van goede betrouwbaarheid zijn. Vervolgens dient te worden gekeken naar de correlatie van individuele indicatoren (idealiter boven .3 (Field, 2018)); evenals wat de Cronbach's Alpha van de hele schaal zou zijn wanneer een indicator uit de schaal zou worden verwijderd. Indien sprake is van een verhoging van de betrouwbaarheid van de gehele schaal als een individuele indicator zou worden verwijderd, dient deze dan ook te worden verwijderd. Voorafgaand hieraan is middels principale componentenanalyse eerst bepaald of specifieke sub-schalen in de data aanwijsbaar zijn. Een criterium hiervoor is wel dat naast dat SPSS bepaalde componenten aanwijst, deze componenten ook inhoudelijk in een overkoepelend concept te plaatsten zijn.

Zodra de betrouwbaarheid en interne samenhang van de beide concepten van *guardianship* bekend zijn, kunnen zij elk ook in hun geheel worden geanalyseerd ten opzichte van FP en cyberslachtofferschap, door het gemiddelde te nemen van de scores op de indicatoren per concept. Dit is zodoende ook gedaan, waardoor nu per analyse waarbij de

indicatoren van een van de concepten van *guardianship* aan bod komen, het concept ook als geheel (separaat) geanalyseerd kan worden.

3.4.3 Werkwijze toetsing van hypothesen

Om te beginnen is in het resultatenhoofdstuk een overzicht van de *descriptive statistics* gepresenteerd. Deze *descriptive statistics* zijn noodzakelijk om de kenmerken van de genomen steekproef te verduidelijken (Curtin University, 2022). Eventuele bijzonderheden ten opzichte van bekende informatie over de algehele populatie waar de steekproef uit is genomen kunnen hiermee (indirect) in beeld komen.

Vervolgens is de basishypothese van dit onderzoek getest: de relatie tussen de FP van een respondent en het slachtofferschap van *hacking* en/of cyberagressie. Door twee multinomiale logistische regressieanalyses te draaien, één voor *hacking* en één voor cyberagressie, kan dit verband worden blootgelegd. Dit legt het fundament voor het nader onderzoeken van een mediërend verband; immers, indien deze hypothese niet aangenomen wordt, vervalt automatisch ook de potentie voor een mediërend verband en de rest van dit onderzoek. In deze toets zijn de controlevariabele leeftijd, geslacht en opleidingsniveau opgenomen.

Daarna is gecontroleerd welke van de indicatoren van de twee vormen van *guardianship* op kunnen worden genomen in een grotere toets die een mediërend verband kan aantonen. Hiertoe zijn alle indicatoren individueel als afhankelijke variabele in een lineair regressiemodel getoetst op een verband met FP als onafhankelijke variabele. De indicatoren die hieruit als significant naar voren zijn gekomen, zijn vervolgens als onafhankelijke variabelen in twee multinomiale logistische regressieanalyses opgenomen, wederom één voor *hacking* en één voor cyberagressie. De indicatoren die zowel zijnde afhankelijke variabele verband houden met FP, als zijnde onafhankelijke variabele verband houden met de bijbehorende vorm van cybercrime, zijn vervolgens meegenomen in een analyse van een mogelijk mediërend effect. Bij elk van de getoetste hypothesen waarbij de indicatoren van een van de vormen van *guardianship* aan bod is gekomen, is eveneens het concept zelf (als schaal) in eenzelfde (separate) regressievorm geanalyseerd.

Afsluitend is de vooraf beoogde toetsingswijze van de potentiële mediërende effecten op twee manieren opgezet. Wederom zijn twee multinomiale regressieanalyses opgezet, een voor elk van de vormen van cybercriminaliteit. In het eerste block is enkel FP opgenomen. In het tweede block zijn de overgebleven indicatoren opgenomen. In het derde block zijn de controlevariabelen leeftijd, geslacht en opleidingsniveau opgenomen. Indien de b-coëfficiënt tussen block een en twee kleiner zou zijn geworden, zou dat betekenen dat sprake is van partiële mediatie. Indien de oorspronkelijke relatie tussen FP en een van de vormen van cybercriminaliteit niet langer significant zou zijn door de aanwezigheid van de overgebleven

indicatoren, zou sprake zijn van volledige mediatie. Bij wijze van robuustheidstoets is vervolgens via PROCESS een nieuwe analyse opgezet, ter controle van een mogelijk mediërend verband. Gegeven dat dit een binomiale regressievorm betreft, zijn als afhankelijke variabelen de eerder gecreëerde dummyvariabelen gebruikt ('nooit' of 'ooit' slachtoffer van *hacking*/cyberagressie). Voor alle regressieanalyses in dit onderzoek geldt dat de grenswaarde voor significantie α=.05 betreft.

3.5 Validiteit en betrouwbaarheid

Het voornaamste betrouwbaarheidsprobleem dat deze thesis treft is de relatief lage N-waarde. Hoewel het afnemen van vierhonderd flitsinterviews in ongeveer een maand tijd de grenzen van haalbaarheid bereikt, neemt dat niet weg dat vierhonderd respondenten als steekproef van een heterogene regiopopulatie zeker groter kan. Hoewel het formaat van een steekproef niet een standaard percentage van de onderzochte populatie hoeft te bedragen, is de homogeniteit van een populatie wél van belang (Vennix, 2016). Naarmate een populatie meer homogeen is, is een kleinere steekproef vereist. Immers, hoe meer bepaalde kenmerken onder een populatie onderling overeenkomstig zijn, hoe groter de kans wordt dat de kenmerken van respondenten in een steekproef dezelfde kenmerken vertonen. Nadelig voor dit onderzoek is dan ook dat juist naar een diverse, heterogene, groep respondenten wordt gezocht, wat zou betekenen dat een hogere N is vereist. Een hogere N-waarde is niet haalbaar, en verdere aanbreng van homogeniserende populatiekenmerken is voor dit onderzoek na een gebiedsafbakening van Gelderland-Midden niet meer mogelijk. De betrouwbaarheid is zodoende gebonden aan deze realiteit.

Ook is bij deze methode van respondentenwerving sprake van enige zelfselectie. Hoewel pure zelfselectie zou betekenen dat respondenten zelf intrinsiek gemotiveerd zijn om zich aan te melden voor deelname aan een onderzoek, geldt voor het huidige onderzoek nog steeds een onderscheid tussen mensen die desgevraagd te overtuigen zijn om deel te nemen aan het onderzoek of dit alsnog weigeren. Hierdoor bestaat de kans dat specifieke groepen in de samenleving relatief vaak weigeren, of juist relatief veel, waardoor de representativiteit van de steekproef achteruit gaat (Heckman, 2010). Om deze kans op vertekeningen in de weerspiegeling van de samenleving te verkleinen, is zoals reeds genoemd in de paragraaf over dataverzameling, de positionering van de onderzoeker ingezet om financieel gezien een zo groot mogelijke diversiteit aan respondenten te werven. Dat neemt echter niet weg dat bepaalde bevolkingsgroepen nog steeds vaker kunnen weigeren om deel te nemen, ook al staat de onderzoeker wel op de juiste plek om deze mensen aan te spreken. Of daarmee wel voldoende spreiding op de variabele FP ontstaat om inhoudelijk solide uitspraken te kunnen doen op basis van de statistische resultaten, valt daarmee te bezien.

Tegenover deze beperkingen staat het voordeel van het mondeling afnemen van voorgestructureerde interviews, in plaats van het individueel invullen van een voorgestructureerde vragenlijst: daar waar nodig kan doorgevraagd worden, of kunnen onduidelijkheden worden verhelderd, vanuit de geest van de vraag. Wanneer hiertoe niet de mogelijkheid was geweest, en respondenten zelf de gehele vragenlijst op de tablet zouden invullen, zou de kwaliteit van de data aanzienlijk lager zijn. De antwoorden van de respondenten zouden immers verder van de werkelijkheid afliggen, omdat zij ofwel elementen van de vragenlijst niet begrepen, ofwel omdat zij een vraag verkeerd interpreteerden. Door hier als interviewer alert op te zijn, kan data gegenereerd worden met een relatief hoge mate van validiteit.

Andere bedenkingen die men kan plaatsen bij het meten van iemands FP, zijn de eerlijkheid bij het geven van antwoorden met betrekking tot FP en het vermogen dat een respondent heeft om diens FP te beoordelen. Met name het laatstgenoemde is een gevolg van de poging om het vragen naar exacte getallen te vermijden. Er ontstaat namelijk meer interpretatie- en beoordelingsruimte naarmate in een vraag verder wordt weggebleven van de ultieme exactheid: een netto maandelijks inkomen. Tegelijkertijd is deze werkwijze een noodzakelijk kwaad: deelnamebereidheid zou sterk verminderen bij het vragen naar een exact bedrag, wat een fundamenteel probleem zou vormen voor de uitvoerbaarheid van dit onderzoek. Echter, in een streven om respondenten zo eerlijk mogelijk te laten zijn, door hen zelf de vragen te laten invullen; meer kwalitatieve vragen te stellen; en enkel op een tienpuntsschaal te laten beantwoorden; ontstaat ondanks de bevorderde laagdrempeligheid wel enige speling. Zou de ene respondent zichzelf eenzelfde cijfer geven op een van de elementen van FP, gegeven eenzelfde financiële situatie als een andere respondent? En wat de een ziet als een groot spaardoel of financiële tegenvaller, is voor een ander wellicht een onbereikbare of een juist relatief haalbare uitgave. Al met al valt te stellen dat de voordelen die bij de mondelinge vragen gelden voor het verhogen van validiteit, komen te vervallen bij de vragen over FP door de maatregelen die zijn genomen om respondenten bereid te krijgen om hier iets (eerlijks) over te beantwoorden.

Tegelijkertijd staat hier tegenover dat de methode om vragen te stellen die de financiële situatie van iemand omschrijven in plaats van te vragen naar de hoogte van een inkomen, meer zegt over de mate waarin iemand financieel gezien enige bewegingsruimte heeft. Iemand kan immers bovenmodaal verdienen, maar als de lasten die deze respondent ervaart gelijk aan- of groter zijn dan dit relatief hoge inkomen, dan voelt deze respondent zich waarschijnlijk meer financieel bekneld dan iemand met een lager inkomen en met nog lagere lasten dan dit inkomen. De een houdt immers maandelijks geen geld over, of komt zelfs rood te staan, terwijl de ander spaargeld opbouwt. Zodoende kent het gebruik van vragen die iemands FP

omschrijven inherent al validiteitsvoordelen ten opzichte van het vragen naar een exact inkomen, ongeacht het streven naar deelnamebereidheid.

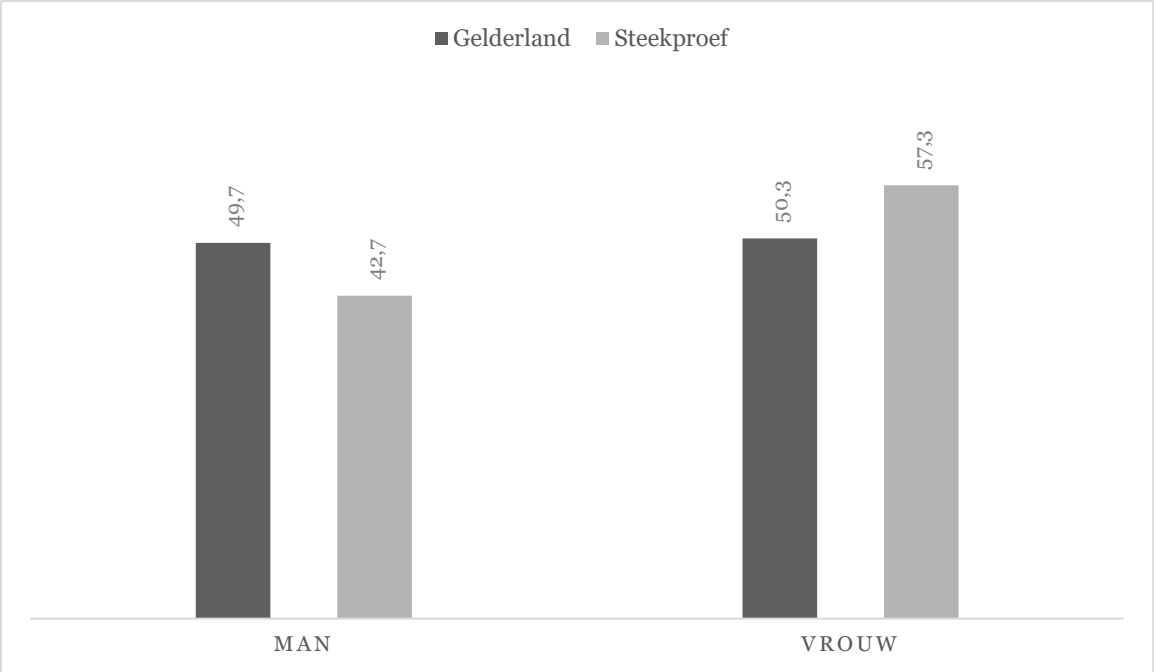
Met de methodologische verantwoording afgerond, zal het volgende hoofdstuk ingaan op de analyseresultaten. De analyse zal aantonen welke hypothesen verworpen dienen te worden, en welke aangenomen kunnen worden. De eerstvolgende gelegenheid waarop wordt ingegaan op methodologische beperkingen, zal in het discussiehoofdstuk zijn aan het eind van deze thesis. Hierin zal onder andere gereflecteerd worden op de beperkingen die gedurende en na het onderzoeksproces aan het licht kwamen.

