Cahier 2020-15

Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland

M.G.C.J. Beerthuizen
T. Sipma
A.M. van der Laan

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Inhoud

Samenvatting — 5

1 Inleiding — 12
1.1 Cyber- en gedigitaliseerde criminaliteit — 12
1.2 Doelstelling — 14
1.3 Meerdere bronnen aanpak — 14
1.4 Leeswijzer — 16

2 Slachtofferschap van cyber- en gedigitaliseerde criminaliteit — 17
2.1 Inleiding — 18
2.2 Cyber- en gedigitaliseerde criminaliteit in het algemeen — 19
2.2.1 Slachtofferschap onder de hele populatie — 19
2.2.2 Aangifte en meldingen in slachtofferenquêtes — 22
2.2.3 Aangifte en meldingen in politieregistraties — 22
2.2.4 Slachtofferschap onder jongeren — 23
2.3 Hacken — 24
2.3.1 Slachtofferschap van hacken onder de hele populatie — 24
2.3.2 Aangifte en meldingen van hacken in politieregistraties — 24
2.3.3 Slachtofferschap van hacken onder jongeren — 26
2.4 DDoS-aanvallen — 26
2.4.1 Aantal gemelde DDoS-aanvallen — 26
2.4.2 Aangifte en meldingen van DDoS-aanvallen in politieregistraties — 26
2.4.3 Toegang tot onlinediensten — 28
2.5 Malware — 28
2.5.1 Slachtofferschap van malware onder de hele populatie — 28
2.5.2 Malware aanvallen en geïnfecteerde computers — 28
2.5.3 Aangifte en meldingen van malware in politieregistraties — 29
2.5.4 Slachtofferschap van malware onder jongeren — 29
2.6 Online bedreiging, cyberpesten en verspreiding seksueel beeldmateriaal — 31
2.6.1 Slachtofferschap van online bedreiging en cyberpesten onder de hele populatie — 31
2.6.2 Aangifte en meldingen van online bedreiging in politieregistraties — 34
2.6.3 Slachtofferschap van online bedreiging en cyberpesten onder jongeren — 34
2.7 Online fraude — 34
2.7.1 Identiteitsfraude — 35
2.7.2 Phishing en pharming — 37
2.7.3 Bank- en creditcardfraude — 37
2.7.4 Aan- en verkoopfraude — 37
2.7.5 Overige vormen van online fraude — 38
2.7.6 Aangifte van online fraude — 38
2.8 Discussie — 43

3 Online bedreigingen in het lokaal bestuur — 46
3.1 Introductie — 47
3.2 Methode — 48
3.2.1 Media-analyse — 48
3.2.2 Sociale media-analyse — 49
3.3 Resultaten — 50

3.3.1 Resultaten media-analyse — 50
3.3.2 Resultaten sociale media-analyse — 52
3.4 Conclusie — 57

4 Daderschap van cyber- en gedigitaliseerde criminaliteit — 59
4.1 Inleiding — 60
4.2 Cyber- en gedigitaliseerde criminaliteit in het algemeen — 60
4.2.1 Politieregistraties: opsporingsonderzoeken en misdrijven — 60
4.2.2 Verdachtenregistraties (OM en politie) — 61
4.2.3 Instroom van strafzaken bij het OM en ZM (RAC-min) — 63
4.2.4 Cyber- en gedigitaliseerde criminaliteit onder jongeren — 64
4.3 Hacken — 66
4.3.1 Politieregistraties: verdachten van hacken — 66
4.3.2 Hacken onder jongeren — 66
4.4 DDoS-aanvallen — 66
4.4.1 DDoS-aanvallen in officiële registraties — 68
4.4.2 DDoS-aanvallen onder jongeren — 68
4.5 Malware — 68
4.5.1 Gedetecteerde malware aanvallen — 68
4.5.2 Malware in officiële registraties — 70
4.5.3 Malware onder jongeren — 71
4.6 Online bedreiging, cyberpesten en verspreiding seksueel beeldmateriaal — 71
4.6.1 Politieregistraties — 71
4.6.2 Online bedreiging en cyberpesten onder jongeren — 71
4.7 Online fraude — 73
4.7.1 Online fraude in officiële registraties — 73
4.7.2 Online fraude onder jongeren — 73
4.8 Discussie — 75

5 Aanbieders en afnemers van cybercrime-as-a-service — 78
5.1 Introductie — 78
5.2 Methode — 79
5.3 Resultaten — 80
5.4 Discussie — 83

6 Conclusie en discussie — 84
6.1 Beantwoording onderzoeksvragen — 84
6.2 Discussie methoden 89
6.3 Afsluiting — 90

Summary — 92

Literatuur — 97

Bijlagen
1 Samenstelling begeleidingscommissie — 103
2 Methoden — 104
3 Online bedreigingen in het lokaal bestuur — 113

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.

1 Inleiding

Auteurs: *Marinus Beerthuizen, Take Sipma en André van der Laan*

Door een sterk toenemende digitalisering van de Nederlandse samenleving (zie, bijv., CBS, 2019a) is een steeds groter aandeel van het leven zich op internet gaan afspelen. Via social media houdt men contact met kennissen en vrienden en via nieuwssites en –apps blijft men op de hoogte van de nieuwste weetjes. Niet alleen in het privéleven is deze digitalisering merkbaar, maar ook contact met bedrijven en overheden is tegenwoordig in eerste instantie vaak digitaal. Kortom, mogelijkheden om met iedereen online in contact te staan zijn alleen maar gegroeid. Meer recentelijk zorgen landelijke maatregelen tegen de verspreiding van COVID-19 dat dergelijke mogelijkheden ook een verplichting kunnen zijn (zoals telewerken). Door deze groei in digitaal verkeer is ook de blootstelling aan cyber- en gedigitaliseerde criminaliteit toegenomen. Dit is onder andere merkbaar in nieuwsberichten over dergelijke criminaliteit (bijv., NOS, 2019), ook specifiek in verband met COVID-19 (bijv., Volkskrant, 2020) en dat de geschatte directe en indirecte kosten van cyber- en gedigitaliseerde criminaliteit groot zijn (bijv., Anderson et al., 2013; 2019). Ofwel, de kans om slachtoffer te worden van cyber- en gedigitaliseerde criminaliteit lijkt nog nooit zo groot te zijn geweest als nu, evenals voor daders de hoeveelheid aan mogelijkheden om via internet misdrijven te plegen.

In het huidige rapport[1] bekijken wij voor de Nederlandse context twee kanten van dergelijke criminaliteit—slachtofferschap en daderschap. Naast slachtoffers en daders als individuen, wordt ook aandacht besteed aan andere aspecten van slachtoffer- en daderschap, zoals gepleegde misdrijven, strafzaken en justitiële registraties. Er wordt getracht een breed overzicht te geven van slachtoffer- en daderschap door gebruik te maken van een meerdere bronnen benadering.

In dit hoofdstuk worden eerst de fenomenen cyber- en gedigitaliseerde criminaliteit uiteengezet. Vervolgens wordt de behoefte aan dit onderzoek besproken, waarna de doelstelling en de aanpak van het huidige onderzoek aan bod komen. Dit hoofdstuk sluit af met een leeswijzer.

1.1 Cyber- en gedigitaliseerde criminaliteit

Hoewel de term cybercriminaliteit vaak wordt gebruikt voor alle criminaliteit waar moderne technologie een belangrijke rol bij speelt, kan men ook nog onderscheid maken naar gedigitaliseerde criminaliteit.

Cybercriminaliteit betreft delicten waarbij informatie- en communicatietechnologie (ICT) het middel en doel is. Hierbij kan gedacht worden aan onrechtmatig toegang verkrijgen tot computers, e-mailaccounts en online bankierplatformen (d.w.z., hacken). Een ander voorbeeld is het via clandestiene software vergrendelen van

1 Het huidige rapport wijkt af van een eerder WODC-rapport waarin aandacht besteed is aan de aard en omvang van cyber- en gedigitaliseerde criminaliteit in Nederland (Smit et al., 2018a, 2018b). Ten eerste, dit rapport richt zich exclusief op cyber- en gedigitaliseerde criminaliteit, waar Smit et al. ook offline criminaliteit belichten. Daarnaast richt dit rapport zich op hetgeen wat we wel weten, waar Smit et al. zich primair richten op methoden die toegepast kunnen worden om inzichten te verkrijgen in zaken die niet bekend zijn.

computers om vervolgens voor ontgrendeling 'losgeld' te eisen (d.w.z., ransomware). Andere termen voor deze criminaliteit zijn cybercrime of computercriminaliteit in enge zin of (de internationale term) cyber-dependent crime.

Gedigitaliseerde criminaliteit betreft traditionele delicten waarbij ICT als middel wordt ingezet, maar niet het doel is. Het bedreigen van personen via e-mail, WhatsApp-berichten of social media en het oplichten van aan- en verkopers op Marktplaats.nl zijn voorbeelden van gedigitaliseerde criminaliteit. Waar daders eerder face-to-face of telefonisch contact moesten zoeken met hun slachtoffers, kan dat nu (potentieel anoniemer) via internet. Andere gangbare termen zijn cybercrime of computercriminaliteit in brede zin of (de internationale term) cyber-enabled crime.

Beide vormen van criminaliteit zijn binnen de Nederlandse samenleving een maatschappelijk probleem. Zo geeft bijna één op de twaalf Nederlanders aan slachtoffer te zijn geweest van cyber- en/of gedigitaliseerde criminaliteit (CBS, 2019b). Daarnaast groeit het aantal aangiftes cybercrime volgens politiestatistieken (Politie, 2020). Ook zegt drie op de tien Nederlandse jongeren enige vorm van cyber- of gedigitaliseerde delinquentie te hebben gepleegd in de 12 maanden vooraf aan enquêtering, wat de prevalentie van zelfgerapporteerde offline delinquentie evenaart (Van der Laan & Goudriaan, 2016). Verder is er in de media regelmatig berichtgeving over slachtoffer- en daderschap van cybercrime (zie bijvoorbeeld NU.nl, 2020). Er is dan ook vanuit de politiek veel aandacht voor het aanpakken, voorkomen en terugdringen van cybercriminaliteit (en gedigitaliseerde criminaliteit; zie o.a. motie Recourt, *Kamerstukken II* 2016, 34 550 VI, nr. 87 en wetten computercriminaliteit I/II/III). Om cyber- en gedigitaliseerde criminaliteit succesvol aan te pakken is kennis over de aard en omvang van slachtoffer- en daderschap noodzakelijk.

