Samenvatting

De Nederlandse samenleving is in hoog tempo gedigitaliseerd. Bijna iedereen maakt dagelijks gebruikt van computer, smartphone of andere vormen van informatie- en communicatietechnologie (ICT). Naast de voordelen die deze digitalisering oplevert is er ook een schaduwzijde—cyber- en gedigitaliseerde criminaliteit.

Cybercriminaliteit betreft delicten waarbij ICT het middel en doel is. Het gaat dan bijvoorbeeld om delicten als hacken en ransomware. Gedigitaliseerde criminaliteit betreft traditionele delicten waarbij ICT als middel wordt ingezet, maar niet het doel is. Daarbij gaat het bijvoorbeeld over (doods)bedreigingen via WhatsApp of aan- en verkoopfraude via Marktplaats.nl.

Dat beide vormen van criminaliteit een probleem zijn wordt, onder andere, duidelijk uit de vele mediaberichten over slachtoffers van dergelijke nieuwe(re) vormen van criminaliteit. Vanuit politie en justitie is er ook speciale aandacht voor de opsporing en vervolging van cybercriminelen en binnen de politiek is dergelijke criminaliteit een belangrijk thema (zie, bijv., motie Recourt en de wetten Computercriminaliteit I/II/III).

Kennis over slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland is beschikbaar op basis van slachtofferenquêtes, zelfrapportage van daderschap, politie- en justitieregistraties en registraties van private partijen. Deze informatie wordt echter afzonderlijk en verspreid door de tijd gerapporteerd. Daarmee is de kennis fragmentarisch. Een overkoepelend beeld over wat nu bekend (en niet bekend) is over slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland ontbreekt vooralsnog. Een bundeling van kennis is zowel voor het justitiële beleid als de praktijk relevant, bijvoorbeeld voor prioritering.

In het huidige rapport wordt uiteengezet wat er bekend is over de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit binnen de Nederlandse context, vanaf 2008. Hierbij staan de volgende drie vragen centraal:

1 *Hoe is de aard van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit geconceptualiseerd?*
2 *Hoe is slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit concreet geoperationaliseerd?*
3 *Hoe groot wordt de omvang geschat van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit?*

Conceptualisatie betreft het bepalen van welke (ervaren) gedragingen onder het fenomeen cyber- en gedigitaliseerde criminaliteit vallen, waarbij operationalisatie de wijze waarop het concept concreet wordt gemeten betreft. Slachtoffer- en daderschap hebben in dit onderzoek betrekking op natuurlijke personen; criminaliteit tussen bedrijven/overheden vallen buiten de reikwijdte van het onderzoek. Bij slachtofferschap gaat het over ervaren slachtofferschap van individuen, en meldingen en aangiften daarvan bij de politie. Bij daderschap gaat het om geregistreerde verdachten en (strafrechtelijke) daders evenals daders die zelf aangeven delicten te hebben gepleegd in enquêteonderzoek en registraties van misdrijven (d.w.z., handelingen van daders). Het gaat in dit onderzoek om Nederlandse slachtoffers of daders of, om cyber- en gedigitaliseerde criminaliteit waartegen de

Nederlandse politie actie onderneemt, maar waar het niet noodzakelijk een Nederlandse dader of slachtoffer hoeft te betreffen. De aard van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit gaat over type delict, ernst en impact. De omvang betreft meetbare aspecten van dergelijke criminaliteit, zoals percentages slachtoffers of absolute aantal daders of misdrijven.

Om dit overzicht te realiseren is een systematische literatuurstudie uitgevoerd, evenals diverse empirische studies van registratiebronnen en publieke digitale platformen (namelijk, internetfora en [sociale] media berichten). Kortom, een meerdere bronnen en meerdere methoden aanpak is gehanteerd.

Slachtofferschap

Slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland wordt voornamelijk in kaart gebracht via slachtofferenquêtes en meldingen en aangiften bij de politie. De omvang van slachtofferschap verschilt sterk per type delict, bron en populatie waarop de bron betrekking heeft.