4. RESULTATEN

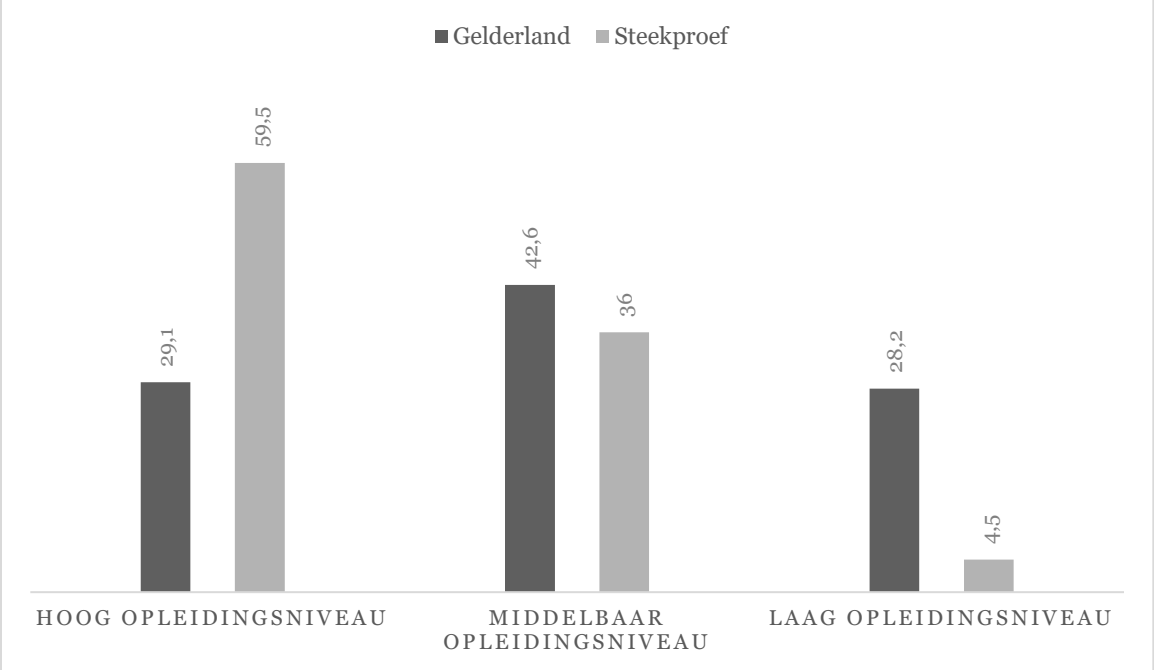
Dit hoofdstuk volgt de structuur van een steeds verder uitbreidende en complexer wordende analyse. Dat begint met een visuele uiteenzetting van de scores op de controlevariabelen van de steekproef in vergelijking met die van de algehele populatie. Zodoende is inzichtelijk in hoeverre, wat betreft deze variabelen, de steekproef representatief is voor de algehele populatie. Daaropvolgend komen eerst de beschrijvende statistieken kort aan bod, waarna de verschillende hypothesen langs worden gelopen zoals deze vooraf zijn geformuleerd. Conform de omschrijving in het methodologisch kader, zullen vervolgens eerst de resultaten van de basishypothese worden gepresenteerd (de relatie tussen FP en slachtofferschap van cybercriminaliteit); waarna de resultaten over de significantie van de mediërende indicatoren worden gepresenteerd; alvorens uiteindelijk de resultaten van de mediërende toetsen worden uiteengezet. Indien op basis van gepresenteerde gegevens een hypothese dient te worden aangenomen of verworpen, zal dit als zodanig staan aangegeven. Per keer dat een van de *guardianship*-concepten voor het eerst aan bod komt, zal de betrouwbaarheid en interne samenhang van deze concepten (als schalen) worden beoordeeld.

4.1 Representativiteit van de steekproef

Onderstaande figuren geven inzicht in de verschillende controlevariabelen. Figuur 3 toont de verschillen tussen de procentuele verhouding tussen mannen en vrouwen in de genomen steekproef, ten opzichte van de cijfers over heel Gelderland. Over politiedistrict Gelderland-Midden specifiek zijn dergelijke cijfers niet bekend. Waarin heel Gelderland 49,7% man is, is dit in de steekproef 42,7%. Voor vrouwen geldt dat zij in heel Gelderland 50,3% van de populatie uitmaken, terwijl dit in de steekproef 57,3% is. Verder is de gemiddelde leeftijd van de respondenten in de steekproef 41,99. Hoewel voor de provincie Gelderland geen gemiddelde leeftijd is te vinden, is de gemiddelde leeftijd in Nederland volgens het CBS (2022[c]) 42,3 jaar. Om afsluitend het de populatieverhoudingen op het gebied van opleidingsniveau te kunnen vergelijken met de steekproef, dient één en dezelfde definitie te worden toegekend aan deze niveaus. Op basis van de definities die AlleCijfers (2022) hanteert, schaart dit onderzoek in haar data de respondenten die ‘vmbo’ hebben aangekruist als laag opgeleid; worden mensen die havo, vwo of mbo hebben aangekruist als middelbaar opgeleid beschouwd; en zijn de mensen die hbo of wo hebben ingevuld gemarkeerd als hoog opgeleid. Volgens deze indeling, is 4,5% van de respondenten laag opgeleid, ten opzichte van 28,2% in heel Gelderland; is 36,0% van de respondenten middelbaar opgeleid, ten opzichte van 42,6% in heel Gelderland; en is 59,5% van de respondenten hoog opgeleid, ten opzichte van 29,1% in heel Gelderland. Figuur 4 geeft de verschillen tussen heel Gelderland en de genomen steekproef weer.



Figuur 3: *procentuele geslachtsverdeling in heel Gelderland ten opzichte van de gebruikte steekproef.*
Gegevens over heel Gelderland zijn op basis van AlleCijfers.nl (2022).



Figuur 4: *procentuele verdeling van opleidingsniveau in heel Gelderland ten opzichte van de gebruikte steekproef.*
Gegevens over heel Gelderland zijn op basis van AlleCijfers.nl (2022).

4.2 Beschrijvende statistieken

In tabel 3 zijn de beschrijvende statistieken betreffende het slachtofferschap van *hacking* en cyberagressie opgenomen. Dit geeft inzicht in de verdeling van de aantallen slachtoffers waar de regressieanalyses mee zijn uitgevoerd.

		Frequency	Valid Percent	Cumulative Percent
Slachtofferschap van *hacking*	Nooit	239	59.8	59.8
	Een enkele keer	109	27.3	87.0
	vaker	52	13.0	100.0
	Totaal	400	100.0	
Slachtofferschap van cyberagressie	Nooit	251	62.7	62.7
	Een enkele keer	102	25.5	88.3
	Vaker	47	11.8	100.0
	Totaal	400	100.0	

Tabel 3: *Beschrijvende statistieken omtrent slachtofferschap in de steekproef*

4.3 Het verband tussen FP en slachtofferschap van cybercrime (hacking en cyberagressie)

Uit de dubbele multinomiale logistische regressieanalyse blijkt dat de financiële positie van respondenten significant negatief verband houdt met hoe vaak zij slachtoffer zijn geworden van zowel *hacking* als cyberagressie. Hierbij zijn de controlevariabelen opleidingsniveau, leeftijd en geslacht opgenomen in de analyse. Een aantal nuances geldt hierbij. Bij zowel *hacking* als cyberagressie is alleen sprake van significantie onder de groep respondenten die 'vaker' (meermaals) slachtoffer zijn geworden van deze digitale delicten. Daarbij geldt dat in het model voor cyberagressie 'leeftijd' als controlevariabele een significant negatief effect vertoont, bij zowel de groep respondenten die een enkele keer slachtoffer zijn geworden van cyberagressie als bij de groep respondenten die dit vaker heeft meegemaakt.

In het kader van onderzoekstransparantie dient te worden vermeld dat in het multinomiale logistische regressiemodel voor hacking sprake is van een compositie-effect, voortkomend uit een disbalans in de steekproef. Het compositie-effect in dit onderzoek behelst dat het verband tussen FP en slachtofferschap van hacking enkel significant blijkt onder de aanwezigheid van de controlevariabelen. Middels PROCESS zijn vervolganalyses gedraaid om een modererend effect bloot te leggen onder de controlevariabelen, dat het compositie-effect zou kunnen verklaren. In lijn met de in dit hoofdstuk eerder gepresenteerde disbalans in de verhoudingen tussen hoog-, middelbaar- en laag opgeleide respondenten ten opzichte van de verhoudingen in opleidingsniveau in heel Gelderland, is opleidingsniveau dan ook de modererende factor gebleken. Door de aanwezigheid van de controlevariabele 'opleidingsniveau' in het oorspronkelijke multinomiale logistische regressiemodel voor *hacking*, controleert het model voor de (scheve) compositie van de steekproef, waardoor FP een significant verband vertoont.

Het geheel overziend is hypothese 1: "Er bestaat een negatief verband tussen iemands financiële positie (FP) en diens kans om slachtoffer te worden van cybercriminaliteit (*hacking*

en cyberagressie)", aangenomen. De exacte resultaten van zowel de twee multinomiale logistische regressieanalyses, als van de vervolganalyse via PROCESS, staan in tabel 4 vermeld. In het kader van repliceerbaarheid dient te worden vermeld dat de vervolganalyse via PROCESS niet in de syntax (bijlage 1) vermeld staat, omdat PROCESS als functionaliteit het technisch niet toestaat om naar syntax te worden vertaald.

Slachtofferschap van *hacking*		B	Std. Error	Sig.	Exp(B)
Een enkele keer	Intercept	.139	.826	.866	
	Financiële positie	-.007	.011	.544	.993
	Geslacht	-.174	.236	.461	.840
	Hoogst genoten opleiding	-.021	.071	.766	.979
	Leeftijd	-.003	.008	.737	.997
vaker	Intercept	.026	1.078	.981	
	Financiële positie	-.032	.015	.027	.968
	Geslacht	-.425	.313	.175	.654
	Hoogst genoten opleiding	.164	.101	.105	1.178
	Leeftijd	.012	.011	.256	1.012
PROCESS	Likelihood ratio test X*M interaction		Chi-sq.	p	
	Hoogst genoten opleiding		4.061	.044	

Slachtofferschap van cyberagressie					
een enkele keer	Intercept	1.192	.866	.169	
	Financiële positie	-.016	.012	.177	,984
	Geslacht	-.052	.243	.830	,949
	Hoogst genoten opleiding	.000	.074	.999	1,000
	Leeftijd	-.023	.009	.007	.977
vaker	Intercept	3.911	1.282	.002	
	Financiële positie	-.037	.018	.036	.964
	Geslacht	.200	.360	.577	1.222
	Hoogst genoten opleiding	-.104	.103	.313	.901
	Leeftijd	-.088	.016	<.001	.916

Tabel 4: *resultaten van de multinomiale logistische regressieanalyses.*

De referentiecategorie is 'nooit'. 'Slachtofferschap van hacking' en 'slachtofferschap van cyberagressie' zijn de afhankelijke variabelen; FP, geslacht, opleidingsniveau en leeftijd zijn de onafhankelijke variabelen.

De resultaten van de analyse middels PROCESS om het compositie-effect in de dataset via de variabele opleidingsniveau bloot te leggen, zijn opgenomen onder de laatste rij van de resultaten bij 'slachtofferschap van hacking'.

Nu de resultaten van hypothese 1 bekend zijn, zal hierna eerst het pad van *hacking* uit het conceptueel model worden uitgewerkt, en daarna het pad van cyberagressie. Dit betekent dat eerst wordt bekeken welke indicatoren voor digitaal *guardianship* zowel verband houden met FP als met het slachtofferschap van *hacking*. Daarna wordt het pad van cyberagressie uitgewerkt, waarbij wordt bekeken welke indicatoren van '*guardianship* uit emotionele en materiële steun' zowel verband houden met FP als met het slachtofferschap van cyberagressie. De indicatoren van beide vormen van *guardianship* die in beide richtingen significant blijken, kunnen aan het eind van dit resultatenhoofdstuk worden opgenomen in een multinomiale logistische regressieanalyse die het mediërend effect van deze indicatoren toetst.