De aard van slachtoffer- en daderschap betreft een kwalitatief aspect van cyber- en gedigitaliseerde criminaliteit, waaronder bijvoorbeeld type delict valt, evenals ernst van de ervaren of uitgevoerde handeling. De omvang van slachtoffer- en daderschap betreft een kwantitatief aspect, waaronder aantallen of percentages slachtoffers en daders vallen, evenals registratieaspecten van dergelijke criminaliteit, zoals geregistreerde misdrijven of strafzaken. Kort gezegd, aard gaat om wat er gebeurt, waarbij de omvang gaat om hoe vaak dit gebeurd. Een combinatie van de aard en omvang indiceert de maatschappelijke ernst van slachtoffer- en daderschap. Het huidige rapport wil op maatschappelijk niveau inzicht geven in slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit, waardoor binnen dit rapport de aard zich beperkt tot die van kwantificeerbaar slachtoffer- en daderschap.

Een overkoepelend beeld van de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit is er (vooralsnog) niet. Dit komt mede doordat bronnen, publicaties en onderzoeken die cyber- en gedigitaliseerde criminaliteit betreffen, op tenminste enige wijze beperkt zijn in wat zij over aard en omvang (kunnen) vertellen. Het recente onderzoek van het CBS (2019b) heeft, bijvoorbeeld, alleen betrekking op de prevalentie van slachtoffers, maar geeft geen inzichten in daderschap of 'slachtofferloze' criminaliteit. Daarnaast geven vervolgings- en veroordelingsgegevens van het Openbaar Ministerie en de rechtelijke macht alleen inzichten in de aantallen strafrechtelijk vervolgde daders. Hier komen daders van dergelijke criminaliteit die buiten het zicht van justitie blijven niet in terug. Kortom, wanneer men zich beperkt tot één of een beperkt aantal

bronnen, kan er geen breed inzicht verkregen worden in de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit. Zonder dit beeld kan bovendien ook geen vergelijking gemaakt worden met traditionele criminaliteit, wat ook weer verdere inzichten zou verschaffen.

1.2 Doelstelling

Een bundeling en uiteenzetting van bronnen betreffende slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit zou kunnen voorzien in nieuwe inzichten, maar is vooralsnog niet gebeurd binnen de Nederlandse context. Het huidige rapport probeert hierin te voorzien. De centrale onderzoeksvraag die beantwoord wordt is dan ook: *wat is er bekend over de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland?*

Door deze vraag te beantwoorden wordt niet alleen duidelijk wat er wel bekend is over cyber- en gedigitaliseerde criminaliteit, maar ook wat er (nog) niet bekend is. Voor welke vormen van cyber- en gedigitaliseerde criminaliteit zijn nog geen cijfers over slachtoffer- en/of daderschap bekend? Over welke jaartallen weten we eigenlijk niks? Dergelijke informatie is relevant voor beleid, praktijk en wetenschappers. Zo kan deze informatie gebruikt worden voor prioritering binnen beleid en praktijk en richting geven aan wetenschappers over op welke gebieden nog kenniswinst te behalen valt.

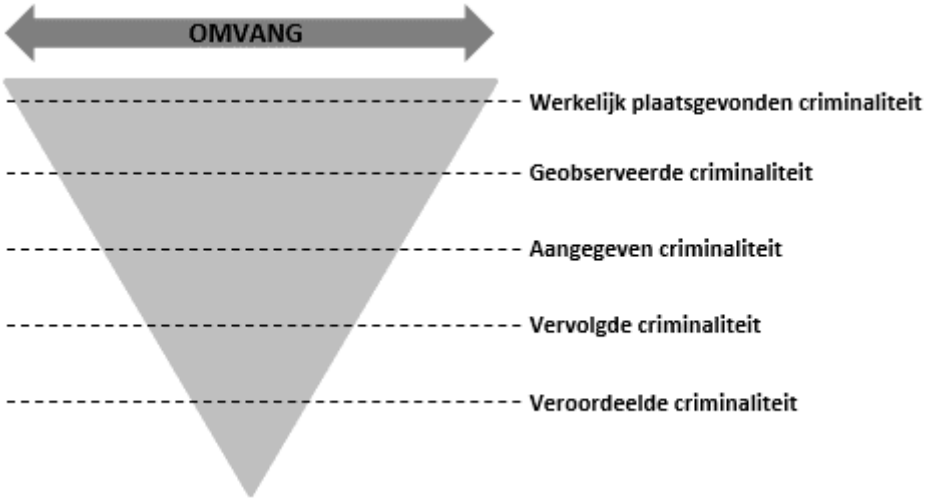
1.3 Meerdere bronnen aanpak

Om antwoord te kunnen geven op de vraagstelling maken we in dit onderzoek gebruik van een meerdere bronnen aanpak. Daarbij gebruiken we zowel literatuur als empirische bronnen, waarbij de initiële focus ligt op individuele slachtoffers en daders (of verdachten). Ook wordt aandacht besteedt aan andere zaken, zoals misdrijven en strafzaken. Daarnaast ligt de focus op de Nederlandse context in plaats van een internationale context. Ook wordt er gekeken naar bronnen over slachtoffers en daders met een niet-Nederlandse of onbekende locatie, wanneer de Nederlandse rechtshandhaving zich desondanks bemoeit met deze personen (bijv., via het verstoren of platleggen van onlinemarkten). Criminaliteit tussen bedrijven onderling en tussen overheden onderling wordt buiten beschouwing gelaten, omdat we ons willen beperken tot criminaliteit en niet (bedrijfs)spionage en cyberwarfare willen meenemen. Het individueel slachtoffer- en daderschap is bij dergelijke vormen van gedrag vaak moeilijk(er) te kwantificeren. Echter, cyber- en gedigitaliseerde criminaliteit tegen bedrijven en overheden uitgevoerd door individuele burgers (zover bekend) wordt wel relevant gevonden.

De meerdere bronnen aanpak betreft ook meerdere methoden. Zo wordt voor de zoektocht naar recente literatuur gebruikgemaakt van een systematische literatuurstudie, aangevuld met snowball-sampling. Daarnaast zijn empirische gegevens verzameld uit traditionelere bronnen van justitie en is gebruikgemaakt van zelfrapportages onder Nederlandse jongeren. Ook is gekeken naar meer actuele methoden, zoals automatische zoekopdrachten op social media naar bedreigingen van burgemeesters en webscraping van onlinemarkten waar cybercrime-as-a-service wordt aangeboden. Voor een overzicht van de in dit rapport gehanteerde methoden, zie bijlage 2 en de specifieke methoden secties van hoofdstuk 3 en 5.

We richten het onderzoek op de periode vanaf 2008. Voor publicaties geldt het jaar van publicatie en voor databronnen geldt het relevante indexjaar van die bron (bijv., voor justitiële veroordelingsgegevens gaat het vaak om het jaar waarin de strafzaak is afgedaan). Een publicatie of bron kan meer dan één tijdspunt belichten —dergelijke publicaties en bronnen zijn waardevol, omdat zij een ontwikkeling door de tijd heen kunnen weergeven. De diverse bronnen die gebruikt zijn voor het beantwoorden van de brede onderzoeksvraag geven informatie over cyber- en gedigitaliseerde criminaliteit op verschillende plekken in een trechtermodel van criminaliteit, welke is weergegeven in figuur 1.

Figuur 1 Trechtermodel van criminaliteit



De trechter loopt van breed naar smal. Bovenaan staat de werkelijk plaatsgevonden criminaliteit, wat de breedste omvang heeft van alle niveaus van criminaliteit. De omvang van dit niveau is wellicht nooit te bepalen. Geobserveerde criminaliteit betreft gedragingen die door anderen geobserveerd of gemeten wordt, maar welke niet noodzakelijk de justitiële keten in gaat. Dergelijke criminaliteit kan geobserveerd worden door politieagenten op straat of op internetfora, kan door slachtoffers en daders gemeld worden aan onderzoekers die een enquête houden, of wordt gemeld bij private organisaties (bijv., bij banken in het geval van fraude bij internetbankieren). Bij de volgende laag begint de justitiële keten, van aangifte naar (eventuele) vervolging naar (eventuele) veroordeling. Naast verschillende niveaus in de lengte zijn er over de breedte van de trechter verschillende meeteenheden. Zo kan bij slachtofferschap gesproken worden van absolute aantallen slachtoffers of van percentage prevalentie binnen (sub)populaties. Voor daderschap kan er naast dergelijke statistieken ook gesproken worden van aantallen gepleegde misdrijven of voorgekomen strafzaken. In het huidige rapport worden in principe alle lagen van de trechter in overweging genomen, evenals meerdere teleenheden.

Deze overwegingen leiden ertoe dat voor slachtoffer- en daderschap drie specifieke onderzoeksvragen worden gesteld:

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?*

1.4 Leeswijzer

Met het huidig rapport bieden we inzicht in de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland. In hoofdstuk 2 komt slachtofferschap van cyber- en gedigitaliseerde criminaliteit aan bod. Naast een algemene benadering van dergelijke criminaliteit, wordt ook naar specifieke delicten gekeken, zoals malware en online fraude. Hierna wordt in hoofdstuk 3 een uitstap gemaakt naar een specifieke populatie slachtoffers van online bedreiging, namelijk burgemeesters van Nederlandse gemeenten. In hoofdstuk 4 komt daderschap aan bod, grotendeels op dezelfde wijze als slachtofferschap eerder is behandeld. In hoofdstuk 5 wordt een uitstap gemaakt naar cybercrime-as-a-service op onlinemarkten, waar daders van cybercriminaliteit hun diensten en goederen aanbieden aan medecriminelen. In het slothoofdstuk worden de onderzoeksvragen beantwoord en vindt een discussie plaats over diverse onderwerpen en resultaten.

2 Slachtofferschap van cyber- en gedigitaliseerde criminaliteit

Auteurs: *Take Sipma, Marinus Beerthuizen, Esther Meijer-van Leijsen en André van der Laan*

Belangrijkste bevindingen

De omvang van Nederlands slachtofferschap van cyber- en gedigitaliseerde criminaliteit is aan de hand van verschillende slachtofferenquêtes en politieregsitraties in kaart gebracht. De meest bevraagde vorm cybercriminaliteit betreft hacken en voor gedigitaliseerde criminaliteit is dit (verschillende vormen van) online fraude en bedreiging. De omvang van slachtofferschap verschilt sterk per type delict.

Algemeen

Gegevens van de CBS Veiligheidsmonitor laten tussen 2008 en 2017 een lichte daling zien in de omvang van slachtofferschap van cyber- en gedigitaliseerde criminaliteit in het algemeen: van ongeveer 12% tot 11%. In 2019 is dat percentage echter weer gestegen tot bijna 13%. Op basis van het LISS-panel lijkt de omvang te dalen van ruim 15% in 2010 tot bijna 10% in 2018. Deze sterkere daling is waarschijnlijk te wijten aan de daling in het aantal mensen dat slachtoffer zegt te zijn is geworden van een computervirus (van bijna 9% tot bijna 2%). In de CBS Veiligheidsmonitor is slachtofferschap van digitale virussen niet gemeten. Uit textmining in het basissysteem van de politie, BVH, blijkt dat in 2016 van de ruim 3,9 miljoen registraties—waaronder meldingen door slachtoffers—ongeveer 4.000-25.000 registraties cyber-criminaliteit betreffen en tussen ongeveer 132.000-293.000 registraties betrekking hebben op gedigitaliseerde criminaliteit.