8-15% van Nederlanders slachtoffer cyber- of gedigitaliseerde criminaliteit, trends door de tijd heen verschillen per bron—relatief stabiel of dalend

Diverse bronnen bieden zicht op slachtofferschap door de tijd heen onder de totale Nederlandse bevolking van 15 jaar en ouder. In de periode 2012-2017 laat de CBS Veiligheidsmonitor een lichte daling zien in het percentage Nederlanders dat aangeeft slachtoffer te zijn geworden van cyber- en/of gedigitaliseerde criminaliteit van ruim 12% tot 11%, waarna dit percentage weer stijgt tot bijna 13% in 2019. Op basis van het LISS-panel lijkt de omvang van slachtofferschap te zijn gedaald van ruim 15% in 2010 naar bijna 10% in 2018. Dat deze twee bronnen een andere ontwikkeling laten zien kan komen door verschillen in methode en bevraging. Zo is de CBS Veiligheidsmonitor een landelijke monitor die voor iedere meting een nieuwe steekproef uit de totale bevolking trekt en daarmee op landelijk niveau ontwikkelingen weergeeft. In het LISS-panel wordt een vaste groep personen gevolgd door de tijd heen (met aanvulling wanneer respondenten uitvallen), waardoor de nadruk meer ligt op ontwikkelingen op individueel niveau. Ook worden in beide bronnen niet dezelfde delicten bevraagd. Zo wordt slachtofferschap van computervirus—hetgeen een sterker dalende trend laat zien dan andere vormen van slachtofferschap—alleen in het LISS-panel bevraagd.

Bij politie bekend slachtofferschap van cyber- en gedigitaliseerde criminaliteit klein deel van alle criminaliteit, maar in absolute aantallen niet verwaarloosbaar

Slechts een klein deel van het slachtofferschap van cyber- en gedigitaliseerde criminaliteit is bekend bij de politie, aangezien 7-8% van Nederlandse slachtoffers aangifte doet bij de politie (de aangiftebereid voor traditionele criminaliteit is over het algemeen hoger). Een textmining analyse van teksten van politieregistraties (onder meer meldingen en aangiften) laat zien dat in 2016 van de ruim 3,9 miljoen registraties ongeveer 4.000-25.000 registraties cybercriminaliteit betreffen en 132.000-293.000 registraties gedigitaliseerde criminaliteit. Dergelijke registraties betreffen weliswaar een minderheid van alle registraties bij de politie, maar zijn in absolute aantallen niet verwaarloosbaar.

Malware maakt naar schatting meeste slachtoffers

De schattingen van Nederlandse slachtoffers van cyber- en gedigitaliseerde criminaliteit varieert naar type delict en bron waaruit de gegevens komen. Computervirussen (malware) maken relatief veel slachtoffers. Het percentage slachtoffers wordt geschat tussen bijna 2% (LISS-panel) en 62% (Eurobarometer) op basis van slachtofferenquêtes. Verklaring voor de grote variatie kan hem zitten in de vraagstelling of er werkelijk schade is opgelopen door malware, wat mogelijk tot een (veel) hogere prevalentie leidt. Het percentage Nederlanders dat rapporteert slachtoffer te zijn geweest van hacken ligt naar schatting tussen de 1-16% en het percentage slachtoffers van online fraude wordt geschat tussen 0-16%, afhankelijk van het type fraude en bron. De schattingen van slachtofferschap van online bedreiging en verwante delicten (zoals cyberpesten en ongewenste verspreiding van seksueel beeldmateriaal) liggen tussen de 0-9%. Binnen politieregistraties uit 2016 komen daarentegen registraties van online bedreiging als meest voorkomende naar voren, terwijl de delicten hacken, ransomware en DDoS-aanvallen beduidend minder voorkomen. Ook wordt er vaker aangifte gedaan door slachtoffers van online fraude (12-22% van de slachtoffers) dan van hacken (2-3% van de slachtoffers).