4.4 Betrouwbaarheid en interne samenhang van digitaal *guardianship*

De betrouwbaarheid en interne samenhang van de *guardianship*-concepten is conform het methodologisch kader middels Cronbach's Alpha vastgesteld. Hiertoe is eerst een principale componentenanalyse uitgevoerd, ter verkenning van eventuele onderliggende dimensies. Binnen het concept 'digitaal *guardianship*', zijn via een principale componentenanalyse geen theoretisch sluitende dimensies aanwijsbaar gebleken. Hoewel uit de factoranalyse vier componenten naar voren zijn gekomen, zijn de indicatoren (na rotatie) die bijdragen aan deze componenten onvoldoende theoretisch samenhangend. Dit heeft ertoe geleid dat alle veertien indicatoren voor 'digitaal *guardianship*' als onderdeel van één concept worden beschouwd.

Cronbach's Alpha voor 'digitaal *guardianship*' als schaal is .755, wat in lijn ligt met het vooraf gestelde doel om een waarde van tussen de .7 en .8 te behalen (tabel 5). Wat betreft de individuele indicatoren is gebleken dat enkele indicatoren net onder de grenswaarde van .3 uitkomen (tabel 6). Echter, gegeven de afnemende betrouwbaarheid van de gehele schaal indien deze worden verwijderd, is ervoor gekozen om deze indicatoren in het concept 'digitaal *guardianship*' te behouden. De indicator 'mate waarin men het nemen van maatregelen tegen hacking effectief acht' is daarentegen verwijderd, omdat de deze zowel ver onder .3 scoort, als de betrouwbaarheid van de hele schaal doet toenemen indien verwijderd. Na verwijdering van deze indicator wordt deze schaal als betrouwbaar en intern samenhangend beschouwd.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.755	.750	14

Tabel 6: Cronbach's Alpha bij 'digitaal *guardianship*' als schaal.

	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
De mate waarin een respondent *hacking* als dreiging ervaart.	.493	.727
Mate waarin men maatschappelijke aandacht ervaart voor *hacking*.	.303	.747
Mate waarin men kennis heeft over hacking als risico.	.340	.743
Mate waarin men persoonlijke risicogevoeligheid ervaart.	.466	.730
Mate waarin men zich kwetsbaar voelt voor hacking.	.484	.729
Mate waarin men kennis heeft over beschermende maatregelen tegen hacking.	.404	.737
Mate waarin met het nemen van maatregelen tegen hacking uitvoerbaar acht.	.218	.753
Mate waarin men het nemen van maatregelen tegen hacking effectief acht.	.156	.758
Ervaart negatieve gevoelens bij hacking als risico.	.476	.728
Grootte van de kans die men schat om gehackt te worden.	.255	.752
Mate van ernst die men toekent aan de gevolgen van hacking.	.372	.740
Mate waarin men invloed uit hun sociale omgeving ervaart om beschermende maatregelen tegen hacking te nemen.	.292	.750
Mate waarin men technische maatregelen neemt tegen hacking.	.432	.734
Mate waarin men het online gedrag aanpast tegen hacking.	.400	.737

Tabel 6: *Correlatie tussen de indicatoren van 'digitaal guardianship' en de totale schaal, evenals de Cronbach's Alpha indien een item verwijderd zou worden*.

4.5 Indicatoren voor digitaal *guardianship*: het verband met FP

Het vaststellen van de indicatoren voor digitaal guardianship die zowel verband houden met FP als met het slachtofferschap van *hacking*, begint met de connectie tussen FP en deze indicatoren. Hiertoe zijn alle indicatoren opgenomen in enkelvoudige lineaire regressieanalyses, waaruit de volgende resultaten voort zijn gekomen. FP houdt significant positief verband met: de mate waarin men maatschappelijke aandacht voor *hacking* ervaart; de mate waarin men kennis heeft over *hacking* als risico; de mate waarin men kennis heeft over beschermende maatregelen tegen *hacking*; de mate waarin men verwacht dat bescherming tegen *hacking* effectief is; de ernst die men aan de gevolgen van *hacking* toekent; de mate waarin men technische maatregelen ter preventie van *hacking*; en de mate waarin men het online gedrag aanpast ter preventie van *hacking*.

Tevens is de totale schaal ook (losstaand) geanalyseerd in relatie tot FP, waarbij een lineaire regressieanalyse is uitgevoerd met FP als onafhankelijke variabele en 'digitaal *guardianship*' als gemiddelde schaal van de verschillende indicatoren, als afhankelijke variabele. Hieruit blijkt eveneens een significant positief verband tussen FP en digitaal *guardianship*. Hypothese 2 "er bestaat een positief verband tussen iemands financiële positie (FP) en diens digitale *guardianship*", is daarmee aangenomen. De exacte resultaten van de lineaire regressieanalyses bij de indicatoren van digitaal *guardianship* en het concept zelf, ten opzichte van FP, staan in tabel 7 vermeld.

Mate waarin men *hacking* als bedreiging ervaart	B	Std. Error	Beta	t	Sig.
(Constant)	5.145	.662		7.774	<.001
Financiële positie	.010	.010	.049	.977	.329
Mate waarin men maatschappelijke aandacht ervaart voor *hacking*					
(Constant)	4.108	.534		7.696	<.001
Financiële positie	.027	.008	.164	3.321	<.001
Mate waarin men kennis heeft over *hacking* als risico					
(Constant)	3.538	.635		5.573	<,001
Financiële positie	.034	.010	.175	3.550	<.001
Mate waarin men persoonlijke risicogevoeligheid ervaart					
(Constant)	4.879	.657		7.426	<,001
Financiële positie	.007	.010	.035	.697	.486
Mate waarin men zich kwetsbaar voelt voor *hacking*					
(Constant)	5.217	.636		8.208	<,001
Financiële positie	.002	.010	.011	.220	.826
Mate waarin men kennis heeft over beschermende maatregelen tegen *hacking*					
(Constant)	3.900	.611		6.380	<,001
Financiële positie	.028	.009	.149	3.003	.003
Mate waarin met het nemen van maatregelen tegen *hacking* uitvoerbaar acht					
(Constant)	5.716	.495		11.539	<,001
Financiële positie	.013	.007	.088	1.764	.078
Ervaart negatieve gevoelens bij *hacking* als risico					
(Constant)	4.712	.757		6.223	<,001
Financiële positie	.014	.011	.064	1.276	.203
Grootte van de kans die men schat om gehackt te worden					
(Constant)	6.279	.676		9.294	<,001
Financiële positie	-.009	,010	-.043	-.850	.396
Mate van ernst die men toekent aan de gevolgen van *hacking*					
(Constant)	4.874	.662		7.360	<,001
Financiële positie	.025	.010	.123	2.476	.014

- Tabel vervolgt op de volgende pagina -

Mate waarin men invloed uit hun sociale omgeving ervaart om beschermende maatregelen tegen *hacking* te nemen					
(Constant)	2.788	.751		3.711	<,001
Financiële positie	.019	.011	.083	1.653	.099
Mate waarin men technische maatregelen neemt tegen *hacking*					
(Constant)	2.891	.665		4.349	<,001
Financiële positie	.043	.010	.210	4.284	<.001
Mate waarin men het online gedrag aanpast tegen *hacking*					
(Constant)	3.897	.599		6.502	<,001
Financiële positie	.035	.009	.194	3.944	<.001
Digitaal *guardianship* (als totale schaal)					
(Constant)	4.457	.323		13.815	<,001
Financiële positie	.019	.005	.193	3.925	<.001

Tabel 7: *resultaten van lineaire regressieanalyses.*

De onafhankelijke variabele is steeds 'financiële positie', met sequentieel de indicatoren voor 'digitaal *guardianship*', en afsluitend het concept als schaal zelf.

4.6 Indicatoren voor digitaal *guardianship*: het verband met slachtofferschap van hacking

De indicatoren van digitaal *guardianship* die verband houden met iemands FP zijn nu bekend. Dan resteert de vraag welke van deze indicatoren ook verband houden met de kans op slachtofferschap van *hacking*. Deze indicatoren kunnen worden meegenomen in een multinomiale logistische regressieanalyse waarin het mediërend effect van deze indicatoren getoetst kan worden.

De indicatoren van digitaal *guardianship* die verband houden met FP zijn conform het methodologisch kader allen opgenomen in een multinomiale logistische regressie, waarin hun effect op de kans op slachtofferschap van *hacking* is geanalyseerd. Hieruit blijkt dat enkel de 'ernst die men aan de gevolgen van *hacking* toekent' significant positief (tegen hypothese 3 in) verband houdt met de kans op slachtofferschap van *hacking*. Dit geldt voor de respondenten die een enkele keer slachtoffer zijn geworden van *hacking*. Hierbij is echter ogenschijnlijk sprake van een omgekeerd effect. De respondenten die al eens slachtoffer zijn geweest van hacking, beschouwen de gevolgen van *hacking* mogelijk als relatief ernstig. Hierover volgt meer in het discussiehoofdstuk.

In een losstaande multinomiale logistische regressieanalyse vertoont het concept 'digitaal *guardianship*' als schaal eveneens een significant positief verband met de kans op slachtofferschap van *hacking*. Hypothese 3 "er bestaat een negatief verband tussen iemands

digitale *guardianship* en diens kans op slachtofferschap van *hacking*", is daarmee verworpen. De exacte resultaten van de multinomiale logistische regressieanalyses zijn in tabel 8 te vinden.

Slachtofferschap van *hacking*		B	Std. Error	Sig.	Exp(B)
Een enkele keer	Intercept	-1.069	.710	.132	
	Mate waarin men maatschappelijke aandacht ervaart voor *hacking*	-.117	.068	.085	.889
	Mate waarin men kennis heeft over *hacking* als risico	-.039	.071	.579	.961
	Mate waarin men kennis heeft over beschermende maatregelen tegen *hacking*	.011	.080	.890	1.011
	Mate van ernst die men toekent aan de gevolgen van *hacking*	.178	.058	.002	1.195
	Mate waarin men technische maatregelen neemt tegen *hacking*	.021	.066	.749	1.021
	Mate waarin men het online gedrag aanpast tegen *hacking*	.002	.067	.982	1.002
	Digitaal *guardianship* (als totale schaal)*	.244	.107	.037	1.251
vaker	Intercept	-2.082	.947	.028	
	Mate waarin men maatschappelijke aandacht ervaart voor *hacking*	-.148	.089	.099	.863
	Mate waarin men kennis heeft over *hacking* als risico	.145	.098	.137	1.156
	Mate waarin men kennis heeft over beschermende maatregelen tegen *hacking*	-.002	.108	.983	.998
	Mate van ernst die men toekent aan de gevolgen van *hacking*	.144	.075	.054	1.155
	Mate waarin men technische maatregelen neemt tegen *hacking*	.103	.091	.260	1.108
	Mate waarin men het online gedrag aanpast tegen *hacking*	-.086	.083	.299	.917
	Digitaal *guardianship* (als totale schaal)*	.521	.152	<.001	1.683

Tabel 8: *resultaten van de multinomiale logistische regressieanalyses.*

De referentiecategorie is 'nooit'.

'Slachtofferschap van hacking' is de afhankelijke variabele; de indicatoren van 'digitaal guardianship' die significant verband hielden met FP, zijn de onafhankelijke variabelen.

*Hoewel opgenomen in dezelfde tabel, is 'digitaal *guardianship*' als schaal onafhankelijk van de rest in een aparte analyse opgenomen.

4.7 Betrouwbaarheid en interne samenhang van *guardianship* uit emotionele en materiële steun

Ter beoordeling van de betrouwbaarheid en interne samenhang van *guardianship* uit emotionele en materiele steun, is dezelfde benadering gehanteerd als bij 'digitaal *guardianship*'. Enkel vervalt bij een concept dat slechts twee indicatoren kent de relevantie van een principale componentenanalyse, evenals van het beoordelen van Cronbach's Alpha indien een indicator zou worden weggehaald. Cronbach's Alpha voor '*guardianship* uit emotioneel en materiële steun' als schaal is .750, wat in lijn ligt met het vooraf gestelde doel om een waarde van tussen de .7 en .8 te behalen (tabel 9).