Hacken

De omvang van zelfgerapporteerd slachtofferschap van hacken ligt tussen de 1% en 16% en lijkt de afgelopen jaren ook te zijn afgenomen. Volgens textmining onderzoek zijn er 3.710 registraties van hacken bij de politie terug te vinden in 2016. Dit is 0,1% van het totale aantal registraties.

DDoS-aanvallen

Het aantal registraties van DDoS-aanvallen op basis van textmining van politieregistraties betreft 2.210, wat bijna 0,1% is van het totale aantal registraties in 2016. Op basis van meldingen gedaan bij de Nationale Beheersorganisatie Internet Providers (NBIP) lijkt de omvang van DDoS-aanvallen toegenomen.

Malware

Malware, waaronder computervirussen, maakt relatief veel slachtoffers. De omvang verschilt echter sterk per bron, aangezien zelfgerapporteerd slachtofferschap varieert van 2-62%. Het aantal politieregistraties van ransomware telt in 2016 ruim 1.930, wat neerkomt op bijna 0,1% van het totale aantal registraties.

Online bedreiging

Omvangcijfers van zelfgerapporteerd slachtofferschap van online bedreiging en cyberpesten onder de algehele populatie liggen tussen bijna 1% en ruim 3%. Slachtofferschap van deze delicten ligt onder jongeren hoger met 2-9%. Online bedreiging met een seksueel component is onder zowel volwassen (bijna 1%) als onder jongeren (0-1%) lager. Het aantal registraties van online bedreiging bij de

politie is aan de hand van textmining van politieregistraties geschat op bijna 117.000 in 2016. Dit is 3% van het totale aantal registraties. De omvang van online smaad is geschat op ruim 103.000 registraties (bijna 3%) en van online stalking op bijna 66.000 registraties (bijna 2%).

Online fraude
De omvang van zelfgerapporteerd slachtofferschap van verschillende soorten online fraude is onder de algehele populatie geschat op 0-16% en onder jongeren op 5-15%. Slachtofferschap van identiteitsfraude komt relatief gezien het minst voor van alle type online fraude (0-1%). Slachtofferschap van aankoopfraude is de afgelopen jaren toegenomen volgens zowel de CBS Veiligheidsmonitor (van 3% in 2012 tot bijna 5% in 2019) en het LISS-panel (ruim 2% in 2008 en ruim 4% in 2018). In 2016 is het aantal geschatte registraties bij de politie van online aan- en verkoopfraude en identiteitsfraude ongeveer 34.000 afzonderlijk voor beide delicten. In beide gevallen is dit 0,9% van het totale aantal registraties.

Aangifte
Aangifte wordt vaker gerapporteerd door slachtoffers van online fraude (12-22% van de slachtoffers) dan slachtoffers van hacken (2-3%) of online bedreiging en cyberpesten (5-6%).

2.1 Inleiding

Slachtoffers zijn, binnen de context van dit onderzoek, personen die het doelwit waren van cyber- of gedigitaliseerde criminaliteit. Het gaat om personen van wie de bankrekening is leeggehaald na een hack, personen wiens computer vergrendeld is door ransomware, of personen die bedreigd zijn via de e-mail of WhatsApp. Het gaat hier niet om slachtoffers in de statelijke of organisatorische sfeer. Hoewel niet noodzakelijk, is het aannemelijk dat slachtoffers enige vorm van schade ondervinden, zoals financiële of psychologische schade (bijv., gevoelens van onveiligheid). Bij sommige cyber- en gedigitaliseerde delicten, zoals hacken of identiteitsfraude, bestaat de kans dat men niet op de hoogte is van zijn of haar slachtofferschap. Maar ook niet ieder slachtoffer ziet zichzelf als slachtoffer en zal hier melding van maken, zelfs als men op de hoogte is het ondervonden delict. Bijvoorbeeld, wanneer de bank iemand schadeloosstelt bij verlies van geld. Het is bovendien mogelijk dat mensen zichzelf wel als slachtoffer zien, terwijl ze dat in werkelijkheid niet zijn. Bijvoorbeeld als computerproblemen vermeend worden veroorzaakt door malware of hacken, terwijl de werkelijke oorzaak een software fout is.

Het bepalen van slachtofferschap gebeurt veelal door mensen te vragen of zij slachtoffer zijn geweest. In dit hoofdstuk is gebruikgemaakt van de volgende slachtofferenquêtes die zijn voorgelegd aan een representatieve steekproef onder de Nederlandse bevolking: CBS Veiligheidsmonitor (zie bijv. CBS, 2020a), CBS Digitale Veiligheid & Criminaliteit (CBS, 2019b), CBS ICT, Kennis & Economie (CBS, 2016), LISS-panel (zie bijv. Sipma & Van Leijsen, 2019), Slachtofferschap in een gedigitaliseerde samenleving (Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013), PwC enquêtes (PwC, 2013) en de statistieken over Nederland uit de Euro-barometer (2012, 2015). Het gaat in deze enquêtes over slachtofferschap in de twaalf maanden voorafgaand aan bevraging.

De Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ; bijv., Van der Laan & Beerthuizen, 2016), Jeugd & Cybersafety (Kerstens & Stol, 2012) en EU Kids

online (Livingstone, Haddon, Görzig,& Ólafsson, 2011) zijn slachtofferenquêtes die alleen aan jongeren zijn voorgelegd. Ook hier gaat het om slachtofferschap gedurende twaalf maanden voorafgaand aan bevraging. In het Jeugd & Cybersafety onderzoek gaat het voor cyberpesten over drie maanden voorafgaand aan bevraging. Voor overige typen cyber- en gedigitaliseerde criminaliteit is gevraagd of respondenten ooit slachtoffer zijn geworden. Naast slachtofferenquêtes, bieden onderzoeken naar politieregistraties van meldingen en aangiftes inzicht in de omvang van slachtofferschap (bijv., Tollenaar, Rokven, Macro, Beerthuizen en Van der Laan, 2019). Zie voor een uitgebreider overzicht van de methodiek die gehanteerd wordt in dit hoofdstuk bijlage 2.

2.2 Cyber- en gedigitaliseerde criminaliteit in het algemeen

In de volgende paragraaf worden resultaten besproken die betrekking hebben op algemene cyber- en gedigitaliseerde criminaliteit. Hiermee wordt bedoeld dat er uitspraken worden gedaan over een collectief van gedragingen, zonder uitsplitsingen naar specifieke vormen van cyber- of gedigitaliseerde criminaliteit (zoals DDoS-aanvallen of online bedreiging). Deze specifieke vormen worden in latere paragrafen besproken.

Afhankelijk van de bron en jaartal waarover de meting gaat varieert het percentage slachtoffers van cyber- en/of gedigitaliseerde criminaliteit in het algemeen onder de hele populatie van 8-15%. In een klein deel daarvan wordt aangifte gedaan. Onder jongeren varieert het percentage slachtoffers van cyber- en/of gedigitaliseerde criminaliteit van 16% onder 10- en 11-jarigen tot 37% onder 18- tot en met 22-jarigen.

2.2.1 Slachtofferschap onder de hele populatie

Studies met representatieve steekproeven van de Nederlandse bevolking kunnen een indicatie gegeven over de omvang van slachtofferschap van cyber- en gedigitaliseerde criminaliteit in het algemeen. Dit gebeurt door te kijken of respondenten ten minste één keer slachtoffer zijn geweest van ten minste één van de bevraagde cyber- of gedigitaliseerde delicten.

In de Veiligheidsmonitor van het CBS is tussen 2012 en 2017 aan respondenten van 15 jaar en ouder gevraagd of zij slachtoffer zijn geweest van diverse delicten: hacken, aankoop- of verkoopfraude, pesten via internet en identiteitsfraude (CBS, 2020a). Waar in 2012 12% van de respondenten aangeeft slachtoffer te zijn geweest van ten minste één delict, is dit in 2017 licht gedaald tot 11% (zie tabel 1). Dit percentage ligt hoger dan de prevalentie van bijna 9% in 2011 uit de studie van Domenie et al. (2013), welke diende als opmaat voor een landelijke monitor slachtofferschap van cyber- en gedigitaliseerde criminaliteit.

Sipma en Van Leijsen (2019) hebben een soortgelijke aanpak gehanteerd. Op basis van het LISS-panel, een panelstudie onder een representatieve steekproef van Nederlandse huishoudens met personen van 15 jaar en ouder, is het aantal slachtoffers van zeven typen online delicten onderzocht. De type delicten zijn: creditcard fraude, gehackt worden, online aankoopfraude, online bedreiging, het oplopen van een computervirus, ongeautoriseerde bankafschrijving en identiteitsfraude. Deze studie suggereert een daling in slachtofferschap van ruim 15% in 2010 tot bijna 10% in 2018 (zie tabel 1).

Tabel 1 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit: algemeen

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
CBS Veiligheidsmonitor[1]												
Zelfgerapporteerd slachtofferschap					12,1%	12,6%	11,2%	11,1%	10,7%	11,0%		12,8%
Percentage slachtoffers die aangifte hebben gedaan					7,1%	7,4%	7,3%	7,8%	7,6%	8,0%		8,2%
Aantal delicten per 100 inwoners					19,7	20,8	18,8	18,7	17,9	18,6		22,3
LISS-panel[2]												
Zelfgerapporteerd slachtofferschap			15,1%		13,2%		8,3%		9,7%		9,5%	
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap internetgebruikers				8,5%								
CBS Digitale veiligheid & criminaliteit[3]												
Zelfgerapporteerd slachtofferschap											8,5%	
y	'08	'09	'10	'11	'12	'13	'14	...	`16	...	`18	`19
Textmining politieregistraties (BVH)[4]												
Aantal registraties cyberdelicten (95% BI)								3.946-24.625				
Percentage registraties cyberdelicten van totaal (95% BI)								0,10%-0,62%				
Aantal registraties gedigitaliseerde delicten (95% BI)								131.569-292.538				
Percentage registraties gedigitaliseerde delicten van totaal (95% BI)								3,33%-7,41%				
Aantal registraties cyber- en gedigitaliseerde delicten (95% BI)								133.305-303.666				
Percentage registraties cyber- en gedigitaliseerde delicten van totaal (95% BI)								3,38%-7,70%				
y	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ)[5]												
Zelfgerapporteerd slachtofferschap cybercriminaliteit												
10- en 11-jarigen								9,4%				
12- tot en met 17-jarigen								19,1%				
18- tot en met 22-jarigen								30,4%				
Zelfgerapporteerd slachtofferschap gedigitaliseerde criminaliteit												
10- en 11-jarigen								11,1%				
12- tot en met 17-jarigen								13,6%				
18- tot en met 22-jarigen								13,0%				
Zelfgerapporteerd slachtofferschap cyber- en gedigitaliseerde criminaliteit												
10- en 11-jarigen								16,3%				
12- tot en met 17-jarigen								27,0%				
18- tot en met 22-jarigen								37,1%				

