# Samenvatting

Online criminaliteit vormt een belangrijk maatschappelijk probleem dat door de digitalisering van de maatschappij in allerlei verschijningsvormen opduikt, zoals pogingen tot oplichting via verkoopsites en online bedreigingen. De continue aansluiting van mensen op het internet creëert een grootschalige potentiële blootstelling aan online criminaliteit. In het onderhavige onderzoek staat de burgerbevolking als doelwit van diverse vormen van online criminaliteit centraal. Het doel is om beter zicht te krijgen op de omvang, risicofactoren en gevolgen van diverse vormen van online slachtofferschap.

Bij online criminaliteit wordt onderscheid gemaakt tussen cybercriminaliteit en gedigitaliseerde criminaliteit. Cybercriminaliteit betreft misdrijven waarbij zowel het middel als het doel een component van informatie- en communicatietechnologie (ICT) bevat. Computervirussen en hacken, waarbij onrechtmatig toegang tot computers, e-mailaccounts of online bankierplatformen wordt verkregen, zijn voorbeelden van cybercriminaliteit. Bij gedigitaliseerde criminaliteit gaat het om misdrijven waarbij alleen het middel een ICT-component bevat en het misdrijf gericht is op de persoon, zoals online bedreiging (bijvoorbeeld via e-mail of social media) en oplichting (zoals aan- of verkoopfraude). Het huidige onderzoek omvat delicten uit beide typen online criminaliteit.

De meerwaarde van het huidige onderzoek is het gebruik van longitudinale paneldata, verzameld tussen 2008 en 2018. De volgorde waarin verschillende gebeurtenissen, gedragingen en gemoedstoestanden zich bij mensen voordoen, kunnen in deze panelstudie duidelijk in de tijd worden geplaatst. Hierdoor is dit onderzoek beter in staat risicofactoren en gevolgen van online slachtofferschap in kaart te brengen dan eerdere cross-sectionele studies die gebruik hebben gemaakt van data verzameld op één meetmoment.

Er is gekeken naar slachtofferschap van zeven online delicten: creditcard fraude, gehackt worden, online aankoopfraude, online bedreiging, het oplopen van een computervirus, ongeautoriseerde bankafschrijving en identiteitsfraude. Allereerst is onderzocht hoe vaak online slachtofferervaringen de afgelopen jaren voorkomen en hoe ernstig deze zijn. Ten tweede is gekeken naar de risicofactoren van verschillende vormen van online slachtofferschap. Risicofactoren die onder de loep zijn genomen, zijn onder andere leeftijd, geslacht, opleidingsniveau, online gedragingen en verschillende persoonlijkheidskenmerken waaronder impulsiviteit. Tevens is vergeleken in hoeverre de risicofactoren van online slachtofferschap overeenkomen met risicofactoren van offline slachtofferschap. Ten derde is onderzocht in hoeverre online slachtofferervaringen samengaan met veranderingen in online gedragingen en welbevinden van burgers. Tot slot is herhaald slachtofferschap in kaart gebracht en is onderzocht of de eerdergenoemde risicofactoren ook verklaren waarom sommige burgers een grotere kans hebben om opnieuw slachtoffer te worden van online criminaliteit.

## Vraagstelling

De centrale vraagstelling van het onderzoek is als volgt: wat zijn patronen van (herhaald) slachtofferschap van online criminaliteit en in hoeverre kunnen die

worden verklaard door persoonskenmerken, online gedragingen en de gevolgen van eerder slachtofferschap?

Op basis van empirisch onderzoek zijn de volgende onderzoeksvragen beantwoord:
1 In welke mate ervaren Nederlandse burgers slachtofferschap van online criminaliteit?
2 In hoeverre hangt online slachtofferschap samen met eerdere slachtoffererva-ringen, internetgebruik, beschermingsmaatregelen en persoonskenmerken?
3 In hoeverre heeft online slachtofferschap gevolgen voor angst voor online criminaliteit, internetgebruik, beschermingsmaatregelen en mentale gezondheids-problemen?
4 In welke mate is er sprake van herhaald slachtofferschap en in welke mate vormen de mogelijke gevolgen van online slachtofferschap een verklaring voor patronen in herhaald slachtofferschap?