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.750	.757	2

Tabel 9: *Cronbach's Alpha bij 'guardianship uit emotionele en materiële steun' als schaal.*

4.8 Indicatoren voor *guardianship* uit emotionele en materiële steun: het verband met FP

Het vaststellen van de indicatoren voor '*guardianship* uit emotionele en materiële steun' die zowel verband houden met FP als met het slachtofferschap van cyberagressie, begint met de connectie tussen FP en deze indicatoren. Hiertoe zijn alle indicatoren opgenomen in enkelvoudige lineaire regressieanalyses, waaruit de volgende resultaten voort zijn gekomen. FP houdt significant positief verband met de mate waarin men (op momenten dat het nodig is) emotionele steun uit hun sociale omgeving ervaart. Voor het verband tussen FP en de mate waarin men (op momenten dat het nodig is) financiële steun uit hun sociale omgeving ervaart, is geen significantie aangetroffen.

Daarnaast is het hele concept als schaal geanalyseerd, waarbij een lineaire regressieanalyse is uitgevoerd met FP als onafhankelijke variabele en '*guardianship* uit emotionele en materiële steun' als gemiddelde van de verschillende indicatoren, als afhankelijke variabele. Hieruit blijkt eveneens een significant positief verband tussen FP en *guardianship* uit emotionele en materiële steun. Hypothese 5 "er bestaat een positief verband tussen iemands financiële positie (FP) en diens *guardianship* uit emotionele en materiële ondersteuning", is daarmee aangenomen. De exacte resultaten van de lineaire regressieanalyses bij de indicatoren en het concept zelf, staan in tabel 10 vermeld.

Mate waarin men emotionele steun ervaart uit hun sociale omgeving	B	Std. Error	Beta	t	Sig.
(Constant)	3.950	.724		5.453	<.001
Financiële positie	.037	.011	.169	3.414	<.001
Mate waarin men financiële steun ervaart uit hun sociale omgeving					
(Constant)	4.431	.877		5.051	<.001
Financiële positie	.017	.013	.066	1.329	.185
Guardianship uit emotionele en materiële steun (als schaal)*					
(Constant)	4.190	.719		5.829	<.001
Financiële positie	.027	.011	.126	2.531	.012

Tabel 10: *resultaten van lineaire regressieanalyses.*

De onafhankelijke variabele is steeds 'financiële positie', met sequentieel 'emotionele steun' en 'financiële steun' als afhankelijke variabelen.

*Hoewel opgenomen in dezelfde tabel, is 'digitaal *guardianship*' als schaal onafhankelijk van de rest in een aparte analyse opgenomen.

4.9 Indicatoren voor *guardianship* uit emotionele en materiële steun: het verband met slachtofferschap van cyberagressie

De indicatoren van '*guardianship* uit emotionele en materiële steun' die verband houden met iemands FP zijn nu bekend. Dit blijk enkel 'de mate waarin men (op momenten dat het nodig is) emotionele steun uit hun sociale omgeving ervaart' te zijn. Dan resteert de vraag of deze indicator ook verband houdt met de kans op slachtofferschap van cyberagressie. Dit zou betekenen dat deze indicator kan worden meegenomen in een multinomiale logistische regressieanalyse waarin het mediërend effect van deze indicator getoetst kan worden.

De indicator 'de mate waarin men (op momenten dat het nodig is) emotionele steun uit hun sociale omgeving ervaart' is conform het methodologisch kader opgenomen in een multinomiale logistische regressie. Hierin is het effect dat deze indicator heeft op de kans op slachtofferschap van cyberagressie geanalyseerd. Hieruit blijkt dat geen sprake is van een significant verband met het slachtofferschap van cyberagressie. Het hele concept '*guardianship* uit emotionele en materiële steun' als schaal vertoont in een aparte multinomiale logistische regressieanalyse dan ook geen significant verband met de kans op slachtofferschap van cyberagressie. Hypothese 6 "er bestaat een negatief verband tussen iemands *guardianship* uit emotionele en materiële ondersteuning, en diens kans om slachtoffer te worden van cyberagressie", is daarmee verworpen. De exacte resultaten van de multinomiale logistische regressieanalyses zijn in tabel 11 te vinden.

Slachtofferschap van cyberagressie		B	Std. Error	Sig.	Exp(B)
Een enkele keer	Intercept	-1.086	.339	.001	
	Emotionele steun	-.033	.061	.596	.968
	Guardianship uit emotionele en materiële steun (als schaal)*	.049	.049	.317	1.050
Vaker	Intercept	-1.414	.418	<.001	
	Emotionele steun	-.151	.080	.061	.860
	Guardianship uit emotionele en materiële steun (als schaal)*	-.005	.065	.936	.995

Tabel 11: *resultaten van de multinomiale logistische regressieanalyses.*

De referentiecategorie is 'nooit'.

'Slachtofferschap van cyberagressie' is de afhankelijke variabele; de indicator emotionele steun' die als enige significant verband hield met FP, is de onafhankelijke variabele.

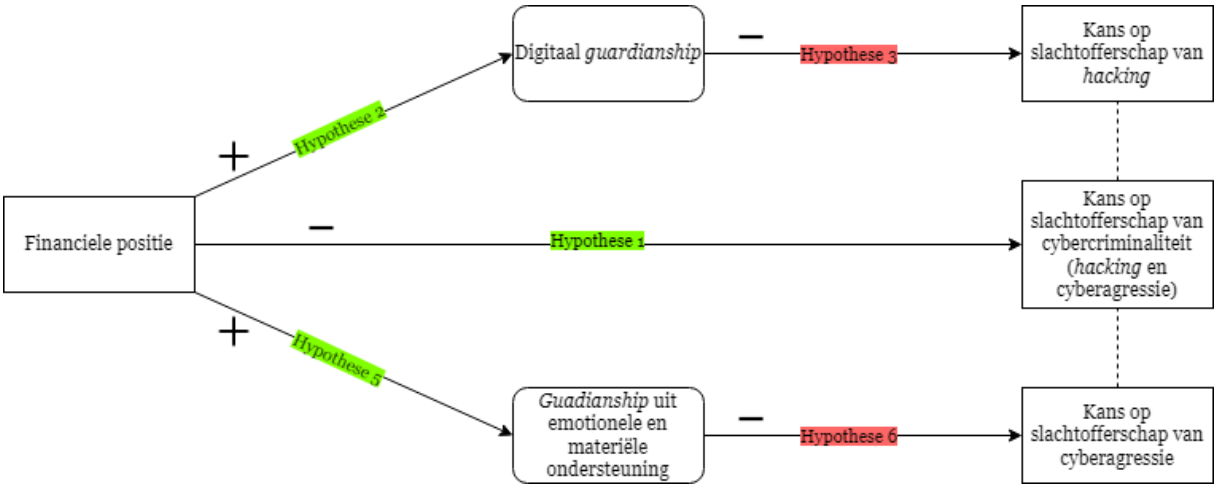
*Hoewel opgenomen in dezelfde tabel, is 'digitaal *guardianship*' als schaal onafhankelijk van de rest in een aparte analyse opgenomen.

4.10 *Guardianship* als mediërende variabele tussen FP en slachtofferschap van hacking en cyberagressie?

De getoetste relaties tussen FP en het slachtofferschap van *hacking* en cyberagressie, evenals tussen FP en de indicatoren voor beide vormen van *guardianship* (en de concepten zelf), hebben grotendeels significante resultaten opgeleverd. Voor de laatste theoretische connecties daarentegen, tussen de indicatoren voor beide vormen van *guardianship* en het slachtofferschap van *hacking* en cyberagressie, zijn geen resultaten gevonden die in lijn liggen met de hypothesen. Daarmee is het fundament voor een groter regressiemodel waarin potentieel mediërende variabelen kunnen worden opgenomen komen te vervallen. Daarmee zijn hypothese 4 "iemands digitale *guardianship* vertoont een negatief mediërend verband tussen iemands financiële positie (FP) en diens kans op slachtofferschap van *hacking*" en hypothese 7 "iemands *guardianship* uit emotionele en materiële ondersteuning vertoont een negatief mediërend verband tussen iemands financiële positie (FP) en diens kans op slachtofferschap van cyberagressie" verworpen.

4.11 Samenvatting

Figuur 5 presenteert het conceptueel model van dit onderzoek opnieuw. De resultaten van de analyses zijn nu in het model verwerkt, zodat zichtbaar is geworden welke hypothesen uit het conceptueel model significant zijn gebleken en welke niet. Hypothesen 4 en 7 staan niet nadrukkelijk vernoemd in de figuur, maar daarvan is impliciet duidelijk dat zij verworpen zijn omdat het mediërende pad dat zij vertegenwoordigen niet voltooid wordt. De verwerpingen van hypothesen 3 en 6 belemmeren dit immers.



Figuur 5: *samenvatting van de resultaten.*

Groen: hypothese aangenomen. Rood: hypothese verworpen.

5. CONCLUSIE & DISCUSSIE

De centrale vraagstelling van dit onderzoek luidde: “Wat is het effect van iemands financiële positie (FP) op de kans op slachtofferschap van cybercrime (*hacking* en cyberpesten [later cyberagressie]) in politiedistrict Gelderland-Midden, en welke causale mechanismen spelen hierin een rol?”. Gegeven de uitkomsten van de analyses zoals gepresenteerd in het voorgaande hoofdstuk, valt te concluderen dat de FP waarin men verkeert een relevante voorspeller is van diens kans op slachtofferschap van zowel *hacking* als cyberagressie. Naarmate iemands FP beter is, wordt het minder waarschijnlijk dat die persoon slachtoffer wordt van *hacking* of cyberagressie. Dat verklaart mede waarom individuen die in een bemoeilijkte FP verkeren, vaker slachtoffer worden van deze delicten, zoals in lijn ligt met de statistieken van het CBS die in de inleiding zijn aangehaald. Dit gevonden verband is echter niet sterk, en betreft enkel de groep mensen die ‘vaker’ slachtoffer zijn geworden van *hacking* en cyberagressie.

Verder hangt de FP waarin men verkeert in positieve richting samen met de gehypothetiseerde mediërende variabelen ‘digitaal *guardianship*’ en ‘*guardianship* uit emotionele en materiële steun’. Hoewel niet alle indicatoren van deze concepten verband houden met FP, dient de relatie tussen FP en deze twee vormen van weerbaarheid serieus te worden genomen. De indicatoren die wél samenhangen met FP, vormen namelijk potentieel bruikbare informatie wat betreft de inhoud van risicocommunicatie in toekomstig preventief cybercrimebeleid.

Om van deze potentie gebruik te kunnen maken, zal echter eerst vervolgonderzoek moeten plaatsvinden. De relatie tussen de mediërende *guardianship*-constructen en het slachtofferschap van *hacking* en/of cyberagressie is namelijk in dit onderzoek niet aangetoond. Veelal bleken deze verbanden niet significant, of bleken ze significant in de tegenovergestelde richting van de geformuleerde hypothese. Hoewel deze analyseresultaten voor ‘*guardianship* uit emotionele en materiële steun’ te verhalen kunnen zijn op een onjuiste theoretische benadering van dit mediërende verband, lijkt er bij ‘digitaal *guardianship*’ iets anders aan de hand te zijn.

Dit vormt dan ook het eerste punt van discussie. Uit de analyses die de verworpen hypothese 3 “er bestaat een negatief verband tussen iemands digitale *guardianship* en diens kans op slachtofferschap van *hacking*” toetsten, zijn namelijk significant positieve resultaten gekomen. Dit zou betekenen dat respondenten die een hogere mate van digitaal *guardianship* kennen, vaker slachtoffer zouden worden van *hacking*. Dit staat echter tegenover de geraadpleegde literatuur over digitaal *guardianship* in het theoretisch kader, en is daarmee een onwaarschijnlijke bevinding.

Wat wel een mogelijke verklaring zou kunnen zijn, is dat respondenten die in het verleden ooit slachtoffer zijn geworden van *hacking*, na dat moment ervoor hebben gekozen om zichzelf beter te beschermen in het digitale domein. Dat zou een mogelijke verklaring

kunnen zijn waarom respondenten zowel hoge scores op indicatoren voor digitaal *guardianship* hebben, als aangeven ooit eens of meermaals te zijn gehackt. Dit lijkt enigszins op wat Helsloot en Scholtens (2015) beschrijven als een 'risico-regelreflex'. Hoewel niet op bestuurlijk niveau, is het een vergelijkbare neiging om na een incident direct de middelen uit te trekken om te voorkomen dat een vergelijkbaar toekomstig incident en/of de gevolgen van een toekomstig incident zich niet nogmaals voordoen. Hoewel de gesprekken met de respondenten buiten de enquêteresultaten om niet zijn vastgelegd, en daarmee geen officieel verzamelde data zijn, werd dit incident-maatregelscenario meermaals genoemd. Een aantal respondenten zou nadat ze gehackt waren, een ICT-expert hebben ingehuurd om hun systemen en netwerken beter te beveiligen. Hier zijn wederom de meer vermogende respondenten makkelijker toe in staat.