1 Hacken, cyberpesten, identiteitsfraude, online aan- en verkoopfraude;

2 Hacken, computervirus, online bedreiging identiteitsfraude, bankfraude, creditcardfraude en online aankoopfraude (omdat in 2008 niet dezelfde aantallen delicten bevraagd zijn als in 2010 en later, is over 2008 geen algemene maat berekend);

3 Hacken, interpersoonlijke delicten (seksueel en niet seksueel), identiteitsfraude, phishing, bankfraude, online aan- en verkoopfraude, nepboete/nepfactuur of nepactie, microsoftscam, wangirifraude;

4 Hacken, DDoS, ransomware, online bedreiging, online stalking, online smaad, identiteitsfraude, online aan- en verkoopfraude;

5 Hacken, computervirus, online bedreiging, online aan- en verkoopfraude.

In 2019 publiceert het CBS een onderzoek naar specifiek slachtofferschap van cyber- en gedigitaliseerde criminaliteit (CBS, 2019b). In dit onderzoek zijn het ondervinden van hacken, vermogensdelicten, (niet-seksuele en seksuele) interpersoonlijke delicten en identiteitsfraude bevraagd. Bijna 9% van de bevraagde internetgebruikers geeft aan van ten minste één delict slachtoffer te zijn geworden in 2018 (zie tabel 1). Naast omvangcijfers is in dit onderzoek onder andere meer te lezen over de financiële en emotionele gevolgen voor slachtoffers en de mate dat slachtoffers beschermingsmaatregelen treffen.

2.2.2 Aangifte en meldingen in slachtofferenquêtes

Op basis van slachtofferenquêtes ligt de omvang van criminaliteit gemiddeld genomen hoger dan, bijvoorbeeld, verdachtenregistraties (zie hoofdstuk 4). Eén van de oorzaken hiervan is dat niet alle slachtoffers aangifte doen, omdat, bijvoorbeeld, de kosten van aangifte doen bij de politie niet opwegen tegen de baten (Jong, Leukfeldt & Van de Weijer, 2018). Het ondervonden delict kan door het slachtoffer niet ernstig genoeg gevonden worden of de verwachte pakkans wordt te laag ingeschat. Ook andere oorzaken kunnen ten grondslag liggen aan deze discrepantie. Zo kan de politie een delict niet ernstig genoeg vinden voor opsporing en/of vervolging, kan er geen duidelijke verdachte in beeld zijn, of is de bewijslast niet rond te krijgen. Bovendien hoeft niet alles wat door slachtoffers als criminaliteit wordt ervaren juridisch gezien ook daadwerkelijk criminaliteit zijn. Om een beter beeld te krijgen van slachtofferschap is het daarom belangrijk om niet alleen naar omvang te kijken, maar ook te kijken naar hoe vaak slachtoffers overgaan tot aangifte.

Onder slachtoffers van cybercriminaliteit heeft in 2012 ruim 7% aangifte gedaan bij de politie (zie tabel 1). Dit percentage is licht gestegen tot ruim 8% in 2019. Dit betekent dat in 2012 0,9% en in 2019 1% van de Nederlandse bevolking naar de politie is gestapt wegens cyber- en/of gedigitaliseerde criminaliteit.

2.2.3 Aangifte en meldingen in politieregistraties

Aangiftes en meldingen bij de politie zijn terug te vinden in politieregistraties. Het is in deze politieregistraties echter niet altijd duidelijk of bij een registratie sprake is van een cyber- of gedigitaliseerde component. Bij gedigitaliseerde criminaliteit, zoals online bedreiging, wordt het delict doorgaans geregistreerd zonder dat aangegeven wordt dat het gaat om een gedigitaliseerd delict. Bovendien worden voorvallen niet altijd door slachtoffers of door de politie herkent als een cyber- of gedigitaliseerd delict. Politieregistraties bevatten echter wel informatie in vrije tekstvelden die gebruikt kunnen worden om de omvang van cyber- of gedigitaliseerde criminaliteit te schatten.

Zo hebben Domenie, Leukfeldt, Toutenhoofd-Visser en Stol (2009) een zoeksleutel ontwikkeld om in een steekproef van politieregistraties uit 2007 in de regio's Zuid-Holland-Zuid en Holland-Midden na te kunnen gaan of er sprake is van cyber- of gedigitaliseerde criminaliteit. In 0,4-0,9% van de meldingen en aangiften uit Zuid-Holland-Zuid is sprake van cyber- of gedigitaliseerde criminaliteit en voor Hollands Midden is dit percentage 0,3-0,6%. Omdat deze statistieken uit 2007 komen, zijn deze niet opgenomen in de tabel.

Verder schatten Montoya, Junger en Hartel (2013) aan de hand van 900 registraties uit de politieregio Oost-Nederland het percentage registraties van traditionele delicten (diefstal/inbraak uit woning, diefstal/inbraak uit bedrijven, bedreiging en fraude)

waarbij sprake is van een digitale modus operandi in het jaar 2011. Met name bij fraude (40%) en bedreiging (16%) blijkt er vaker sprake te zijn van een digitale modus operandi. Bij diefstal uit woning is dit percentage aanzienlijk lager (3%) en bij diefstal uit bedrijven is er helemaal geen sprake van digitaal handelen.

De studies van Domenie et al. (2009) en Montoya et al. (2013) geven alleen inzicht in de relatieve omvang van cyber- en gedigitaliseerde criminaliteit binnen een steekproef van politieregistraties van enkele eenheden. Er kan niets gezegd worden van de daadwerkelijke omvang van registraties van cyber- en gedigitaliseerde criminaliteit in heel Nederland.

Tollenaar et al. (2019; zie ook Van der Laan & Tollenaar, nog te verschijnen) hebben de omvang van registraties van cyber- en gedigitaliseerde criminaliteit in de Basisvoorziening Handhaving (BVH) uit 2016 geschat (zie tabel 1). BVH-registraties bestaan zowel uit meldingen en aangiftes door slachtoffers, als registraties van handelingen die door de politie zelf geïnitieerd zijn tegen slachtofferloos crimineel gedrag (bijvoorbeeld drugs- of verkeerscriminaliteit). Omdat bij de onderzochte cyber- en gedigitaliseerde delicten uit sprake is van delicten die slachtoffers maken, is het aannemelijk dat de registraties die dergelijke delicten bevatten voornamelijk voortkomen uit meldingen en aangiftes van slachtoffers. Om deze reden zijn de BVH-registraties van cyber- en gedigitaliseerde criminaliteit uit Tollenaar et al. (2019) bij slachtofferschap ondergebracht. Aan de hand van predictieve textmining is het mogelijk om cyber- en gedigitaliseerd delicten automatisch te classificeren. De onderzoekers schatten dat bijna 13.500 (95% BI: 3.950-24.630) registraties van cybercriminaliteit en ruim 220.400 (95% BI: 131.570-292.540) registraties van gedigitaliseerde criminaliteit terug te vinden zijn in de BVH. Dit komt neer op respectievelijk 0,1-0,6% en 3-7% van alle registraties (zie tabel 1).

Ook worden vanaf oktober 2019 aantallen aangiftes van cybercrime publiekelijk gepresenteerd via open data van de politie[2]. Omdat het gaat om maandcijfers en er nog geen volledig kalenderjaar beschikbaar is, zijn de cijfers niet in de tabel opgenomen. Het gaat echter om bijna 400 tot ruim 1.800 aangiftes per maand in de periode oktober 2019 tot en met juni 2020.

2.2.4 Slachtofferschap onder jongeren

In de Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ) 2015 is, ten opzichte van daderschap, in mindere mate aandacht voor slachtofferschap. Slachtofferschap cybercriminaliteit betreft twee items (computervirus en hacken), waarvan de prevalentie in het jaar voorafgaand aan bevraging 9-30% is, afhankelijk van leeftijd (zie tabel 1). Er moet wel gezegd worden dat dit relatief hoge percentage vooral komt doordat relatief veel respondenten aangeven een schadelijk computervirus te hebben gehad. De schaal van slachtofferschap gedigitaliseerde criminaliteit betreft vier items (online bedreiging, cyberpesten, verspreiding seksueel beeldmateriaal en aan- of verkoopfraude) met een prevalentie van 11-14%, ook afhankelijk van leeftijd. Wanneer beide vormen van criminaliteit samengenomen worden, dan is de prevalentie slachtofferschap 16-37%.

2 https://data.politie.nl

Box 1 Dreigingsniveau slachtofferschap

Een indicatie voor dreiging voor slachtofferschap van cyber- en gedigitaliseerde criminaliteit is het aantal gestolen wachtwoorden van mailadressen. Volgens het Centraal Planbureau (CPB) zijn er 3,1 miljoen Nederlandse e-mailaccounts waarvan het wachtwoord gestolen of gelekt is (CPB, 2018). Deze wachtwoorden kunnen gebruikt worden om accounts te hacken en identiteitsfraude te plegen. Een andere indicator voor het dreigingsniveau van slachtofferschap zijn het aantal ontvangen phishing mails. Dit aantal ligt in Nederland relatief hoog. In 2018 betreft, onder Nederlandse gebruikers van Symantec antivirussoftware, één op de 877 ontvangen e-mails een poging tot phishing (Symantec, 2019). Alleen in Saudi-Arabië (één op 675) en in Noorwegen (één op 860) is het relatieve aantal ontvangen phishing e-mails nog groter. Daarnaast bevat in 2017 één op de bijna 1.300 e-mails in Nederland een poging tot phishing (Symantec, 2018).

2.3 Hacken

Met hacken wordt kortweg bedoeld dat op onrechtmatige wijze toegang wordt verkregen tot een digitale omgeving. Dergelijke omgevingen kunnen e-mail boxen, onlinebankiersystemen, afgesloten netwerken op werk en dergelijke zijn. De juridische term die gebruikt wordt voor hacken is computervredebreuk. De omvang van hacken verschilt sterk per bron.

2.3.1 Slachtofferschap van hacken onder de hele populatie

Oneigenlijke toegang tot iemands computer of onlineaccount is in meerdere bronnen bevraagd, waar iedere bron een andere omvang rapporteert (zie tabel 2). Waar volgens de Veiligheidsmonitor 6% van de respondenten gehackt zegt te zijn in 2012, is dat op basis van het LISS-panel slechts 2%. Beide bronnen laten tot 2018 min of meer een afname zien in het percentage respondenten dat zegt gehackt te zijn. Op basis van de Veiligheidsmonitor van 6% naar 5%, en op basis van het LISS-panel van bijna 3% tot 0,9%. In de laatste meting van de Veiligheidsmonitor uit 2019 is het percentage slachtoffers echter weer gestegen tot bijna 6%.