## Methoden

In dit onderzoek is gebruikgemaakt van het LISS-panel, een online dataverzameling onder een representatieve steekproef van Nederlandse huishoudens, waarin panel-leden sinds 2007 maandelijks online een wisselende vragenlijst invullen over onder andere hun persoonlijkheid, werksituatie en vrijetijdsbesteding. Sinds februari 2008 heeft eens in de twee jaar ook een uitgebreide slachtofferenquête plaatsgevonden, waarin respondenten zijn gevraagd naar slachtoffererervaringen van diverse vormen van offline en online criminaliteit. Inmiddels is er sprake van zes meetmomenten (2008-2018), waarbij iedere keer vijf- à zesduizend respondenten hebben mee-gewerkt. Aan de hand van deze longitudinale panelgegevens zijn de prevalentie, risicofactoren en gevolgen van (herhaald) online slachtofferschap bestudeerd.

## Resultaten

*Online slachtofferschap gedaald tussen 2010 en 2018*

Uit de resultaten blijkt een significante daling in de prevalentie van slachtofferschap van de totaalscore van de zeven typen online delicten, van 15,1% in 2010 naar 9,5% in 2018. Ook het type online delict blijkt veranderd te zijn, in 2010 komen computervirussen het meest voor, in 2018 is dit aankoopfraude. Het aantal perso-nen dat aangeeft slachtoffer te zijn geweest van offline delicten is hoger dan dat van online delicten, al is ook deze prevalentie significant gedaald (van 20,5% in 2010 naar 12,4% in 2018). De daling in online slachtofferschap is vooral te zien in de daling in het aantal slachtoffers van computervirussen (8,9% in 2010 en 1,7% in 2018). In iets mindere mate is tevens een daling in het aantal slachtoffers van hacken (1,4% in 2010 en 0,9% in 2018) en ongeautoriseerde bankafschrijvingen (3,0% in 2010 en 1,2% in 2018) te zien. Daarentegen zijn de prevalenties van online aankoopfraude en identiteitsfraude in diezelfde periode significant gestegen, respectievelijk van 2,4% in 2010 naar 4,4% in 2018 en van 0,1% naar 0,3%. Bij een aantal online delicten is gevraagd of slachtoffers aangifte hebben gedaan, waaruit blijkt dat slechts een minderheid van de slachtoffers naar de politie stapt. 11,6% van de slachtoffers van ongeautoriseerde bankafschrijving heeft aangifte gedaan bij de politie. Bij slachtoffers van online aankoopfraude is dit 12,0%, bij online bedreiging 20,2% en bij identiteitsfraude 46,0%.

*Onder andere eerdere slachtoffers, jongeren, mannen en frequente internetgebruikers hebben meer risico op online slachtofferschap*

Eerdere slachtofferervaringen hangen samen met de kans op een nieuwe slachtofferervaring: respondenten die tijdens een eerder meetmoment hebben aangegeven slachtoffer te zijn geweest van online criminaliteit, hebben een grotere kans ook op een volgend meetmoment slachtoffer te zijn. Verder hebben respondenten die meer gebruikmaken van internet een grotere kans om slachtoffer van online criminaliteit te worden. De kans op online slachtofferschap is echter niet geassocieerd met het aantal genomen beschermingsmaatregelen tijdens een voorgaand meetmoment. Daarnaast hangen diverse persoonskenmerken samen met de kans op online slachtofferschap. Zowel jongere als mannelijke respondenten hebben een grotere kans om slachtoffer te worden van online criminaliteit. Daarnaast blijken respondenten die impulsief, open of emotioneel instabiel zijn vatbaarder voor online slachtofferschap. Leeftijd, emotionele instabiliteit en openheid vormen ook risicofactoren van offline criminaliteit. Geslacht vormt voor beide vormen van criminaliteit een risicofactor. Waar mannen een grotere kans hebben om slachtoffer te worden van online criminaliteit, hebben vrouwen juist een grotere kans om slachtoffer te worden van offline criminaliteit. Een hogere score op altruïsme en een lagere score op consciëntieusheid hangen samen met offline slachtofferschap, maar niet met online slachtofferschap. Impulsiviteit is de enige risicofactor die enkel is voorbehouden aan online slachtoffers, en kan daardoor worden gezien als een kenmerkende risicofactor van online criminaliteit.