Indien dit onderzoek gerepliceerd zou worden, of in een andere vorm een vervolg zou krijgen, dient dan ook gecontroleerd te worden voor de volgorde waarin iemands digitale weerbaarheid is ontwikkeld. Gedroeg iemand zich voor eventueel slachtofferschap van *hacking* al voorzichtig op het internet, of is dat gedrag daarna pas ontstaan? Hetzelfde geldt voor genomen technische maatregelen. Alleen met een onderzoeksdesign waarin dit element is opgenomen, kan voor deze drijvende kracht gecontroleerd worden in de relatie tussen digitaal *guardianship* en de kans op slachtofferschap van *hacking*. Zodoende zou vervolgonderzoek mogelijk, in tegenstelling tot dit onderzoek, wel in staat zijn om een volledige analyse kunnen uitvoeren van de relatie tussen FP en slachtofferschap van *hacking*, onder mediërende invloed van digitaal *guardianship*. Daarmee zou de potentiële bruikbaarheid van de informatie over de relatie tussen FP en digitaal *guardianship* voor toepassing in risicocommunicatie verwezenlijkt worden.

Een tweede punt van discussie is de representativiteit en heterogeniteit van de steekproef(populatie). Hoewel qua leeftijd en geslacht niet sterk wordt afgeweken van het provinciaal gemiddelde, is onder hoog- en laagopgeleiden sprake van over- en onderrepresentatie, respectievelijk. Dit is ook wat heeft geleid tot een compositie-effect, blijkt uit de onderzoeksresultaten. De scheef verdeelde representatie op het gebied van opleidingsniveau is verklaarbaar: Walter en Davis (2016) hebben een verband aangetoond tussen opleidingsniveau en bereidheid om deel te nemen aan (klinisch) onderzoek.

Een vraag die hieruit voortkomt, is in hoeverre in dit onderzoek voldoende spreiding op de variabele FP bestaat, uitgaande van enige samenhang tussen opleidingsniveau en inkomen (Wolla & Sullivan, 2017). Hoewel gedurende het proces van dataverzameling meerdere pogingen zijn gedaan om meer respondenten te werven die in de eerdergenoemde categorie '(langdurig) lage inkomens' van het CBS vallen, is deze doelgroep lastig bereikbaar gebleken. Vervolgonderzoek zou dan ook idealiter (mede) via (gemeentelijke) kanalen moeten waardoor de laagstopgeleiden en laagste inkomens een groter aandeel in de gebruikte

steekproef zouden kennen. Het gebruik van een onderzoekspanel zou dit ook kunnen faciliteren, evenals dat het grotere formaat van de steekproef dan beter de betrouwbaarheid van het onderzoek zou handhaven, gegeven de heterogeniteit van de steekproef(populatie). Een keerzijde van deze methode zou zijn dat het arbeidsintensiever wordt om een grotere steekproef mondeling te woord te blijven staan, in tegenstelling tot het overstappen op een digitale enquête. Daarmee zou de validiteit die dit onderzoek kenmerkt deels moeten worden ingeruild voor nieuw gewonnen betrouwbaarheid.

Een derde punt van discussie is de theoretische achtergrond van het mechanisme achter het slachtofferschap van cyberagressie, die niet in lijn ligt met de bevindingen. De *guardianship* uit emotionele en materiële steun bleek immers geenszins verband te houden met het slachtofferschap van cyberagressie. De theoretische fundering en operationalisatie voor deze vorm van *guardianship* was ook minder sterk dan die van 'digitaal *guardianship*'. De hiervoor gebruikte literatuur is voornamelijk gericht op jongeren en de context waarin jongeren opereren, welke een voedingsbodem kan zijn voor cyberagressie. In lijn met deze aangehaalde literatuur is dan ook de bevinding in dit onderzoek dat een significant negatief verband bestaat tussen iemands leeftijd en diens kans om slachtoffer te worden van cyberagressie. Hoe verder mensen van de status 'jongere' af staan, en daarmee ook van de context waarin jongeren opereren, hoe minder groot de kans is dat men slachtoffer wordt van cyberagressie.

Een vierde punt van theoretische discussie is het gebruik van de CFPB-schaal als meetinstrument voor FP. Hoewel blijkt dat deze methode een grote beantwoordingsbereidheid heeft opgeleverd, wat gunstig is gegeven de sensitieve aard van het onderwerp en de N-waarde van 'slechts' 400, laat het type vragen ruimte voor subjectiviteit bij de beantwoording. Waar de ene respondent bij de vraag over het bereiken van diens financiële doelen al tevreden is wanneer de respondent zichzelf kan voorzien in diens bierconsumptie, en daar 9 of 10 beantwoordt; kan een andere respondent, die wellicht vermogender is en een groter doel voor ogen heeft, bij die vraag een 7 of 8 beantwoorden. Hoewel de FP van respondent 2 over het algemeen als beter beschouwd kan worden, is het doel dat men voor zichzelf stelt doorslaggevend in hun antwoord, en eindigt respondent 1 bij deze vraag met een hogere score. Daar komt bij dat de ene respondent aangeeft zichzelf laag te beoordelen en daarom een 5 als antwoord opgeeft, terwijl een andere respondent qua intonatie en woordkeus tot een vergelijkbare visie op zichzelf komt, en hier vervolgens een 1 of 2 als score aan koppelt. Hoewel opvallende cijfertoekenningen niet vaak voor zijn gekomen, en doorvragen al snel tot genuanceerdere antwoorden heeft geleid, laat de CFPB-schaal wel de ruimte voor dit type onzuiverheden.

Het geheel overziend, is het geformuleerde interne doel van dit onderzoek ten dele bereikt. De negatieve relatie tussen FP en het slachtofferschap van *hacking* en cyberagressie is

geverifieerd. Tegelijkertijd zijn de potentiële achterliggende mechanismen slechts deels in beeld gebracht; en zal vervolgonderzoek moeten uitwijzen of de aanleiding die dit onderzoek biedt om het mediërend effect van digitaal *guardianship* tussen FP en slachtofferschap van *hacking* verder te onderzoeken, ook resulteert in significante uitkomsten.

Daarmee is het externe doel "tot concrete en gefundeerde beleidsmaatregelen te kunnen komen waarmee politiedistrict Gelderland-Midden (en de driehoek) de cyberweerbaarheid van de beoogde doelgroep kan stimuleren", ook ten dele bereikt. De gevonden relatie tussen iemands FP en diens kans op slachtofferschap van *hacking* en cyberagressie schijnt namelijk licht op een relevante doelgroep voor risicocommunicatie omtrent cybercriminaliteit. Daarmee krijgt cyberweerbaarheidsbeleid een concrete en wetenschappelijk gefundeerde invulling. Op het gebied van *hacking* zijn in dit onderzoek ook aanwijsbare weerbaarheidsfactoren naar voren gekomen die onderdeel zouden kunnen vormen in het mechanisme tussen iemands FP en diens kans op slachtofferschap van *hacking*. Deze factoren kunnen de concrete inhoud vormen van risicocommunicatie richting mensen met een (langdurig) laag inkomen, omdat specifiek deze factoren in dit onderzoek verband hielden met de FP van de onderzochte respondenten. Zo zou risicocommunicatie over *hacking* ingevuld kunnen worden met boodschappen die mensen met een (langdurig) laag inkomen bewuster maken over de ernst van de gevolgen van *hacking*, of boodschappen die hun kennis over '*hacking* als risico' verhoogt. Deze weerbaarheidsfactoren houden namelijk mede verband met de FP van respondenten.

De woorden 'zouden' en 'kunnen' worden hierboven gebruikt, omdat zoals eerder aangegeven, een volledige relatie tussen FP en slachtofferschap van *hacking* of cyberagressie met tussenkomst van weerbaarheidsfactoren niet kon worden aangetoond in dit onderzoek. Om deze relatie op betrouwbaardere wijze alsnog aan te kunnen tonen, zal hetzelfde onderzoek op grotere schaal gerepliceerd moeten worden, waarbij ook gecompenseerd dient te worden voor eventuele veranderingen in individuele cyberweerbaarheid na cyberincidenten.

Daarmee vormt dit onderzoek een discussiestuk voor de beleidsmakers van de driehoek, waarbij het civiele cybervraagstuk met dit onderzoek een financieel component heeft gekregen. Omdat onderzoekers die vanuit gemeentelijke kanalen dit onderzoek zouden repliceren wellicht betere toegang hebben tot financieel kwetsbare mensen, gegeven de rol van de gemeente en de plaats die de gemeente in het beleidsnetwerk van het sociale domein inneemt. Hierdoor zou een grotere (representatievere) diversiteit op de scores van FP en opleidingsniveau kunnen worden bewerkstelligd, waardoor gevonden verbanden mogelijk sterker uit analyses naar voren komen. Hoewel altijd voor sciëntisme gewaakt dient te worden, zou dergelijk vervolgonderzoek een relatief minder betwistbare fundatie vormen voor de invulling van risicocommunicatie vanuit de veiligheidsdriehoek omtrent *hacking* en cyberagressie.

BIBLIOGRAFIE

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

AlleCijfers. (2022). *Heel veel informatie over provincie Gelderland (update 2022!)*. AlleCijfers.nl. Geraadpleegd op 12 juni 2022, van https://allecijfers.nl/provincie/gelderland/

Belsley, D. A., Kuh, E., & Welsch, R. E. (1980). *Regression Diagnostics - Identifying Influential Data and Sources of Collinearity* (1ste editie). Wiley & Sons, Inc. https://doi.org/10.1002/0471725153

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie*. Sdu. https://www.politieenwetenschap.nl/cache/files/62c57e190b68fPK102.pdf

CBS. (2016, 24 februari). *Cyberpesten*. Geraadpleegd op 31 maart 2022, van https://www.cbs.nl/nl-nl/nieuws/2013/30/een-op-tien-jongeren-gepest-op-internet/cyberpesten

CBS. (2019[a], juli). *Digitale Veiligheid & Criminaliteit 2018*. Centraal Bureau voor de Statistiek. https://www.cbs.nl/-/media/_pdf/2019/29/veiligheid-en-criminaliteit.pdf

CBS. (2019[b], december 9). *De sociale context van armoede - Armoede en sociale uitsluiting 2019*. Centraal Bureau voor de Statistiek. Geraadpleegd op 22 maart 2022, van https://longreads.cbs.nl/armoede-en-sociale-uitsluiting-2019/de-sociale-context-van-armoede/

CBS. (2019[c], 16 juli). *Hacken*. Geraadpleegd op 31 maart 2022, van https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit/hacken

CBS. (2021[a]-03-01). *Scherpe daling traditionele vormen van criminaliteit*. Geraadpleegd op 17 maart 2022, van https://www.cbs.nl/nl-nl/nieuws/2021/09/scherpe-daling-traditionele-vormen-van-criminaliteit

CBS. (2021[b]-02-25). *Inwoners per gemeente*. Centraal Bureau voor de Statistiek. Geraadpleegd op 28 april 2022, van https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking/regionaal/inwoners

CBS. (2022[a], maart 1). *Minder traditionele criminaliteit, meer online criminaliteit*. Geraadpleegd op 17 maart 2022, van https://www.cbs.nl/nl-nl/nieuws/2022/09/minder-traditionele-criminaliteit-meer-online-criminaliteit

CBS. (2022[b], april 20). *Beloningen*. Geraadpleegd op 10 juni 2022, van https://www.cbs.nl/nl-nl/deelnemers-enquetes/beloningen

CBS. (2022[c], 25 februari). *Leeftijdsverdeling*. Centraal Bureau voor de Statistiek. Geraadpleegd op 28 juni 2022, van https://www.cbs.nl/nl-nl/visualisaties/dashboard-bevolking/leeftijd/bevolking#:%7E:text=Gemiddeld%20zijn%20inwoners%20van%20Nederland%2042%2C3%20jaar%20oud.