Statistieken uit Domenie et al. (2013) suggereren dat rond de 4% van alle respondenten slachtoffer zegt te zijn geweest van hacken. Net als bij andere delicten laat de Eurobarometer een relatief hoog slachtofferpercentages zien: 16% van hun respondenten geeft aan in het afgelopen jaar gehackt te zijn geweest.

Het rapport Digitale Veiligheid en Criminaliteit van het CBS (2019b) laat tot slot een nog ander percentage zien. Slechts 2% van de ondervraagde internetgebruikers van 12 jaar en ouder is slachtoffer geweest van hacken in 2018. Aan slachtoffers is doorgevraagd in hoeverre ze gevolgen van hacken hebben ondervonden. De meest genoemde gevolgen waren misbruik van e-mail of profielsite (27%), misbruik van persoonlijke gegevens op het internet (9%), virus met verlies van gegevens (7%), ransomware (6%) en malware (5%). In 39% van de gevallen ondervonden slachtoffers geen negatieve gevolgen.

2.3.2 Aangifte en meldingen van hacken in politieregistraties

Tollenaar et al. (2019) schatten dat er in 2016 3.710 politieregistraties van hacken zijn. Dit komt neer op 0,1% van alle registraties.

Tabel 2 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit hacken

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
CBS Veiligheidsmonitor												
Zelfgerapporteerd slachtofferschap					6,0%	6,2%	5,2%	5,1%	4,9%	4,9%		5,5%
Computer					1,5%	1,5%	1,2%	1,1%	1,0%	0,9%		0,8%
E-mailaccount					3,9%	3,5%	3,2%	2,7%	2,5%	2,3%		2,6%
Website					2,2%	2,5%	2,1%	2,4%	2,5%	2,6%		3,2%
Anders					3,3%	2,7%	2,1%	2,1%	2,1%	2,2%		2,2%
Percentage slachtoffers die aangifte hebben gedaan					2,4%	1,8%	1,8%	1,8%	2,3%	2,3%		2,7%
Aantal delicten per 100 inwoners					8,8	9,3	7,9	7,6	7,4	7,5		8,2
LISS-panel												
Zelfgerapporteerd slachtofferschap	2,7%		1,4%		1,9%		1,3%		1,3%		0,9%	
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap											1,8%	
Percentage slachtoffers die aangifte hebben gedaan											5,1%	
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap alle respondenten				3,7%								
Zelfgerapporteerd slachtofferschap internetgebruikers				4,3%								
Percentage slachtoffers die aangifte hebben gedaan				4,1%								
Eurobarometer												
Zelfgerapporteerd slachtofferschap							16%					
Textmining politieregistraties (BVH)												
Aantal registraties hacken									3.710			
Percentage registraties hacken van totaal									0,09%			
Monitor Zelfgerapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd slachtofferschap hacken												
10- en 11-jarigen								1,8%				
12- tot en met 17-jarigen								3,5%				
18- tot en met 22-jarigen								5,7%				

2.3.3 Slachtofferschap van hacken onder jongeren

In de MZJ 2015 geeft grofweg 2-6% van de jongeren aan slachtoffer te zijn geweest van een hack in het jaar voorafgaand aan deelname (zie tabel 2). Met bijna 2% bij 10- en 11-jarigen lijken zij het minst slachtoffer te zijn, tegenover bijna 4% en 6% bij respectievelijk 12- tot en met 17-jarigen en jongvolwassenen.

2.4 DDoS-aanvallen

Denial of Service (DoS-)aanvallen worden ingezet om computers of systemen onbruikbaar te maken voor hun eigenlijke doeleindes. Dit kan op kleine schaal een privécomputer raken, waardoor iemand tijdelijk het internet niet op kan. Op grote schaal kan het websites van banken of overheidsinstanties raken, waardoor online-diensten niet meer bruikbaar zijn. Er zijn verschillende methoden om een DoS-aanval succesvol uit te voeren, maar meestal wordt een computer- of systeem overladen ver boven de gebruikelijke capaciteit. Hierdoor worden de diensten trager om te gebruiken of vallen zij geheel weg.

Een Distributed Denial of Service (DDoS-)aanval is een ernstigere variant van een DoS-aanval, omdat in plaats van één aanvaller meerdere aanvallers tegelijkertijd actief zijn. Dit kunnen verschillende individuen zijn die samen een aanval coördineren of kan met behulp van een botnet uitgevoerd worden (d.w.z., een netwerk van geïnfecteerde computers of apparaten). Daarnaast worden DDoS-aanvallen ook vaak aangeboden als cybercrime-as-a-service (Karami, Park & McCoy,2016; zie ook hoofdstuk 5). Afhankelijk van het doelwit en de gebruikte methode, kunnen dergelijke aanvallen relatief triviaal zijn tot en met zeer ernstig.

2.4.1 Aantal gemelde DDoS-aanvallen

Aangezien DDoS-aanvallen niet gericht zijn op individuen, maar op computers of systemen, is het aantal slachtoffers van DDoS-aanvallen vaak niet uit te drukken als percentages van de Nederlandse bevolking. Het Nationale Beheersingsorganisatie Internet Providers (NBIP) biedt wel op een andere manier inzicht geboden in de omvang van dit type criminaliteit (NBIP, 2017; 2018; 2019). In 2016 heeft het NBIP 680 meldingen van een DDoS-aanval verwerkt en dit aantal is de daaropvolgende jaren toegenomen tot ongeveer 900 meldingen per jaar (zie tabel 3). Bij de politie zijn tussen april 2014 en april 2015 67 aangiftes geregistreerd van DDoS-aanvallen (NCSC, 2015). Deze aangiftes zijn overigens voornamelijk gedaan door organisaties.

2.4.2 Aangifte en meldingen van DDoS-aanvallen in politieregistraties

In een textmining onderzoek binnen politieregistraties naar cyberdelicten wordt een schatting gegeven van 2.210 registraties met DDoS-aanvallen in 2016 (Tollenaar et al., 2019; zie tabel 3). Dit komt neer op 0,1% van alle registraties.

Tabel 3 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit DDoS-aanvallen

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
NBIP												
Aantal gemelde aanvallen									680	826	938	919
Cybersecuritybeeld Nederland												
Aantal aangiften								67				
Textmining politieregistraties (BVH)												
Aantal registraties DDoS-aanvallen									2.210			
Percentage registraties DDoS-aanvallen van totaal									0,06%			

2.4.3 Toegang tot onlinediensten

In de Eurobarometer is gevraagd of respondenten ooit geen toegang konden krijgen tot onlinediensten van een bank of overheid. Dit wijst mogelijk op systemen die zijn getroffen door een DDoS-aanval (maar het kan evengoed het gevolg zijn van een reguliere storing). Van de Nederlandse respondenten antwoordt 28% in 2012 en 43% in 2014 bevestigend. In 2014 was dat bijna twee keer zo hoog als in andere Europese landen.

2.5 Malware

Onder malware worden alle vormen van software verstaan die als doel hebben om een computer of systeem te beschadigen. Daarbij hoeft niet noodzakelijk sprake te zijn van zichtbare schade, zoals het totaal onbruikbaar maken van een systeem, maar ook van onzichtbare, indirecte schade, zoals installeren van spionagesoftware. Naast spionagesoftware vallen, onder andere, computervirussen, Trojaanse paarden en ransomware ook onder de noemer malware. Hoewel het programmeren van malware op zichzelf niet noodzakelijk een strafbaar feit is, is de distributie van malware dat wel, omdat er dan (pas) schade kan optreden. De afgelopen jaren is slachtofferschap van malware afgenomen.

2.5.1 Slachtofferschap van malware onder de hele populatie

Malware is een vorm van cybercrime waar relatief veel mensen slachtoffer van worden. Op basis van het LISS-panel is 14% van de respondenten slachtoffer van een schadelijk computervirus in 2008 (zie tabel 4). Dit percentage is gedaald tot bijna 2% in 2018. In ander onderzoek is het percentage slachtoffers van een computervirus waarbij gegevens zijn verloren 6% in 2015 (CBS, 2016).

Volgens de Eurobarometer is 62% van de Nederlanders in 2014 slachtoffer van malware—een aanzienlijk verschil met andere cijfers. Echter, bij de Eurobarometer is niet in de vraag opgenomen dat malware schade heeft toegebracht. Ook in Domenie et al. (2013) was een relatief hoog percentage van bijna 17% in 2011 slachtoffer van malware. Ook hier is in de vraagstelling niet als voorwaarde gesteld dat er schade moest zijn, maar uit een vervolgvraag blijkt slechts 16% van de slachtoffers schade heeft opgelopen. Het merendeel van deze schade betreft tussen € 1 tot € 100 (ruim 57%).

Gegevens uit het LISS-panel suggereren een daling van slachtofferschap van dit type delict. Het is goed mogelijk dat de daling komt door daadwerkelijke afname, bijvoorbeeld omdat beschermingssoftware beter is geworden in het herkennen van malware of omdat mensen bewuster internet zijn gaan gebruiken. Een andere verklaring is dat de term computervirus misschien verouderd is, waardoor men bij het ondervinden van nieuwe vormen van malware (mogelijk onterecht) zegt geen slachtoffer te zijn geweest van een computervirus.

2.5.2 Malware aanvallen en geïnfecteerde computers

Aangezien malwareaanvallen zich richten op computers in plaats van personen, zijn geïnfecteerde computers een andere relevante indicator voor slachtofferschap van malware. Echter, dergelijke gegevens omtrent geïnfecteerde computers zijn echter

niet noodzakelijk accuraat, omdat deze gegevens afkomstig zijn van partijen die een belang hebben bij (een groeiende) omvang van malware.

Van Eeten, Asghari, Bauer en Tabatabaie (2011) laten zien dat 5-10% van Nederlandse IP-adressen gerelateerd zijn aan een geïnfecteerde computer (zie tabel 4). Het daadwerkelijke aantal geïnfecteerde computers ligt waarschijnlijk hoger, omdat de onderzoekers niet alle mogelijke datasets hebben gebruikt (p. 23).

Panda, een aanbieder van antivirussoftware, rapporteert op basis van hun eigen gebruikers ook percentages geïnfecteerde computers (PandaLabs, 2009; 2011; 2012; 2013; 2014; 2015; zie tabel 4). Tussen 2009 en 2015 is het aantal geïnfecteerde computers afgenomen van 38% tot bijna 27%. Dit stemt overeen met de eerder beschreven dalende trend in zelfgerapporteerd slachtofferschap.

Andere partijen presenteren het aantal doelwitten van malware per land relatief ten opzichte van het totale aantal doelwitten wereldwijd. Volgens Akamai (2017) is in het tweede kwartaal van 2017 ruim 6% van alle malware aanvallen gericht op Nederlandse computers of systemen. Nederland behoort daarmee tot de vier meest aangevallen landen met ruim 23 miljoen malware aanvallen (zie tabel 4). Echter, in ranglijsten gepresenteerd door Kaspersky komt Nederland niet terug in de top tien van meest aangevallen landen (Gudkova, Vergelis, Shcherbakova, & Demidova, 2017; Unuchek, Sinitsyn, Parinov, & Liskin, 2017).