*Angst neemt toe, maar mentale gezondheid verslechtert niet na online slachtofferschap*

Slachtoffers van online criminaliteit hebben na hun slachtofferervaring meer angst voor online criminaliteit dan voorheen. Deze angst zou er mogelijk voor kunnen zorgen dat slachtoffers wegblijven van het internet. Echter, in het huidige onderzoek hangt slachtofferschap niet significant samen met een daling in internetgebruik. In plaats van weg te blijven van het internet, hebben respondenten nadat zij slachtoffer zijn geworden van online criminaliteit significant meer beschermingsmaatregelen getroffen. Wanneer nader onderscheid is gemaakt op basis van aangiftebereidheid, is zichtbaar dat slachtoffers die geen aangifte hebben gedaan van hun slachtofferervaring meer beschermingsmaatregelen treffen, terwijl dat niet het geval was bij slachtoffers die wel aangifte hadden gedaan. Een mogelijke verklaring is dat voornamelijk slachtoffers van computervirussen meer beschermingsmaatregelen treffen, terwijl deze slachtoffers waarschijnlijk relatief minder vaak aangifte doen bij politie dan slachtoffers van ander type delicten.
Tenslotte neemt de mentale gezondheid niet af onder de totale groep van online slachtoffers. Dat is echter wel het geval als alleen slachtoffers van online bedreiging worden meegenomen: na slachtofferschap van online bedreiging neemt het mentaal welbevinden van slachtoffers af, mogelijk omdat van de onderzochte delicten dit delict de grootste impact op iemands persoonlijke levenssfeer heeft.

*Impulsiviteit, emotionele stabiliteit en openheid belangrijke voorspellers van herhaald slachtofferschap*

Van de respondenten die tenminste tweemaal hadden deelgenomen aan de slachtofferschap-vragenlijst, gaf 16,6% aan eenmalig slachtoffer en 17,5% herhaald slachtoffer te zijn geweest van online criminaliteit. De resultaten van dit onderzoek laten zien dat mannen, of impulsieve, emotioneel instabiele of meer open respon-

denten een grotere kans hebben om herhaald slachtoffer te worden dan om eenmalig slachtoffer te worden. Impulsiviteit, emotionele instabiliteit en openheid hangen bovendien samen met de frequentie van slachtofferervaringen. De samenhang verloopt gradueel: hoe hoger men scoort op deze persoonlijkheidskenmerken, hoe vaker men kans loopt slachtoffer te worden van online criminaliteit. Deze bevinding wordt bevestigd in verschillende robuustheidsanalyses.

Daarnaast kan eerder online slachtofferschap en de gevolgen daarvan, een risicofactor vormen voor een nieuwe slachtofferervaring. Een daling in internetgebruik en mentale gezondheid zou een gevolg van eerder slachtofferschap kunnen zijn, maar deze kenmerken blijken niet te veranderen na online slachtofferschap. Hoewel internetgebruik wel samenhangt met de kans om (een eerste keer) slachtoffer te worden, vormen internetgebruik en mentale gezondheid geen verklaring waarom sommige slachtoffers *opnieuw* slachtoffer worden. Beschermingsmaatregelen nemen wel toe na een slachtofferervaring, maar het nemen van beschermingsmaatregelen lijkt vervolgens het risico op slachtofferschap niet te verlagen. Deze resultaten over herhaald slachtofferschap suggereren dat het eerder de meer stabiele persoonskenmerken zijn die herhaald slachtofferschap verklaren, dan de hier onderzochte gevolgen van een eerdere slachtofferervaring.