Online bedreigingen lokaal bestuur weinig zichtbaar op social media

Ook is verkennend onderzoek gedaan naar online bedreigingen van individuen in lokaal bestuur. Met de komst van onlinekanalen zoals Facebook en Twitter is de drempel om bedreigingen te uiten, waaronder die aan politici, verlaagd. In Nederland blijkt dat een steeds groter aandeel van burgemeesters te maken heeft met bedreigingen, agressie en geweld, maar dat er weinig bekend is over online bedreigingen aan deze gezagsdragers. Uit verkennend onderzoek naar bedreigingen richting burgemeesters die via Twitter zijn gedaan en uit traditionele media analyse blijkt dat er vooral drie contexten zijn waaruit deze bedreigingen gedaan worden: georganiseerde criminaliteit en motorbendes, burgers die ontevreden zijn over genomen beslissingen en enkele individuele burgers met andere overwegingen. Echter, op basis van verkennend onderzoek kunnen (vooralsnog) geen uitspraken gedaan worden over de omvang van het fenomeen en de representativiteit van de resultaten.

Daderschap

Daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland wordt voornamelijk in kaart gebracht via justitiële registraties en enquêtes. De omvang van daderschap verschilt per type delict en bron.

Beperkt inzicht daderschap cybercriminaliteit en nauwelijks inzicht daderschap gedigitaliseerde criminaliteit in registratiebronnen politie en justitie

Er is maar een beperkt aantal bronnen dat inzicht geeft in de aard en omvang van Nederlands daderschap van cyber- en gedigitaliseerde criminaliteit. Vaak gaat het om schattingen van aantallen daders, strafzaken, geregistreerde delicten of opsporingsonderzoeken. Deze verschillende teleenheden maakt vergelijken van schattingen van daderschap van cyber- en gedigitaliseerde criminaliteit lastig. De beschikbare informatie is beperkt tot enkele typen delicten. Politie- en justitieregistraties zijn voornamelijk beperkt tot daders van computervredebreuk (d.w.z., hacken). Over daders van gedigitaliseerde criminaliteit is op basis van deze bronnen

weinig te zeggen, omdat deze vooral als traditioneel delict geregistreerd worden (zo is er alleen de categorie bedreiging waar zowel offline als online varianten gerekend worden).

Omvang bij justitie bekende daders cybercriminaliteit beperkt in absolute aantallen, wel stijgende trend door de tijd

Als we afgaan op politie- en justitiebronnen is het aantal daders in Nederland van cybercriminaliteit beperkt. In absolute aantallen neemt het aantal verdachten, daders of strafzaken met gedigitaliseerde criminaliteit door de tijd heen af, terwijl deze bij cybercriminaliteit lijkt toe te nemen (hoewel beperkt in absolute aantallen). Volgens politieregistraties zijn er ruim 70 verdachten cybercriminaliteit in 2008, terwijl dit er in 2019 bijna 430 zijn. Verder neemt in de (langere) periode van 2008-2018 het aantal strafzaken dat bij het OM binnenstroomt betreffende cybercriminaliteit toe en betreffende gedigitaliseerde criminaliteit af (respectievelijk van bijna 90 naar ruim 280 en van ruim 540 naar ruim 360). Ook het aantal door de rechter in eerste aanleg afgedane strafzaken voor cyberdelicten neemt toe en voor gedigitaliseerde criminaliteit af (respectievelijk van bijna 20 naar ruim 70 en van bijna 370 naar ruim 170). Deze aantallen betreffen minder dan 1% van het jaarlijkse totale aantal verdachten en strafzaken.

Delicten in strafzaken cyber- en gedigitaliseerde criminaliteit lijken door de jaren heen ernstiger te worden

De strafrechtelijke indicatoren die wijzen op de ernst van een delict in strafzaken suggereren bij cyber- en gedigitaliseerde criminaliteit een toenemende ernst. Dit blijkt uit een hogere strafdreiging en zwaardere straffen voor dit type zaken door de jaren heen. Zo wordt, bijvoorbeeld, in de periode 2008-2014 tot ongeveer 30% van de strafzaken met cybercriminaliteit afgedaan met een onvoorwaardelijke vrijheidsstraf, terwijl in de periode 2015-2018 dit 34-47% van de strafzaken betreft. Voor gedigitaliseerde criminaliteit ligt dit percentage op 47% in 2008 en stijgt door de jaren heen naar 83% in 2018.