CBS-InUwBuurt. (2022). *Gemiddeld inkomen per inwoner - Wijken*. Centraal Bureau voor de Statistiek. Geraadpleegd op 24 april 2022, van https://cbsinuwbuurt.nl/#wijken2018_gemiddeld_inkomen_inwoner

CFPB. (2022[a]). *Financial Well-Being full scorecard*. Consumer Financial Protection Bureau. https://files.consumerfinance.gov/f/documents/bcfp_fin-well-being_full-scorecard.pdf

CFPB. (2022[b], februari 19). *Measuring financial well-being: A guide to using the CFPB Financial Well-Being Scale*. Consumer Financial Protection Bureau. Geraadpleegd op 23 februari 2022, van https://www.consumerfinance.gov/data-research/research-reports/financial-well-being-scale/

Chen, Q., Lo, C. K., Zhu, Y., Cheung, A., Chan, K. L., & Ip, P. (2018). Family poly-victimization and cyberbullying among adolescents in a Chinese school sample. *Child Abuse & Neglect*, *77*, 180–187. https://doi.org/10.1016/j.chiabu.2018.01.015

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review*, *46*(5), 505. https://doi.org/10.2307/2094935

Curtin University Library. (2021). *Descriptive statistics - Introduction to statistics - UniSkills - Curtin Library*. LibGuides. Geraadpleegd op 4 maart 2022, van https://uniskills.library.curtin.edu.au:443/numeracy/statistics/descriptive/

Duncan, G. J., & Petersen, E. (2001). The Long and Short of Asking Questions about Income, Wealth, and Labor Supply. *Social Science Research*, *30*(2), 248–263. https://doi.org/10.1006/ssre.2000.0696

EdeInCijfers. (2022). *Beroepsbevolking in beeld*. Gemeente Ede. Geraadpleegd op 28 april 2022, van https://ede.incijfers.nl/dashboard/ede-in-cijfers/economie--werk-en-inkomen/

Eden, S., Heiman, T., & Olenik-Shemesh, D. (2014). Bully versus victim on the internet: The correlation with emotional-social characteristics. *Education and Information Technologies*, *21*(3), 699–713. https://doi.org/10.1007/s10639-014-9348-2

Field, A. (2018). *Discovering Statistics Using IBM SPSS Statistics* (5de editie). SAGE Publications.

Gallo, A. (2022, 2 februari). *A Refresher on Regression Analysis*. Harvard Business Review. Geraadpleegd op 4 maart 2022, van https://hbr.org/2015/11/a-refresher-on-regression-analysis

Gardella, J. H., Fisher, B. W., Teurbe-Tolon, A. R., Ketner, B., & Nation, M. (2019). Students' Reasons for Why They Were Targeted for In-School Victimization and Bullying. *International Journal of Bullying Prevention*, *2*(2), 114–128. https://doi.org/10.1007/s42380-019-00017-7

Gemeente Arnhem. (2022). *Armoede en inkomensondersteuning (buurt/wijk)*. Arnhem in Cijfers. Geraadpleegd op 28 april 2022, van https://arnhem.incijfers.nl/dashboard/staat-van-de-stad/armoede-en-inkomensondersteuning--buurt-wijk-

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405

Guerra, C., & Ingram, J. R. (2020). Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, *43*(1), 44–60. https://doi.org/10.1080/01639625.2020.1774707

Hay, C., & Ray, K. (2020). General Strain Theory and Cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 583–600. https://doi.org/10.1007/978-3-319-78440-3_21

Hayes, C. (2022). *Limitations to Correlation and Regression*. Montana State University. Geraadpleegd op 4 maart 2022, van https://math.montana.edu/hayes/powerpoint-lectures/l2_4/01.html

Heckman, J. J. (2010). Selection Bias and Self-Selection. *Microeconometrics*, 242–266. https://doi.org/10.1057/9780230280816_29

Helsloot, I., & Groenendaal, J. (2014, januari). *Naar meer inzicht in de politiële netwerkpraktijk in de casus cybercrime, zeehavens en veiligheidshuizen* (Nr. BSK14-01). Radboud University. https://crisislab.nl/wordpress/wp-content/uploads/Naar-meer-inzicht-in-de-politie%CC%88le-netwerkpraktijk-in-de-casus-cybercrime-zeehavens-en-veiligheidshuizen.pdf

Helsloot, I., Pieterman, R., & Hanekamp, J. C. (2010). *Risico's en redelijkheid*. Boom Lemma.

Helsloot, I., Scholtens, A. (2015). *Crisisbeheersing en veiligheidszorg - Krachten rond de risico-regelreflex beschreven en geïllustreerd in 27 voorbeelden* (1ste editie). Boom Lemma.

Henson, B. (2020). Routine Activities. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 469–489. https://doi.org/10.1007/978-3-319-78440-3_23

Holt, T. J., & Bossler, A. M. (2013). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Izmeth, R. (2015, 22 augustus). *Evolution of Strengths and Weaknesses of Online Surveys*. ResearchGate. Geraadpleegd op 21 april 2022, van https://www.researchgate.net/publication/305348901_Evolution_of_Strengths_and_Weaknesses_of_Online_Surveys

Jansen, P. W., Verlinden, M., Berkel, A. D. V., Mieloo, C., Van der Ende, J., Veenstra, R., Verhulst, F. C., Jansen, W., & Tiemeier, H. (2012). Prevalence of bullying and

victimization among children in early elementary school: Do family and school neighbourhood socioeconomic status matter? *BMC Public Health*, *12*(1). https://doi.org/10.1186/1471-2458-12-494

Kaspersky. (2022, 9 februari). *What is a Zero-day Attack? - Definition and Explanation*. Www.Kaspersky.Com. Geraadpleegd op 11 april 2022, van https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Kingston, S., & Webster, C. (2015a). The most 'undeserving' of all? How poverty drives young men to victimisation and crime. *Journal of Poverty and Social Justice*, *23*(3), 215–227. https://doi.org/10.1332/175982715x14448287452303

Kingston, S., & Webster, C. (2015b). The most 'undeserving' of all? How poverty drives young men to victimisation and crime. *Journal of Poverty and Social Justice*, *23*(3), 215–227. https://doi.org/10.1332/175982715x14448287452303

Lanier, M. M., Henry, S., & Anastasia, D. J. M. (2015). *Essential Criminology* (4de editie). Routledge.

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

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit*. WODC, Ministerie van Justitie en Veiligheid. https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Levitt, S. D. (1999). The Changing Relationship between Income and Crime Victimization. *FRBNY ECONOMIC POLICY REVIEW*, 87–98.

Lewandowski, C. A., & Hill, T. J. (2009). The Impact of Emotional and Material Social Support on Women's Drug Treatment Completion. *Health & Social Work*, *34*(3), 213–221. https://doi.org/10.1093/hsw/34.3.213

Michael Collins, J., & Urban, C. (2019). Measuring financial well-being over the lifecourse. *The European Journal of Finance*, *26*(4–5), 341–359. https://doi.org/10.1080/1351847x.2019.1682631

Ministerie van Justitie en Veiligheid. (2021, 21 januari). *Vervolging van cyberboef nog niet zo gemakkelijk: OM laat knelpunten zien*. Nieuwsbericht | Openbaar Ministerie. Geraadpleegd op 17 maart 2022, van https://www.om.nl/actueel/nieuws/2021/01/21/vervolging-van-cyberboef-nog-niet-zo-gemakkelijk-om-laat-knelpunten-zien

Miró, F. (2014). Routine Activity Theory. *The Encyclopedia of Theoretical Criminology*, 1–7. https://doi.org/10.1002/9781118517390.wbetc198

Misana-ter Huurne, E., Van 't Hoff-de Goede, S., Bekkers, L., Van Houten, Y., Walther, M., Spithoven, R., & Leukfeldt, R. (2021). *Cyberweerbaarheid - Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime*. Regieorgaan SIA. https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/cyberweerbaarheid_deelrapport-wp1_2.pdf

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793. http://www.cybercrimejournal.com/ngo2011ijcc.pdf

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? *Criminal Justice Review*, *45*(4), 430–451. https://doi.org/10.1177/0734016820934175

Nilsson, A., & Estrada, F. (2006). The Inequality of Victimization. *European Journal of Criminology*, *3*(4), 387–412. https://doi.org/10.1177/1477370806067910

Patchin, J. W., & Hinduja, S. (2010). Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory. *Youth & Society*, *43*(2), 727–751. https://doi.org/10.1177/0044118x10366951

Politie. (2022, februari). *Jaarplan Cyber-digi GLM 2022–2023 [intern document]*.

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, *3*(9), 369–387. https://doi.org/10.1080/1351847x.2019.1682631

Schuilenburg, M., Besseling, B., & Uitendaal, F. (2017). Vertrouwen in de politie. *Justitiële verkenningen*, *43*(4), 47–63. https://doi.org/10.5553/jv/016758502017043004005

Seo, H. J., Jung, Y. E., Kim, M. D., & Bahk, W. M. (2017). Factors associated with bullying victimization among Korean adolescents. *Neuropsychiatric Disease and Treatment*, *Volume 13*, 2429–2435. https://doi.org/10.2147/ndt.s140535

Shaheen, A. M., Hammad, S., Haourani, E. M., & Nassar, O. S. (2018). Factors Affecting Jordanian School Adolescents' Experience of Being Bullied. *Journal of Pediatric Nursing*, *38*, e66–e71. https://doi.org/10.1016/j.pedn.2017.09.003

Spithoven, R., Foppen, E., Van Houten, Y., & Misana-ter Huurne, E. (2020, december). *Naar een cyberweerbaar Amersfoort*. Hogeschool Saxion. https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/rapportage-cyberweerbaarheid-burgerpanel-amersfoort---def-extern.pdf

Thacher, D. (2004). The Rich Get Richer and the Poor Get Robbed: Inequality in U.S. Criminal Victimization, 1974–2000. *Journal of Quantitative Criminology*, *20*(2), 89–116. https://doi.org/10.1023/b:joqc.0000029090.28541.4f

Van 't Hoff-de Goede, M. S., Leukfeldt, E. R., Van der Kleij, R., & Van de Weijer, S. G. A. (2021). The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization. *Cybercrime in Context*, *1*, 21–41. https://doi.org/10.1007/978-3-030-60527-8_3

Van de Weijer, S. G. A., Leukfeldt, E. R., & Van der Zee, S. (2020a). *Slachtoffer van onlinecriminaliteit, wat nu?* (Nr. 120). Sdu. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2020/slachtoffer-van-onlinecriminaliteit-wat-nu-356/

Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020b). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17–34. https://doi.org/10.1108/pijpsm-07-2019-0122

Vennix, J. (2016). *Onderzoeks- en interventiemethodologie* (6de editie). Pearson Benelux B.V.

Wall, D. (2004). Cybercrimes and the internet. In D. Wall (Red.), *Crime and the internet - Cybercrimes and Cyberfears* (pp. 1–14). Taylor & Francis.

Walter, J. K., & Davis, M. M. (2016). Who's Willing? Characteristics Associated with Willingness to Participate in Clinical Research. *The Hastings Center*, *38*(2), 15–21. https://www.jstor.org/stable/26776035

Wohlfarth, T., Winkel, F. W., Ybema, J. F., & Van den Brink, W. (2001). The relationship between socio-economic inequality and criminal victimisation: a prospective study. *Social Psychiatry and Psychiatric Epidemiology*, *36*(7), 361–370. https://doi.org/10.1007/s001270170042

Wolla, S. A., & Sullivan, J. (2017, 3 januari). *Education Income And Wealth*. Economic Research - Federal Reserve Bank of St. Louis. Geraadpleegd op 6 juli 2022, van https://research.stlouisfed.org/publications/page1-econ/2017/01/03/education-income-and-wealth/#:%7E:text=The%20relationship%20between%20education%20and,incomes%20(see%20the%20table).