Als specifiek wordt gekeken naar ransomware behoort Nederland wel tot de meest getroffen landen (Symantec, 2017). In 2016 en 2017 zijn 3% van de ransomware aanvallen wereldwijd gericht op Nederlandse systemen. In slechts vijf landen zijn meer ransomware aanvallen gedetecteerd.

2.5.3 Aangifte en meldingen van malware in politieregistraties

Tollenaar et al. (2019) schatten dat er ruim 1.930 registraties van ransomware in de BVH geregistreerd staan in 2016 (zie tabel 4). Dat komt neer op bijna 0,1% van het totale aantal registraties.

2.5.4 Slachtofferschap van malware onder jongeren

Een relatief hoog percentage van jongeren geeft aan in het jaar voorafgaand aan deelname aan de MZJ 2015 slachtoffer te zijn geweest van een computervirus. De prevalentie is 8-27%, waarbij de ondergrens van prevalentie bij de 10- en 11-jarigen zit en de bovengrens bij de jongvolwassenen (zie tabel 4).

Tabel 4 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit malware

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Domenie et al. (2013)												
Zelfgeraporteerd slachtofferschap malware				16,6%								
LISS-panel												
Zelfgeraporteerd slachtofferschap computervirus met schade	14,0%		8,9%		6,1%		2,4%		3,3%		1,7%	
CBS ICT												
Zelfgeraporteerd slachtofferschap computervirus met verlies								6,0%				
Eurobarometer												
Zelfgeraporteerd slachtofferschap malware							62%					
Van Eeten et al. (2011)												
Percentage IP-adress gelinkt aan geïnfecteerde apparaten van het totale aantal IP-adressen (95% BI)				5-10%								
PandaLabs												
Percentage geïnfecteerde computers van het totale aantal computers van gebruikers		38,0%		34,0%	24,0%	23,6%	23,6%	26,5%				
Akamai												
Web application attacks op Nederlandse systemen (in absolute aantallen) van gebruikers										5.326.137		
Textmining politieregistraties (BVH)												
Aantal registraties ransomware									1.934			
Percentage registraties ransomware van totaal									0,05%			
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd slachtofferschap virus ontvangen												
10- en 11-jarigen								7,7%				
12- tot en met 17-jarigen								17,4%				
18- tot en met 22-jarigen								27,1%				

2.6 Online bedreiging, cyberpesten en verspreiding seksueel beeldmateriaal

Bedreigen is het uiten van intenties van schade toebrengen, waarbij het dreigen met fysiek geweld een veel voorkomende variant is. Ook kan gedreigd worden met financiële of sociale schade, door bijvoorbeeld schadelijke leugens over iemand te verspreiden. De meest ernstige vorm van bedreiging is de doodsbedreiging.
Ver voor het internettijdperk werden bedreigingen al geuit, maar tegenwoordig is het makkelijk om te bedreigen via digitale kanalen, zoals e-mail, social media of WhatsApp. Niet alle dreigende uitingen zullen strafrechtelijke dreigingen van geweld zijn, maar kunnen afhankelijk van het karakter cyberpesten of stalking betreffen. Ook is het belangrijk voor een strafrechtelijk vervolgbare bedreiging dat de bedreiger in staat is om de dreiging werkelijkheid te maken.

Cyberpesten is in dit onderzoek naar criminaliteit wel meegenomen, omdat het onderdeel uitmaakt van de CBS Veiligheidsmonitor. In de CBS Veiligheidsmonitor wordt cyberpesten in de volgende categorieën opgesplitst: laster, chantage, stalking, bedreiging en overig. Bedreigingen die geuit worden om een persoon te dwingen tot iets anders, zoals de afgifte van geld, worden gezien als afpersing. Gezien het niet-fysieke, maar wel dreigende en schadelijke karakter van de gedraging (naast eventuele inbreuk op portretrecht), wordt het verspreiden van seksueel beeldmateriaal zonder toestemming van degene in beeld door ons geschaard bij bedreiging en cyberpesten.

Slachtofferschap van online bedreiging en cyberpesten onder de gehele populatie ligt tussen de 1% en 3% tot en met 2018. In 2019 is het percentage slachtoffers van cyberpesten in de Veiligheidsmonitor gestegen tot ruim 4% (CBS, 2020a). Onder jongeren ligt dit percentage hoger.

2.6.1 Slachtofferschap van online bedreiging en cyberpesten onder de hele populatie

Online bedreiging is een gedigitaliseerd delict waarvan verwacht kan worden dat door de toename van internetgebruik en social media een verplaatsing van offline naar online heeft plaatsgevonden. Slachtofferenquêtes laten echter geen stijging in online bedreiging of cyberpesten zien. Het aantal slachtoffers van cyberpesten ligt op basis van de Veiligheidsmonitor tot 2017 rond de 3% (zie tabel 5). In 2019 is dit percentage gestegen tot ruim 4%. Slachtofferschap van online bedreiging ligt op basis van het LISS-panel lager met 1-2%. Aan deze slachtoffers is doorgevraagd hoe ernstig zij de online bedreiging hebben ervaren. Ongeveer de helft van de slachtoffers heeft aangegeven het voorval niet als ernstig te hebben ervaren (bijna 53%), terwijl bijna een derde (33%) het als redelijk ernstig en 15% het als bijzonder ernstig heeft ervaren (Sipma & Van Leijsen, 2019).

Domenie et al. (2013), rapporteren dat 0,6% slachtoffer is geworden van online bedreiging en 1% van cyberstalking (zie tabel 5). Het rapport CBS Digitale Veiligheid en Criminaliteit laat een vergelijkbaar cijfer zien: ruim 1% is slachtoffer geworden van interpersoonlijke incidenten zonder seksuele bijbedoeling. In dit onderzoek is ook expliciet gevraagd naar interpersoonlijke incidenten waarbij sprake was van een seksuele bedoeling (CBS, 2019b). 0,7% van de respondenten is hier slachtoffer van geweest.

Tabel 5 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit online bedreiging

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
CBS Veiligheidsmonitor												
Zelfgerapporteerd slachtofferschap cyberpesten					3,1%	3,3%	3,1%	3,2%	3,2%	3,1%		4,2%
Laster					1,0%	1,1%	0,9%	1,0%	1,0%	1,0%		1,0%
Chantage					0,3%	0,2%	0,2%	0,3%	0,3%	0,3%		1,0%
Stalken					0,7%	0,7%	0,7%	0,8%	0,8%	0,8%		0,8%
Bedreiging					0,6%	0,6%	0,6%	0,5%	0,6%	0,6%		0,6%
Anders					1,1%	1,2%	1,1%	1,1%	1,1%	1,1%		1,3%
Percentage slachtoffers die aangifte hebben gedaan					5,0%	5,3%	5,4%	6,4%	4,9%	5,7%		5,6%
Aantal delicten per 100 inwoners					5,9	6,3	6,0	6,3	6,0	6,1		7,9
LISS-panel												
Zelfgerapporteerd slachtofferschap online bedreiging	2,4%		1,4%		1,5%		0,9%		1,7%		1,8%	
Percentage slachtoffers die aangifte hebben gedaan			23,9%								18,9%	
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap online bedreiging				0,6%								
Percentage slachtoffers die aangifte hebben gedaan online bedreiging				30,4%								
Zelfgerapporteerd slachtofferschap cyberstalking				1,0%								
Percentage slachtoffers die aangifte hebben gedaan cyberstalking				27,8%								
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap niet-seks. incident											1,4%	
Laster											1,0%	
Roddelen											0,7%	
Foto's en filmpjes verspreiden											0,2%	
Overig laster											0,2%	
Stalken											0,5%	
Bedreiging met geweld											0,3%	
Percentage slachtoffers die aangifte hebben gedaan												
Laster											6,4%	
Stalken											11,1%	
Bedreiging met geweld											11,4%	
Zelfgerapporteerd slachtofferschap seksueel incident											0,7%	
Laster											0,3%	
Roddelen											0,2%	
Foto's en filmpjes verspreiden											0,1%	
Overig laster											0,1%	

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Stalken											0,4%	
Bedreiging met geweld											0,1%	
Percentage slachtoffers die aangifte hebben gedaan												
Laster											9,6%	
Stalken											9,8%	
Textmining politieregistraties (BVH)												
Aantal registraties online bedreiging									116.770			
Percentage registraties online bedreiging van totaal									2,96%			
Aantal registraties online stalking									65.903			
Percentage registraties online stalking van totaal									1,67%			
Aantal registraties online smaad									103.471			
Percentage registraties online smaad van totaal									2,62%			
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd slachtofferschap cyberpesten												
10- en 11-jarigen								6,4%				
12- tot en met 17-jarigen								7,4%				
18- tot en met 22-jarigen								3,3%				
Zelfgerapporteerd slachtofferschap online bedreiging												
10- en 11-jarigen								2,4%				
12- tot en met 17-jarigen								5,0%				
18- tot en met 22-jarigen								4,3%				
Zelfgerapporteerd slachtofferschap seksueel beeldmateriaal verspreid zien worden												
10- en 11-jarigen								0,0%				
12- tot en met 17-jarigen								0,7%				
18- tot en met 22-jarigen								0,0%				
Jeugd en Cybersafety (10- tot en met 18-jarigen)												
Zelfgerapporteerd slachtofferschap cyberpesten				9,4%								
Roddelen				7,3%								
Uitschelden en/of bedreigen				4,6%								
Buitensluiten				2,2%								
Het op internet plaatsen van vervelende foto's of filmpjes.				1,3%								
Ontvangen van vervelende foto's of filmpjes				0,6%								
EU Kids Online (9- tot en met 16-jarigen)												
Zelfgerapporteerd slachtofferschap cyberpesten				4,0%								

2.6.2 Aangifte en meldingen van online bedreiging in politieregistraties

Omvangcijfers van slachtofferschap van online bedreiging en verwante delicten op basis van BVH-registraties komen uit Tollenaar et al. (2019). In dit onderzoek is gekeken naar online bedreiging, online stalking en online smaad. Zij schatten dat er 116.770 registraties zijn van online bedreiging in 2016 (zie tabel 5). Dit is 3% van het totale aantal registraties. Het aantal registraties van online stalking wordt geschat op ruim 65.900 en van online smaad op ruim 103.470, wat afzonderlijk 2-3% van het totale aantal registraties is.

2.6.3 Slachtofferschap van online bedreiging en cyberpesten onder jongeren

Bij slachtofferschap gedigitaliseerde criminaliteit van de MZJ 2015 gaan drie items over online bedreiging, cyberpesten en het verspreiden seksueel beeldmateriaal. Cyberpesten komt het meeste voor met een prevalentie van 3-7% (zie tabel 5). Binnen de leeftijdsgroepen komt dit het meest voor bij minderjarigen (6-7%) en het minst bij jongvolwassenen (ruim 3%). Online bedreiging komt met 2-5% iets minder vaak voor en de prevalentie van slachtofferschap van de verspreiding van seksueel beeldmateriaal komt, ongeacht leeftijdsgroep, niet boven de 1% uit.