Gat tussen aantal jongeren dat zegt dader te zijn van cyber- of gedigitaliseerde criminaliteit en aantal geregistreerde verdachten of strafrechtelijk daders

Zelfrapportage van daderschap van cyber- of gedigitaliseerde criminaliteit is alleen bekend voor jongeren. Het percentage jongeren van 10 tot en met 22 jaar dat een cyberdelict rapporteert is 7-22% in 2015, schattingen voor gedigitaliseerde delicten liggen tussen 4-13%. Er zit een groot gat tussen zelfgerapporteerd daderschap en aantallen verdachten of strafrechtelijk daders.

Hacken meest gerapporteerde cybercrime onder jongeren

Van de Nederlandse jongeren zegt ongeveer 1% weleens een virus te hebben verstuurd, tussen 0-2% een DDoS-aanval te hebben gepleegd en 1-18% weleens te hebben gehacked (dan wel met of zonder het manipuleren van gegevens na binnendringen). Wat betreft gedigitaliseerde criminaliteit rapport 0-8% van de jongeren weleens iemand online bedreigd te hebben (of een aanverwant delict te hebben gepleegd), en 0-10% van jongeren zegt een vorm van online aan- of verkoopfraude te hebben gepleegd.

Cybercrime-as-a-service lijkt toe te nemen

Tot slot zijn ontwikkeling van cybercrime-as-a-service (CAAS) op onlinemarkten onderzocht. Op onlinemarkten bieden criminelen ook diensten en goederen aan ten behoeve van het plegen van cybercriminaliteit. Zo zijn er diensten waar je DDoS-aanvallen kan kopen en zijn er diensten die ransomware voor je installeren op andermans computer. Door advertenties van dergelijke diensten op online-markten via geautomatiseerde methoden te observeren en coderen (d.w.z., text-mining) is het mogelijk om uitspraken te doen over ontwikkelingen in de aanbieding van CAAS. Over het algemeen lijkt er sprake te zijn van een toename in de aan-biedingen van CAAS in de periode 2011-2017, wanneer gekeken wordt naar een aantal grote markten (bijv., AlphaBay). Echter, vanwege beperkingen in de metho-diek is het moeilijk interpreteerbaar hoe groot het fenomeen nu werkelijk is.

Beantwoording onderzoeksvragen

In de volgende paragrafen wordt antwoord gegeven op de drie onderzoeksvragen.

1 *Hoe is de aard van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit geconceptualiseerd?*
2 *Hoe is slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit concreet geoperationaliseerd?*

De aard van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland is in de bestudeerde studies op twee manieren geconceptualiseerd en geoperationaliseerd. Ten eerste gaat het om korte omschrijvingen van type delicten waar men slachtoffer of dader van is, zoals in items van enquêtes. Daarnaast gaat het om afleidingen uit justitiële registratiebronnen, zoals relevante wetsartikelen of de maatschappelijke kwalificatie computervredebreuk. De prevalentie van slacht-offer- en daderschap zijn voornamelijk concreet geoperationaliseerd als percentage slachtoffers en daders binnen onderzochte populaties. Enkele andere teleenheden, zoals absolute aantallen individuen, strafzaken en delicten komen ook voor.

3 *Hoe groot wordt de omvang geschat van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit?*

Er is niet één antwoord te geven op deze vraag. Dit wordt duidelijk uit de uiteenlopende ranges en teleenheden betreffende slachtoffer- en daderschap die besproken zijn in dit rapport. Zo blijkt, bijvoorbeeld, uit zelfrapportage onder jongeren in 2015 dat respectievelijk 7-22% en 4-13% van de respondenten een cyber- of gedigitaliseerde delict heeft gepleegd in het voorafgaande jaar, terwijl het aantal verdachten in dat jaar tussen de ruim 120 en bijna 200 personen telt. Ook tussen onderzoekspopulaties, jaartallen en type delicten zijn er verschillen in de schattingen van omvang. Zo rapporteren jongeren meer slachtofferschap dan naar voren komt in de gehele populatie (van 15 jaar en ouder), neemt volgens officiële indicatoren zoals verdachten en strafzaken cybercriminaliteit toe, terwijl gedigitaliseerde criminaliteit juist afneemt, en komt slachtofferschap van malware vaker voor dan verschillende vormen van online fraude. Kortom, een fragmentatie van conceptualisatie en operationalisatie van cyber- en gedigitaliseerde criminaliteit maakt het vooralsnog niet mogelijk een eenduidig antwoord te geven op de vraag naar de omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland.