Yar, M. (2005). The Novelty of 'Cybercrime'. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yucedal, B. (2010, augustus). *VICTIMIZATION IN CYBERSPACE: AN APPLICATION OF ROUTINE ACTIVITY AND LIFESTYLE EXPOSURE THEORIES*. Kent State University. https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=kent1279290984&disposition=attachment

BIJLAGE 1: SYNTAX

```
* Encoding: UTF-8.
DELETE VARIABLES StartDate EndDate Status IPAddress Progress
Duration__in_seconds_ Finished RecordedDate RecipientLastName RecipientFirstName
RecipientEmail ExternalReference ResponseId
   LocationLatitude LocationLongitude DistributionChannel UserLanguage Vdslbnk

Variable level Lftd (Ordinal)

Recode Lftd (CONVERT) INTO Leeftijd.

COMPUTE FinPosRaw=fn_ctrl_1 + fn_tgvllr_1 + brkn_fn_dln_1 + fn_kzs_lvnsglk_1.

DO IF  (Lftd < '62').
RECODE FinPosRaw (0=14) (1=19) (2=22) (3=25) (4=27) (5=29) (6=31) (7=32) (8=34)
(9=35) (10=37)
   (11=38) (12=40) (13=41) (14=42) (15=44) (16=45) (17=46) (18=47) (19=49) (20=50)
(21=51) (22=52)
   (23=54) (24=55) (25=56) (26=58) (27=59) (28=60) (29=62) (30=63) (31=65) (32=66)
(33=68) (34=69)
   (35=71) (36=73) (37=75) (38=78) (39=81) (40=86) (SYSMIS=0) INTO FinPos1861.
END IF.

DO IF  (Lftd >'61').
RECODE FinPosRaw (0=14) (SYSMIS=0) (1=20) (2=24) (3=26) (4=29) (5=31) (6=33)
(7=35) (8=36)
   (9=38) (10=39) (11=41) (12=42) (13=44) (14=45) (15=46) (16=48) (17=49) (18=50)
(19=52) (20=53)
   (21=54) (22=56) (23=57) (24=58) (25=60) (26=61) (27=63) (28=64) (29=66) (30=67)
(31=69) (32=71)
   (33=73) (34=75) (35=77) (36=79) (37=82) (38=84) (39=81) (40=95) INTO FinPos62.
END IF.

Variable level FinPos1861 (Ordinal)

Variable level FinPos62 (Ordinal)

COMPUTE FinPosDEF=FinPos1861 + FinPos62.

RECODE Qhckngslchtffr (1=1) (2=2) (SYSMIS=SYSMIS) (ELSE=3) INTO HackingSlchtffr.

RECODE Qcbrgrssslchtffr (1=1) (2=2) (SYSMIS=SYSMIS) (ELSE=3) INTO AgressieSlchtffr.

VARIABLE LEVEL AgressieSlchtffr (SCALE)

VARIABLE LEVEL HackingSlchtffr (SCALE)

VALUE LABELS
   AgressieSlchtffr
   0 'nooit'
   1 'een enkele keer'
```

```
   2 'vaker'.


VALUE LABELS
   HackingSlchtffr
   0 'nooit'
   1 'een enkele keer'
   2 'vaker'.


REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA COLLIN TOL
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT HackingSlchtffr
  /METHOD=ENTER Bdrgng_1 Mtsch_ndcht_1 knnsrsc_1 prsgvlghd_1 kwtsbrhckng_1
knnsbschrmndmtrgln_1
    gdrg_tvrbr_1 gdrg_ffctf_1 ngtvgvlnshckng_1 knsghcktwrdn_1 rnstgvlgnhckng_1
sc_mgvng_ffct_1
    tchnsch_mtrgln_1 npssng_nlngdrg_1


REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA COLLIN TOL
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT AgressieSlchtffr
  /METHOD=ENTER mtnl_stn_1 fnncl_stn_1


COMPUTE trbedreig=ln(Bdrgng_1)*Bdrgng_1.
COMPUTE traandacht=ln(Mtsch_ndcht_1)*Mtsch_ndcht_1.
COMPUTE trkennisrsc=ln(knnsrsc_1)*knnsrsc_1.
COMPUTE trprikkel=ln(prsgvlghd_1)*prsgvlghd_1.
COMPUTE trkwetsbaar=ln(kwtsbrhckng_1)*kwtsbrhckng_1.
COMPUTE trkennisbeschrm=ln(knnsbschrmndmtrgln_1)*knnsbschrmndmtrgln_1.
COMPUTE truitvoerbaar=ln(gdrg_tvrbr_1)*gdrg_tvrbr_1.
COMPUTE treffectief=ln(gdrg_ffctf_1)*gdrg_ffctf_1.
COMPUTE trneggevoel=ln(ngtvgvlnshckng_1)*ngtvgvlnshckng_1.
COMPUTE trkans=ln(knsghcktwrdn_1)*knsghcktwrdn_1.
COMPUTE trernst=ln(rnstgvlgnhckng_1)*rnstgvlgnhckng_1.
COMPUTE trsocinvloed=ln(sc_mgvng_ffct_1)*sc_mgvng_ffct_1.
COMPUTE trtechnisch=ln(tchnsch_mtrgln_1)*tchnsch_mtrgln_1.
COMPUTE trgedrag=ln(npssng_nlngdrg_1)*npssng_nlngdrg_1.
COMPUTE tremosteun=ln(mtnl_stn_1)*mtnl_stn_1.
COMPUTE trfinsteun=ln(fnncl_stn_1)*fnncl_stn_1.
COMPUTE trfinposDEF=ln(FinPosDEF)*FinPosDEF.
```

```
RECODE HackingSlchtffr (1=1) (SYSMIS=SYSMIS) (ELSE=2) INTO DummyHacking.

RECODE AgressieSlchtffr (1=1) (SYSMIS=SYSMIS) (ELSE=2) INTO DummyAgressie.

COMPUTE Digitaal_Guardianship=Bdrgng_1 + Mtsch_ndcht_1 + knnsrsc_1 + prsgvlghd_1
+ kwtsbrhckng_1 +
    knnsbschrmndmtrgln_1 + gdrg_tvrbr_1 + ngtvgvlnshckng_1 + knsghcktwrdn_1 +
    rnstgvlgnhckng_1 + sc_mgvng_ffct_1 + tchnsch_mtrgln_1 + npssng_nlngdrg_1.

Compute E_F_SteunGuardian=fnncl_stn_1 + mtnl_stn_1.

VALUE LABELS
   DummyHacking
   1 'nooit gehackt'
   2 'ooit gehackt'.

VALUE LABELS
   DummyAgressie
   1 'nooit AgrSlachtoffer'
   2 'ooit AgrSlachtoffer'.

FACTOR
  /VARIABLES Bdrgng_1 Mtsch_ndcht_1 knnsrsc_1 prsgvlghd_1 kwtsbrhckng_1
knnsbschrmndmtrgln_1
    gdrg_tvrbr_1 gdrg_ffctf_1 ngtvgvlnshckng_1 knsghcktwrdn_1 rnstgvlgnhckng_1
sc_mgvng_ffct_1
    tchnsch_mtrgln_1 npssng_nlngdrg_1
  /MISSING LISTWISE
  /ANALYSIS Bdrgng_1 Mtsch_ndcht_1 knnsrsc_1 prsgvlghd_1 kwtsbrhckng_1
knnsbschrmndmtrgln_1
    gdrg_tvrbr_1 gdrg_ffctf_1 ngtvgvlnshckng_1 knsghcktwrdn_1 rnstgvlgnhckng_1
sc_mgvng_ffct_1
    tchnsch_mtrgln_1 npssng_nlngdrg_1
  /PRINT UNIVARIATE INITIAL DET KMO EXTRACTION ROTATION
  /PLOT EIGEN ROTATION
  /CRITERIA MINEIGEN(1) ITERATE(25)
  /EXTRACTION PC
  /CRITERIA ITERATE(25) DELTA(0)
  /ROTATION OBLIMIN
  /METHOD=CORRELATION.

RELIABILITY
  /VARIABLES=Bdrgng_1 Mtsch_ndcht_1 knnsrsc_1 prsgvlghd_1 kwtsbrhckng_1
knnsbschrmndmtrgln_1
    gdrg_tvrbr_1 gdrg_ffctf_1 ngtvgvlnshckng_1 knsghcktwrdn_1 rnstgvlgnhckng_1
sc_mgvng_ffct_1
    tchnsch_mtrgln_1 npssng_nlngdrg_1
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=CORR
```

```
  /SUMMARY=TOTAL.

RELIABILITY
  /VARIABLES=mtnl_stn_1 fnncl_stn_1
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=CORR
  /SUMMARY=TOTAL.

LOGISTIC REGRESSION VARIABLES DummyHacking
  /METHOD=ENTER Bdrgng_1 Mtsch_ndcht_1 knnsrsc_1 prsgvlghd_1 kwtsbrhckng_1
knnsbschrmndmtrgln_1
    gdrg_tvrbr_1 gdrg_ffctf_1 ngtvgvlnshckng_1 knsghcktwrdn_1 rnstgvlgnhckng_1
sc_mgvng_ffct_1
    tchnsch_mtrgln_1 npssng_nlngdrg_1 trbedreig traandacht trkennisrsc trprikkel
trkwetsbaar
    trkennisbeschrm truitvoerbaar treffectief trneggevoel trkans trernst trsocinvloed
trtechnisch
    trgedrag
  /CRITERIA=PIN(.05) POUT(.10) ITERATE(20) CUT(.5).

LOGISTIC REGRESSION VARIABLES DummyAgressie
  /METHOD=ENTER mtnl_stn_1 fnncl_stn_1 trfinsteun tremosteun
  /CRITERIA=PIN(.05) POUT(.10) ITERATE(20) CUT(.5).

LOGISTIC REGRESSION VARIABLES DummyHacking
  /METHOD=ENTER FinPosDEF trfinposDEF
  /CRITERIA=PIN(.05) POUT(.10) ITERATE(20) CUT(.5).

LOGISTIC REGRESSION VARIABLES DummyAgressie
  /METHOD=ENTER FinPosDEF trfinposDEF
  /CRITERIA=PIN(.05) POUT(.10) ITERATE(20) CUT(.5).

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Digitaal_Guardianship
  /METHOD=ENTER FinPosDEF
  /SCATTERPLOT=(*ZRESID ,*ZPRED).

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Guardianship_E_M_steun
  /METHOD=ENTER FinPosDEF
  /SCATTERPLOT=(*ZRESID ,*ZPRED).
```

```
FREQUENCIES VARIABLES=Gndr Leeftijd
  /PERCENTILES=1.0
  /STATISTICS=MEAN MEDIAN
  /ORDER=ANALYSIS.

USE ALL.
COMPUTE filter_$=(Pldng = 1).
VARIABLE LABELS filter_$ 'Pldng = 1 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.

FREQUENCIES VARIABLES=Pldng
  /ORDER=ANALYSIS.

USE ALL.
COMPUTE filter_$=(RANGE(Pldng,2,4)).
VARIABLE LABELS filter_$ 'RANGE(Pldng,2,4) (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.

FREQUENCIES VARIABLES=Pldng
  /ORDER=ANALYSIS.

USE ALL.
COMPUTE filter_$=(Pldng >= 5).
VARIABLE LABELS filter_$ 'Pldng >= 5 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.

FREQUENCIES VARIABLES=Pldng
  /ORDER=ANALYSIS.

FILTER OFF.
USE ALL.

FREQUENCIES VARIABLES=HackingSlchtffr AgressieSlchtffr
  /ORDER=ANALYSIS.

NOMREG HackingSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH FinPosDEF Gndr
Pldng Leeftijd
  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5) CHKSEP(20) LCONVERGE(0)
PCONVERGE(0.000001)
    SINGULAR(0.00000001)
  /MODEL
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.
```

```
NOMREG AgressieSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH FinPosDEF Gndr
Pldng Leeftijd
  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5) CHKSEP(20) LCONVERGE(0)
PCONVERGE(0.000001)
    SINGULAR(0.00000001)
  /MODEL
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Bdrgng_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Mtsch_ndcht_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT knnsrsc_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT prsgvlghd_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
```

```
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT kwtsbrhckng_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT knnsbschrmndmtrgln_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT gdrg_tvrbr_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT gdrg_ffctf_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT ngtvgvlnshckng_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT knsghcktwrdn_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.
```

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT rnstgvlgnhckng_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT sc_mgvng_ffct_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT tchnsch_mtrgln_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT npssng_nlngdrg_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Digitaal_Guardianship
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

NOMREG HackingSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH Mtsch_ndcht_1
knnsrsc_1
    knnsbschrmndmtrgln_1 gdrg_ffctf_1 rnstgvlgnhckng_1 tchnsch_mtrgln_1
npssng_nlngdrg_1
  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5) CHKSEP(20) LCONVERGE(0)
PCONVERGE(0.000001)
```

```
   SINGULAR(0.00000001)
  /MODEL
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.

NOMREG HackingSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH
Digitaal_Guardianship
  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5) CHKSEP(20) LCONVERGE(0)
PCONVERGE(0.000001)
   SINGULAR(0.00000001)
  /MODEL
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT mtnl_stn_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT fnncl_stn_1
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT Guardianship_E_M_steun
  /METHOD=ENTER FinPosDEF
  /RESIDUALS DURBIN.

NOMREG AgressieSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH mtnl_stn_1
fnncl_stn_1
  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5) CHKSEP(20) LCONVERGE(0)
PCONVERGE(0.000001)
   SINGULAR(0.00000001)
  /MODEL
```

```
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.