Slachtofferschap van cyberpesten onder jongeren is ook gemeten in het Jeugd en Cybersafety onderzoek (Kerstens & Stol, 2012). In totaal geeft ruim 9% van de bevraagde jongeren aan in de afgelopen drie maanden slachtoffer te zijn geworden van ten minste één vorm van cyberpesten (zie tabel 5). Dit percentage ligt hoger dan de MZJ-prevalentie. Mogelijk omdat roddelen, een item dat in het Jeugd en Cybersafety onderzoek relatief veel voorkomt (ruim 7%), niet door MZJ-jongeren beschouwd wordt als cyberpesten. Andere vormen van cyberpesten komen minder vaak voor. Bijna 5% van de ondervraagden is uitgescholden of bedreigd, ruim 2% is buitengesloten, ruim 1% heeft vervelende filmpjes/foto's van zichzelf op het internet geplaatst zien worden en 0,6% heeft vervelende filmpjes/foto's ontvangen.

Afsluitend, volgens het door de Europese Unie uitgezette onderzoek EU Kids Online (Livingstone et al., 2011) is 4% van de Nederlandse jongeren tussen de 9 en 16 jaar slachtoffer geworden van cyberpesten (zie tabel 5).

2.7 Online fraude

Bij fraude bevoordeelt een dader zich onder valse voorwendselen, vaak ten koste van een slachtoffer. De strafrechtelijke term voor fraude is bedrog. Horizontale fraude treedt op tussen twee (of meer) private burgers, waarbij één partij de dader is en de andere partij het slachtoffer. Ook fraude tussen burgers en rechtspersonen valt onder horizontale fraude, zoals bank- en hypotheekfraude. Voor horizontale online fraude kan gedacht worden aan aan- en verkoopfraude, waar via Marktplaats verkochte producten niet opgestuurd worden na ontvangen van betaling, of juist geen betaling wordt gedaan wanneer een product wel is ontvangen. Andere vormen van horizontale online fraude zijn phishing (waar men onder valse voorwendselen via digitale kanalen gegevens probeert te verkrijgen) en identiteitsfraude (wanneer iemands identiteit wordt misbruikt voor eigen gewin). Verticale fraude treedt op tussen burger en overheid, waarbij de burger de dader is. In de huidige paragraaf wordt echter alleen gekeken naar horizontale fraude via onlinekanalen. Doordat

bankieren en winkelen steeds vaker online plaatsvinden, wordt verondersteld dat online fraude de afgelopen jaren is toegenomen. Aan de hand van verschillende bronnen kan een beeld worden geschetst in hoeverre deze veronderstelling klopt.

2.7.1 Identiteitsfraude

Identiteitsfraudeurs doen zich online voor als iemands anders, vaak voor eigen gewin en ten koste van het slachtoffer wiens identiteit wordt gebruikt. De mate waarin slachtofferschap van dit type delict voorkomt onder de Nederlandse bevolking is relatief gering (zie tabel 6). In 2012 is ruim 1% slachtoffer van identiteitsfraude, terwijl dit in 2019 nog slechts 0,5% is volgens de CBS Veiligheidsmonitor). Hoewel het LISS-panel weliswaar een lichte stijging meldt (0,1% in 2010 en 0,3% in 2018), blijft het aantal slachtoffers relatief laag. Ook CBS Digitale Veiligheid & Criminaliteit (2019b), Domenie et al. (2013) en CBS ICT, kennis en economie (2016) laten omvangschattingen van 1% of minder zien. Een studie uitgevoerd door PricewaterhouseCoopers onder een representatieve steekproef van de Nederlandse bevolking laat een hoger prevalentiecijfer zien van bijna 5% in 2012 (PwC, 2013). In dit onderzoek zijn enkele vormen van identiteitsfraude uitgebreid bevraagd met toelichtingen.[3] Hierdoor herkennen slachtoffers hetgeen hen is overkomen mogelijk eerder, dan wanneer alleen gevraagd is naar identiteitsfraude in het algemeen. Volgens de Eurobarometer is de omvang van slachtofferschap van identiteitsfraude gestegen van 1% in 2012 naar 3% in 2014.

Aangiften en meldingen van identiteitsfraude in politieregistraties (en elders)
Tollenaar et al. (2019) schatten dat het aantal registraties van identiteitsfraude op ruim 34.210 ligt in 2016, wat neerkomt op 0,9% van het totale aantal registraties in het BVH (zie tabel 6). In 2009 tot en met 2012 worden er jaarlijks tussen de 160 en 300 meldingen van identiteitsfraude gemaakt bij het Centraal Meld- en Informatiepunt Identiteitsfraude.

Identiteitsfraude onder jongeren
Onder jongeren van 11 tot en met 18 jaar is het percentage slachtofferschap identiteitsfraude met 9% relatief hoog (zie tabel 6). Een verklaring kan zijn dat jongeren meer tijd online doorbrengen dan ouderen, en daardoor meer gegevens van zichzelf online plaatsen of opslaan, die vervolgens misbruikt kunnen worden.

3 Financiële identiteitsfraude: bijvoorbeeld skimmen van uw pinpas, automatische incasso's op naam, diefstal van creditcard gegevens, aankoop van spullen op uw naam, huren van voertuigen of spullen met gebruik van (een kopie van) uw paspoort of rijbewijs.
Criminele identiteitsfraude, bedoeld om de eigen identiteit te verhullen: bijvoorbeeld gebruik van uw identiteit bij een aanhouding, opgeven van uw identiteit bij zwartrijden in openbaar vervoer, gebruik van uw identiteit bij een rechtszaak.
Misbruik van uw naam en BSN bij een huisarts of ziekenhuis: bijvoorbeeld gebruik van uw naam (en BSN) door iemand anders bij de huisarts of in het ziekenhuis om medische hulp te krijgen.
Identiteitsfraude op het web: bijvoorbeeld gebruik van uw naam om op het internet producten aan te schaffen, gebruik van uw identiteit om een website of e-mailadres aan te vragen, publicatie van een bericht op een site onder uw naam zonder toestemming.

Tabel 6 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit identiteitsfraude

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
CBS Veiligheidsmonitor												
Zelfgerapporteerd slachtofferschap identiteitsfraude					1,3%	0,8%	0,6%	0,4%	0,4%	0,4%		0,5%
Percentage slachtoffers die aangifte hebben gedaan					12,5%	13,0%	11,6%	13,1%	16,9%	16,9%		21,9%
Aantal delicten per 100 inwoners					1,6	1,3	0,7	0,6	0,4	0,4		0,60
LISS-panel												
Zelfgerapporteerd slachtofferschap identiteitsfraude			0,1%		0,2%		0,2%		0,3%		0,3%	
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap lening, abonnement, goederen of diensten verkregen op naam											0,2%	
Zelfgerapporteerd slachtofferschap identiteitsfraude zonder financiële schade											1,0%	
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap identiteitsfraude				0,5%								
Percentage slachtoffers die aangifte hebben gedaan				15,6%								
CBS ICT												
Zelfgerapporteerd slachtofferschap identiteitsfraude					0,03%							
PwC												
Zelfgerapporteerd slachtofferschap identiteitsfraude					4,6%							
Eurobarometer												
Zelfgerapporteerd slachtofferschap identiteitsfraude					1%		3%					
Textmining politieregistraties (BVH)												
Aantal registraties identiteitsfraude									34.214			
Percentage registraties identiteitsfraude van totaal									0,9%			
Centraal Meld- en Informatiepunt Identiteitsfraude												
Aantal meldingen		245	163	221	291							
Jeugd en Cybersafety (10- tot en met 18-jarigen)												
Zelfgerapporteerd slachtofferschap identiteitsfraude				9,0%								

2.7.2 Phishing en pharming

Een vorm van online fraude betreft het via phishingmails lokken van slachtoffers naar besmette websites. Op basis van studies van het CBS (2016; 2019b) blijkt dat tussen de 1-2% van de respondenten slachtoffer is geweest van phishing (zie tabel 7). Het aantal mensen dat ooit een poging tot phishing heeft ondervonden ligt vele malen hoger (35-59%). Microsoft rapporteert dat het aantal phishingsmails in 2018 met 250% is toegenomen ten opzichte van 2017 (NCSC, 2019).

2.7.3 Bank- en creditcardfraude

Via phishing proberen daders onder andere toegang te krijgen tot bankgegevens om bank- of creditcardfraude te plegen. Het aantal slachtoffers van ongeautoriseerde bankafschrijvingen is gedaald van meer dan 3% in 2010 tot ruim 1% in 2018 volgens het LISS-panel (zie tabel 8). In datzelfde laatste jaar rapporteert het CBS (2019b) ook bijna 1% slachtofferschap. De Eurobarometer rapporteert in het eerdere jaar 2014 een relatief hoog percentage van 8%. Creditcard- en betaalkaartfraude is met jaarlijks 0,5-1% slachtofferschap redelijk stabiel.

2.7.4 Aan- en verkoopfraude

Het percentage slachtoffers van aan- of verkoopfraude schommelt tussen 3-5% (zie tabel 9). De CBS Veiligheidsmonitor (CBS, 2020a), die aan- en verkoopfraude tezamen meet, laat een lichte stijging zien van bijna 3% in 2012 tot bijna 5% in 2019. Ook onder respondenten van het LISS-panel, waar alleen een vraag over online aankoopfraude is opgenomen, is slachtofferschap toegenomen van ruim 2% in 2008 tot ruim 4% in 2018. Ook andere bronnen van online aankoopfraude rapporteren tevens percentages van 2-3%. Alleen de Eurobarometer laat hogere percentages zien (9-16%) en betreft zowel aan- als verkoopfraude. De omvang van zelfgerapporteerd slachtofferschap van online verkoopfraude ligt tussen 0,2% en de 0,3% volgens verschillende bronnen. Slachtofferschap van online verkoopfraude lijkt dus minder vaak voor te komen dan aankoopfraude.

Aangifte en meldingen van online aan- en verkoopfraude in politieregistraties
Predictief textminingsonderzoek heeft een schatting gemaakt van het aantal BVH-registraties met online aan- en verkoopfraude in 2016 (Tollenaar et al., 2019). De omvang van online aan- en verkoopfraude is bijna 33.900 registraties, wat 0,9% van het totale aantal registraties is (zie tabel 9).