Conclusie en aanbevelingen

Het huidige rapport draagt bij aan het bundelen van beschikbare kennis over slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland. Welke lering kan getrokken worden op basis van dit rapport?

Er is (vooralsnog) geen uniformiteit in de conceptualisatie en operationalisatie van cyber- en gedigitaliseerde criminaliteit. Het is echter ook maar de vraag of uniformiteit mogelijk of wenselijk is gegeven de snelheid waarin de digitale ontwikkelingen zich voordoen. Immers, vroegtijdig vastleggen in één concept of operationalisatie kan innovatie en daarmee kennisverwerving belemmeren.

Het is wel duidelijk dat cyber- en gedigitaliseerde criminaliteit in Nederland een maatschappelijk probleem is. Er zijn immers ieder jaar veel Nederlanders slachtoffer hiervan. Het beeld dat dit totale fenomeen alleen maar groter zou zijn geworden door de tijd heen blijkt echter niet uit de beschikbare cijfers, aangezien slachtofferschap een lichte daling of stabiele trend laat zien. Specifieke delicten, zoals online aan- en verkoopfraude, nemen door de tijd wel toe. Ook zijn er steeds meer cybercriminelen in beeld bij justitie.

Verder doen cyber- en gedigitaliseerde criminaliteit als maatschappelijke problemen niet veel onder voor traditionele criminaliteit. Hoewel slachtofferschap van traditionele criminaliteit wel meer voorkomt, is het ook een afnemend fenomeen, terwijl de prevalentie van slachtofferschap cyber- en gedigitaliseerde criminaliteit mogelijk aan het stabiliseren is.

Uit dit rapport komen twee beleidsaanbevelingen naar voren. Ten eerste, investeer in verbetering en doorontwikkeling van instrumentaria om slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit te registeren en te meten. Hierbij moet niet alleen gedacht worden aan hoe te meten, maar ook wat te meten. Voor de aanpak van cyber- en gedigitaliseerde criminaliteit is het belangrijk om op de hoogte te zijn van nieuwe criminaliteit. Om in te kunnen spelen op deze ontwikkelingen is het aan te raden om aansluiting te zoeken bij organisaties en experts die (vroegtijdig) zicht hebben op nieuw opkomende criminaliteit. Daar moet wel bij gezegd worden dat er niet een te smalle focus moet zijn op alleen maar actuele criminaliteit die mogelijk maar kort relevant zal blijven. Binnen registratiesystemen hoeft de focus niet alleen te liggen op het meer gedetailleerd registreren naar verschillende vormen van cyber- en gedigitaliseerde criminaliteit, omdat dit de toch al zware registratiedruk alleen maar vergroot. Een wel te behalen winst zit hem hier in het verrijken van al bestaande gegevens, bijvoorbeeld, door het gebruik van text-mining of andere innovatieve technieken. Binnen het justitiële domein is immers al veel tekstuele data met detailinformatie beschikbaar.

Ten tweede, blijf investeren in expertise over cyber- en gedigitaliseerde criminaliteit in de justitiële keten. Uit dit rapport wordt duidelijk dat volgens niet-officiële bronnen er veel meer slachtoffers en daders van cyber- en gedigitaliseerde criminaliteit zijn, dan dat politie, OM en ZM-statistieken suggereren. Deels komt dit door zaken waarop beleid en praktijk geen of moeilijk invloed hebben, zoals aangiftebereidheid. Deels kan het ook komen door zaken waarop beleid en praktijk wel grip kunnen hebben, zoals expertise bij politie, OM en ZM. Beperkte expertise kan ervoor zorgen dat aangiftes van burgers niet adequaat in behandeling worden genomen, waardoor deze niet verder de keten ingaan of niet herkenbaar als cyber- en gedigitaliseerde criminaliteit de keten ingaan. Ook kan beperkte expertise ertoe leiden dat cyber-

en gedigitaliseerde criminaliteit niet goed op ernst wordt ingeschat en kan het de opsporing en vervolging van daders belemmeren. Verwacht mag worden dat investeren in expertise bij politie en justitie op dit terrein eraan kan bijdragen dat het fenomeen van cyber- en gedigitaliseerde criminaliteit adequaat kan worden opgepakt.