*Sterke punten en verbeterpunten*

Een belangrijke meerwaarde ten opzichte van eerder onderzoek is het longitudinale en representatieve karakter van het huidige onderzoek. Door mensen over een langere periode te volgen, is het in dit onderzoek mogelijk geweest om verschillende gebeurtenissen, gedragingen en gemoedstoestanden voor en na een slachtofferervaring te meten. Hiermee kunnen deze factoren duidelijker in de tijd worden geplaatst dan mogelijk is met een studie die gebruikmaakt van slechts één meetmoment. Een ander pluspunt is dat er gebruik is gemaakt van zelfrapportage van online slachtofferschap. Omdat slechts een beperkt deel van de cyber- en gedigitaliseerde criminaliteit in beeld is bij politie of justitie – in het huidige onderzoek stapte een minderheid van de online slachtoffers naar de politie – levert het gebruik van zelfrapportage naar verwachting een beter beeld op van de omvang van online slachtofferschap. De zelfrapportage kent echter ook een aantal beperkingen. Vanwege de retrospectieve aard van zelfrapportage, kunnen slachtoffers zich mogelijk gebeurtenissen niet meer (goed) herinneren of plaatsen zij gebeurtenissen eerder of later in de tijd. Naast deze beperkingen van zelfrapportage zijn in dit onderzoek niet alle typen online delicten meegenomen. Op sommige meer recent ontstane delicten, zoals malware en ransomware, is hierdoor geen zicht gekomen.

## Conclusie

De eerste conclusie van dit rapport is dat slachtofferschap van zeven typen online delicten tussen 2010 en 2018 is gedaald onder een representatieve steekproef van de Nederlandse bevolking, waarbij het meest voorkomende type online delict is verschoven van computervirussen naar aankoopfraude. Hoewel over het algemeen een dalende trend aanwezig is, laat dit onderzoek onverminderd zien dat een deel van de Nederlandse bevolking ooit slachtoffer is geworden van één van de onderzochte online delicten. Om die reden zijn ook de risicofactoren en gevolgen van deze slachtofferervaringen in kaart gebracht.

Internetgebruik blijkt – niet geheel verassend – één van de risicofactoren voor online slachtofferschap, aangezien de gelegenheid tot online criminaliteit groter is naarmate men zich meer online begeeft. Mensen die eerder online slachtoffer zijn geworden, mannen en jongere mensen, lopen ook een verhoogd risico op online slachtofferschap. Impulsieve mensen, emotioneel instabiele mensen en meer open mensen hebben daarentegen niet alleen meer kans om één keer slachtoffer te worden, maar ook om herhaald slachtoffer te worden van online criminaliteit. Een mogelijke verklaring voor de sterke samenhang tussen deze persoonlijkheidskenmerken en online slachtofferschap, is dat deze kenmerken een indicatie zijn voor online risicogedrag. Zo zullen impulsieve mensen tijdens hun handelen minder nadenken over mogelijke risico's, hebben emotioneel instabiele mensen meer moeite om risico's in te schatten, en hebben open mensen een grotere kans om online gegevens te delen. Niet alleen het internetgebruik zelf, maar ook de manier waarop men zich op het internet gedraagt, lijkt dus een risicofactor voor online slachtofferschap. Beleid dat burgers wil wijzen op online gevaren kan rekening houden met de persoonlijkheidskenmerken van potentiële slachtoffers. Waarschuwingen over online risico's hebben mogelijk een minder goede uitwerking op impulsieve mensen dan op niet-impulsieve mensen, omdat impulsieve mensen eerder geneigd zijn te handelen zonder na te denken over de mogelijke consequenties van hun online gedrag.

Het huidige onderzoek laat zien dat slachtoffers van online criminaliteit niet minder gebruikmaken van het internet na hun slachtofferervaring. Uit de literatuur naar offline slachtofferschap weten we dat die slachtoffers de plek waar het delict heeft plaatsgevonden na hun slachtofferervaring zijn gaan mijden. In deze steeds meer gedigitaliseerde samenleving is het echter voor online slachtoffers haast onmogelijk om zich aan het digitale leven te onttrekken. Slachtoffers van online criminaliteit ervaren over het algemeen geen verslechtering in hun mentale gezondheid. Alleen slachtoffers van online bedreiging laten een daling in hun mentale gezondheid zien. Slachtoffers van online criminaliteit lijken zich desalniettemin bewust van hun eerdere slachtofferervaring, gezien de bevinding dat ze gemiddeld genomen een grotere angst voor online criminaliteit rapporteren en meer beschermingsmaatregelen hebben getroffen dan vóór hun slachtofferervaring. Deze bevinding laat zien dat slachtoffers bereid zijn hun online gedrag aan te passen, en dat het relevant is (potentiële) slachtoffers te wijzen op wat ze kunnen doen om de kans op een (nieuwe) slachtofferervaring te verkleinen.