NOMREG AgressieSlchtffr (BASE=FIRST ORDER=ASCENDING) WITH
Guardianship_E_M_steun  /CRITERIA CIN(95) DELTA(0) MXITER(100) MXSTEP(5)
CHKSEP(20) LCONVERGE(0) PCONVERGE(0.000001)
    SINGULAR(0.00000001)
  /MODEL
  /STEPWISE=PIN(.05) POUT(0.1) MINEFFECT(0) RULE(SINGLE) ENTRYMETHOD(LR)
REMOVALMETHOD(LR)
  /INTERCEPT=INCLUDE
  /PRINT=PARAMETER SUMMARY LRT CPS STEP MFI.
```

BIJLAGE 2: RESULTATEN VAN ASSUMPTIETOETSEN

Onafhankelijkheid van observaties (Durbin-Watson test)

Afhankelijke variabele:	Durbin-Watson
De mate waarin een respondent *hacking* als dreiging ervaart.	2.031
Mate waarin men maatschappelijke aandacht ervaart voor *hacking*.	1.925
Mate waarin men kennis heeft over *hacking* als risico.	1.904
Mate waarin men persoonlijke risicogevoeligheid ervaart.	2.043
Mate waarin men zich kwetsbaar voelt voor *hacking*.	1.947
Mate waarin men kennis heeft over beschermende maatregelen tegen *hacking*.	2.138
Mate waarin met het nemen van maatregelen tegen *hacking* uitvoerbaar acht.	2.104
Mate waarin men het nemen van maatregelen tegen *hacking* effectief acht.	2.069
Ervaart negatieve gevoelens bij *hacking* als risico.	1.930
Grootte van de kans die men schat om gehackt te worden.	1.776
Mate van ernst die men toekent aan de gevolgen van *hacking*.	1.761
Mate waarin men invloed uit hun sociale omgeving ervaart om beschermende maatregelen tegen *hacking* te nemen.	2.040
Mate waarin men technische maatregelen neemt tegen *hacking*.	2.211
Mate waarin men het online gedrag aanpast tegen *hacking*.	1.934
Mate waarin men emotionele steun ervaart uit hun sociale omgeving.	2.067
Mate waarin men financiële steun ervaart uit hun sociale omgeving.	2.054

Tabel 12: *Durbin-Watson test per lineaire regressieanalyse, tussen onafhankelijke variabele FP en alle guardianship-indicatoren (afhankelijke variabelen).* Waarden buiten de range 1-3 zijn kritiek

Multicollineariteit (Pearson correlation, collinearity diagnostics, collinearity statistics)

Digitaal *Guardianship*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Hacking als dreiging =A	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Maatsch. aandacht voor *hacking* =B	.115*	-	-	-	-	-	-	-	-	-	-	-	-	-
Kennis over risico *hacking* =C	.098*	.186*	-	-	-	-	-	-	-	-	-	-	-	-
Persoonlijke risicogevoeligheid =D	.337*	.189*	.151*	-	-	-	-	-	-	-	-	-	-	-
Gevoel kwetsbaarheid voor *hacking* =E	.555*	.142*	.107*	.404*	-	-	-	-	-	-	-	-	-	-
Kennis beschermende maatregelen *hacking* =F	.092*	.180*	.639*	.164*	.055	-	-	-	-	-	-	-	-	-
Uitvoerbaarheid maatregelen *hacking* =G	.025	.174*	.155*	.127*	-.018	.348*	-	-	-	-	-	-	-	-
Effectiviteit maatregelen *hacking* =H	.080	.078	.052	.159*	-.027	.114*	.387*	-	-	-	-	-	-	-
Negatieve gevoelens bij *hacking* =I	.462*	.150*	.050	.420*	.434*	.081	.079	.093*	-	-	-	-	-	-
Kans op slachtofferschap *hacking* =J	.349*	.045	.068	.132*	.502*	.020	-.093*	-.175*	.274*	-	-	-	-	-
Ernst gevolgen slachtofferschap *hacking* =K	.303*	.221*	.046	.290*	.315*	.065	.000	-.002	.335*	.147*	-	-	-	-
Invloed soc. omgeving op zelfbescherming *hacking* =L	.228*	.230*	-.026	.196*	.158*	.029	.076	.100*	.244*	.100*	.224*	-	-	-
Technische maatregelen tegen *hacking* =M	.208*	.111*	.414*	.159*	.078	.528*	.172*	.163*	.113*	.058	.174*	.136*	-	-
Aanpassing online gedrag tegen *hacking* =N	.111*	.132*	.317*	.162*	.181*	.346*	.109*	.085*	.180*	.089*	.158*	.175*	.474*	-

Tabel 13: *Pearson correlation voor de indicatoren van 'digitaal guardianship'*

*= significant bij α=.05 (1-tailed)

Dimension	Condition Index	(Constant)	HAD	MAH	KRH	PRG	GKH	KBH	UMH	EMH	NGH	KSH	EGH	IOZ	TMH	AOG
1	1.000	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00	.00
2	6.734	.00	.01	.00	.03	.01	.01	.03	.00	.00	.03	.01	.00	.24	.02	.01
3	7.549	.00	.02	.00	.00	.01	.04	.00	.00	.00	.02	.04	.00	.57	.01	.00
4	9.845	.00	.01	.02	.02	.13	.02	.01	.03	.05	.04	.18	.01	.07	.04	.01
5	10.459	.01	.01	.07	.01	.12	.00	.01	.03	.03	.13	.12	.00	.00	.08	.01
6	11.866	.00	.02	.02	.12	.28	.02	.02	.00	.02	.08	.01	.09	.05	.12	.05
7	12.264	.00	.03	.07	.00	.03	.00	.01	.04	.05	.16	.01	.47	.01	.00	.01
8	12.635	.00	.08	.09	.06	.15	.03	.02	.00	.04	.47	.00	.01	.00	.08	.00
9	13.129	.00	.38	.02	.04	.12	.00	.02	.00	.00	.02	.12	.03	.00	.00	.25
10	14.500	.00	.03	.16	.00	.05	.17	.03	.01	.00	.00	.24	.15	.01	.03	.30
11	15.115	.00	.01	.49	.08	.04	.08	.01	.01	.02	.01	.05	.15	.03	.27	.05
12	16.894	.01	.12	.00	.29	.03	.38	.21	.11	.05	.00	.04	.00	.00	.04	.05
13	17.954	.00	.28	.00	.14	.04	.24	.15	.06	.17	.04	.01	.00	.01	.22	.21
14	21.432	.00	.00	.01	.18	.00	.00	.48	.60	.36	.00	.01	.00	.00	.08	.00
15	28.007	.97	.01	.04	.02	.00	.01	.00	.10	.22	.01	.14	.07	.00	.01	.05

Tabel 14: *collinearity diagnostics voor de indicatoren van 'digitaal guardianship'*

HAD: hacking als dreiging. MAH: maatschappelijke aandacht voor *hacking*. KRH: kennis over risico *hacking*. PRG: persoonlijke risicogevoeligheid. GKH: gevoel kwetsbaarheid voor *hacking*. KBH: kennis beschermende maatregelen tegen *hacking*. UMH: uitvoerbaarheid maatregelen *hacking*. EMH: effectiviteit maatregelen *hacking*. NGH: negatieve gevoelens bij *hacking*. KSH: Kans op slachtofferschap *hacking*. EGH: ernst gevolgen slachtofferschap *hacking*. IOZ: invloed sociale omgeving op zelfbescherming *hacking*. TMH: technische maatregelen tegen *hacking*. AOG: aanpassing online gedrag tegen *hacking*.

	Tolerance	VIF
Hacking als dreiging	.583	1.716
Maatsch. aandacht voor *hacking*	.857	1.166
Kennis over risico *hacking*	.554	1.803
Persoonlijke risicogevoeligheid	.705	1.419
Gevoel kwetsbaarheid voor *hacking*	.502	1.992
Kennis beschermende maatregelen *hacking*	.454	2.203
Uitvoerbaarheid maatregelen *hacking*	.733	1.364
Effectiviteit maatregelen *hacking*	.785	1.274
Negatieve gevoelens bij *hacking*	.647	1.545
Kans op slachtofferschap *hacking*	.698	1.433
Ernst gevolgen slachtofferschap *hacking*	.782	1.279
Invloed soc. omgeving op zelfbescherming *hacking*	.843	1.186
Technische maatregelen tegen *hacking*	.576	1.735
Aanpassing online gedrag tegen *hacking*	.710	1.409

Tabel 15: *collinearity statistics voor de indicatoren van 'digitaal guardianship'.*

Guardianship uit emotionele en materiële steun

	Emotionele steun	Financiële steun
Emotionele steun	-	-
Financiële steun	.610*	-

Tabel 16: *Pearson correlation voor de indicatoren van 'guardianship uit emotionele en materiele steun'.*

*= significant bij α=.05 (1-tailed)

	Condition			
Dimension	Index	(Constant)	Emotionele steun	Financiële steun
1	1.000	.01	.01	.02
2	4.925	.51	.00	.63
3	7.209	.47	.99	.36

Tabel 17: Collinearity diagnostics voor de indicatoren van 'guardianship uit emotionele en materiële steun'.

	Tolerance	VIF
Emotionele steun	.628	1.591
Financiele steun	.628	1.591

Tabel 18: collinearity statistics voor de indicatoren van *guardianship* uit emotionele en financiele steun

Lineariteit van de logit (Box-Tidwell procedure)

Digitaal *Guardianship*

	B	S.E.	Sig.	Exp(B)
HAD	.453	.620	.465	1.573
MAH	-.605	.876	.490	.546
KRH	1.020	.638	.110	2.772
PRG	-.075	.565	.895	.928
GKH	-1.197	.725	.099	.302
KBH	-.150	.671	.822	.860
UMH	-.310	.965	.748	.734
EMH	-.680	.936	.468	.507
NGH	.382	.527	.469	1.465
KSH	.169	.643	.792	1.184
EGH	1.404	.785	.074	4.072
IOZ	.458	.389	.239	1.581
TMH	-.338	.550	.540	.714
AOG	-.065	.642	.919	.937
TR-HAD	-.192	.231	.406	.826
TR-MAH	.173	.327	.598	1.188
TR-KRH	-386	.245	.115	.680
TR-PRG	-.027	.216	.900	.973
TR-GKH	.521	.276	.059	1.684
TR-KBH	.065	.257	.801	1.067
TR-UMH	.128	.351	.715	1.137
TR-EMH	.247	.342	.470	1.280
TR-NGH	-.110	.197	.578	.896
TR-KSH	-.011	.240	.965	.990
TR-EGH	-.457	.281	.104	.633
TR-IOZ	-.172	.159	.278	.842
TR-TMH	.161	.214	.451	1.175
TR-AOG	-.011	.246	.963	.989
Constant	-2.226	2.755	.419	.108

Tabel 19: *Box-Tidwell procedure uitgevoerd op de indicatoren voor 'digitaal guardianship'.*

'TR' staat voor de getransformeerde variabelen (ln(VAR)*VAR). HAD: hacking als dreiging. MAH: maatschappelijke aandacht voor *hacking*. KRH: kennis over risico *hacking*. PRG: persoonlijke risicogevoeligheid. GKH: gevoel kwetsbaarheid voor *hacking*. KBH: kennis beschermende maatregelen tegen *hacking*. UMH: uitvoerbaarheid maatregelen *hacking*. EMH: effectiviteit maatregelen *hacking*. NGH: negatieve gevoelens bij *hacking*. KSH: Kans op slachtofferschap *hacking*. EGH: ernst gevolgen slachtofferschap *hacking*. IOZ: invloed sociale omgeving op zelfbescherming *hacking*. TMH: technische maatregelen tegen *hacking*. AOG: aanpassing online gedrag tegen *hacking*. α=.05

Guardianship uit emotionele en financiële steun

	B	S.E.	Sig.	Exp(B)
Emotionele steun	-.051	.354	.885	.950
Financiële steun	.535	.283	.058	1.708
TR-emotionele steun	-.183	.113	.105	.832
TR-financiële steun	-.010	.136	.941	.990
Constant	-1.121	.553	.043	.326

Tabel 20: *Box-Tidwell procedure uitgevoerd op de indicatoren voor 'guardianship uit emotionele en financiële steun'.*

'TR' staat voor de getransformeerde variabelen (ln(VAR)*VAR). α=.05

Financiële positie

	B	S.E.	Sig.	Exp(B)
Financiële positie	-.033	.366	.929	.968
TR-Financiële positie	.004	.071	.957	1.004
Constant	.695	4.505	.877	2.004

Tabel 21: *Box-Tidwell procedure uitgevoerd op de variabele 'financiële positie', ten opzichte van een binomiale versie van 'slachtofferschap van hacking'.*

'TR' staat voor de getransformeerde variabele (ln(VAR)*VAR). α=.05

	B	S.E.	Sig.	Exp(B)
Financiële positie	-,089	,398	,823	,915
TR-Financiële positie	,010	,077	,896	1,010
Constant	2,521	4,860	,604	12,437

Tabel 22: *Box-Tidwell procedure uitgevoerd op de variabele 'financiële positie', ten opzichte van een binomiale versie van 'slachtofferschap van cyberagressie.*

'TR' staat voor de getransformeerde variabele (ln(VAR)*VAR). α=.05