Aan- en verkoopfraude onder jongeren
In de MZJ 2015 is aan jongeren gevraagd of zij slachtoffer zijn geweest van online aan- of verkoopfraude. De prevalentie van dit slachtofferschap ligt op grofweg 5-9% van de jongeren, afhankelijk van leeftijd (zie tabel 9). Het minst komt dit voor bij 10- en 11-jarigen (bijna 5%) en het meest bij jongvolwassenen (ruim 9%). Door de vraagstelling kan geen onderscheid gemaakt worden tussen aan- en verkoopfraude. Het aantal jongeren tussen 10 en 18 jaar dat volgens het Jeugd en Cybersafety onderzoek slachtoffer is geworden van online aankoopfraude is ruim 5% in 2011.

2.7.5 Overige vormen van online fraude

Voorschotfraude is een vorm van fraude waarbij slachtoffers grote geldbedragen wordt beloofd als zij eerst een relatief klein bedrag aan onkosten voorschieten of een kleine investering doen. Vervolgens worden slachtoffers niet uitbetaald (Domenie et al. 2013). Slechts 0,2% van de bevraagden was daar in 2011 slachtoffer van geworden (zie tabel 10).

In de het CBS-onderzoek Digitale Veiligheid & Criminaliteit zijn een drietal online vermogensdelicten bevraagd (CBS, 2019b; zie tabel 10). Van de bevraagden heeft 0,3% een nepboete of -factuur betaald en is 0,2% slachtoffer geworden van een Microsoftscam. Deze mensen zijn gebeld door iemand die zich voordoet als een medewerker van Microsoft en vraagt bepaalde software te installeren op de computer van het slachtoffer. Wangirifraude, waarbij daders slachtoffer bellen en vervolgens direct of snel ophangen, in de hoop dat slachtoffers terugbellen naar dure (buitenlandse) nummers, treft 0,5% van de respondenten.

Cyberafpersing, wat in de Eurobarometer geoperationaliseerd is als het eisen van geld in ruil voor het vrijgeven van een device (en dus onder ransomware zou kunnen vallen), komt bij 10% van de respondenten voor in 2014 (zie tabel 10).

Overige vormen van online fraude onder jongeren
De studie van Kerstens & Jansen (2016) laat zien dat ruim 15% van de door hun bevraagde jongeren tussen van 11-18 jaar slachtoffer is geworden van virtuele diefstal (zie tabel 10). Virtuele diefstal betreft in dit geval het stelen van virtuele goederen, zoals skins, in online games. Dat dit delict relatief veel voorkomt, in vergelijking met andere vormen van fraude, komt hoogstwaarschijnlijk omdat Kerstens en Jansen (2016) jongeren hebben bevraagd. Jongeren hebben gemiddeld genomen een grotere kans om slachtoffer te worden van online criminaliteit (zie bijv., Sipma & Van Leijsen, 2019) en zullen bovendien vaker online gamen dan ouderen. Hierdoor is het aannemelijk dat zij een grotere kans hebben om slachtoffer te worden van virtuele diefstal. Bovendien speelt mee dat diefstal van virtuele goederen gezien kan worden als spelelement, waardoor afgevraagd kan worden in hoeverre jongeren zich strafrechtelijk slachtoffer zullen voelen.

2.7.6 Aangifte van online fraude

Bij online fraude wordt relatief vaak aangifte gedaan, zoals de 19-20% van slachtoffers van online aan- of verkoopfraude laten zien (zie tabel 9). Een ruime meerderheid van slachtoffers van bankfraude maakt ook melding bij hun bank (Van Wilsem et al., 2013). Aangezien slachtoffers van deze typen delicten financiële schade hebben opgelopen, liggen potentiële baten van aangifte of andersoortige melding mogelijk hoger dan bij andere cyber- of gedigitaliseerde delicten.

Tabel 7 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit phishing

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap phishing											1,0-1,5%	
Phishing mail ontvangen											35%	
CBS ICT												
Zelfgerapporteerd slachtofferschap phishing								1,0-2,0%				
Phishing mail ontvangen								59%				

Tabel 8 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit bankfraude

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
LISS-panel												
Zelfgerapporteerd slachtofferschap ongeautoriseerde bankafschrijving			3,0%		2,7%		1,7%		1,7%		1,2%	
Percentage slachtoffers die aangifte hebben gedaan ongeautoriseerde bankafschrijving			12,1%								9,8%	
Zelfgerapporteerd slachtofferschap creditcardfraude	0,5%		0,7%		0,7%		0,7%		0,5%		0,7%	
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap geld van rekening gehaald en/of betalingen gedaan											0,5%	
Percentage slachtoffers die aangifte hebben gedaan											18,3%	
CBS ICT												
Zelfgerapporteerd slachtofferschap fraude met betaalkaarten								1,0%				
Eurobarometer												
Zelfgerapporteerd slachtofferschap online bankfraude							8,0%					

Tabel 9 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit online aan- en verkoopfraude

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
CBS Veiligheidsmonitor												
Zelfgerapporteerd slachtofferschap aan- en verkoopfraude					2,9%	3,3%	3,5%	3,5%	3,4%	3,9%		4,6%
Aankoopfraude					2,7%	3,1%	3,3%	3,4%	3,3%	3,6%		4,3%
Verkoopfraude					0,2%	0,2%	0,1%	0,2%	0,2%	0,2%		0,3%
Percentage slachtoffers die aangifte hebben gedaan aan- en verkoopfraude					20,2%	21,8%	20,1%	20,0%	20,2%	20,2%		19%
Aantal delicten per 100 inwoners aan- en verkoopfraude					3,4	3,9	4,1	4,2	4,1	4,6		5,7
LISS-panel												
Zelfgerapporteerd slachtofferschap aankoopfraude	2,2%		2,4%		2,6%		2,1%		2,9%		4,4%	
Percentage slachtoffers die aangifte hebben gedaan aankoopfraude			12,0%				26,4%				12,0%	
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap aankoopfraude											2,7%	
Percentage slachtoffers die aangifte hebben gedaan aankoopfraude											22,6%	
Zelfgerapporteerd slachtofferschap verkoopfraude											0,2%	
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap aankoopfraude internetgebruikers				2,4%								
Zelfgerapporteerd slachtofferschap aankoopfraude online kopers				3,1%								
Percentage slachtoffers die aangifte hebben gedaan aankoopfraude				21,1%								
Zelfgerapporteerd slachtofferschap verkoopfraude internetgebruikers				0,3%								
Zelfgerapporteerd slachtofferschap verkoopfraude online kopers				1,0%								
Percentage slachtoffers die aangifte hebben gedaan verkoopfraude				8,0%								
CBS ICT (12 jaar en ouder)												
Zelfgerapporteerd slachtofferschap aankoopfraude								2%	3%	3%		
Eurobarometer												
Zelfgerapporteerd slachtofferschap aan- en verkoopfraude					9%		16%					
Jeugd en Cybersafety (10- tot en met 18-jarigen)												
Zelfgerapporteerd slachtofferschap aankoopfraude				5,2%								
Textmining politieregistraties (BVH)												
Aantal registraties online aan- en verkoopfraude									33.899			
Percentage registraties online aan- en verkoopfraude van totaal									0,9%			
Monitor Zelfgerapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd slachtofferschap online aan- en verkoopfraude												
10- en 11-jarigen								4,5%				
12- tot en met 17-jarigen								5,1%				
18- tot en met 22-jarigen								9,1%				

Tabel 10 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit overige vormen online fraude

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Domenie et al. (2013)												
Zelfgerapporteerd slachtofferschap voorschotfraude				0,2%								
Percentage slachtoffers die aangifte hebben gedaan				5,6%								
CBS Digitale veiligheid & criminaliteit												
Zelfgerapporteerd slachtofferschap nepboete/nepfactuur/nepactie											0,3%	
Percentage slachtoffers die aangifte hebben gedaan nepboete/nepfactuur/nepactie											23,8%	
Zelfgerapporteerd slachtofferschap microsoftscam											0,2%	
Zelfgerapporteerd slachtofferschap wangirifraude											0,5%	
Percentage slachtoffers die aangifte hebben gedaan wangirifraude											2,0%	
Eurobarometer												
Zelfgerapporteerd slachtofferschap cyberafpersing							10%					
Zelfgerapporteerd slachtofferschap poging tot oplichting via telefoon of e-mail					54%		59%					
Jeugd en Cybersafety (10- tot en met 18-jarigen)												
Zelfgerapporteerd slachtofferschap virtuele diefstal				15,3%								

Box 2 Geleden schade

Naast de omvang van aanvallen of slachtoffers zijn de maatschappelijke gevolgen van cyber- en gedigitaliseerde criminaliteit in geleden schade uit te drukken. Op basis van een studie door McAfee blijkt dat de kosten van cyberactiviteit wereldwijd gemiddeld 0,8% van het bruto binnenlands product (BBP) bedragen (Gehem, Usanov, Frinking & Rademaker, 2015). De geleden schade in Nederland wordt relatief hooggeschat met bijna 2% BPP. De methodologie achter deze gegevens is echter onduidelijk.

Geleden schade wordt ook gerapporteerd door de Nederlandse Vereniging van Banken (NVB, 2016; 2017; 2018; 2019). Aangezien niet alle gegevens van de NVB zijn terug te vinden online, zijn we deels afhankelijk van cijfers gerapporteerd in andere onderzoeken. De geleden schade door fraude bij bankieren neemt aan het begin van dit decennium sterk toe van 2,1 miljoen euro in 2008 tot 33,3 miljoen euro in 2013 (zie tabel 11). De afgelopen jaren is de jaarlijkse schade afgenomen tot 12,6 miljoen euro in 2018.

Deze schade is bovendien uit te splitsen naar typen van online fraude. De schade door phishing was tussen 2013 en 2018 jaarlijks tussen de 1,1-4,7 miljoen euro en is in 2019 gestegen naar 7,9 miljoen euro. De schade door skimmen, een vorm van bankpasfraude, is tussen 2008 en 2011 jaarlijks rond de 30 miljoen euro. Dit is lager dan de schade die PwC (2013) rapporteert: 118 miljoen euro. Deze schatting is gebaseerd op basis van de zelfgerapporteerde geleden schade door slachtoffers van skimmen.

De geleden schade is niet alleen op landelijk niveau, maar ook individueel niveau uit te drukken. Aan slachtoffers van bankfraude en online aankoopfraude is in het LISS-panel gevraagd naar financiële schade (Sipma & Van Leijsen, 2019). Slachtoffers bij wie onterecht geld van hun rekening werd geschreven krijgen in bijna 82% van de gevallen financiële compensatie van hun bank. De mediaan van de geleden schade is € 33,50 (range: € 1 tot € 1.250) in 2010 en is € 99 (range: € 1 tot € 1.500) in 2018.

Gegevens van het CBS (2019b) suggereren een soortgelijk beeld: 78% van de bankfraudeslachtoffers krijgt in 2018 de schade helemaal vergoed. Slachtoffers van online aankoopfraude krijgen in ruim 30% van de gevallen hun geld terug (Sipma & Van Leijsen, 2019). De mediaan van de geleden schade is € 30 en de maximale geleden schade is € 6.000. Het percentage slachtoffers van aankoopfraude dat in onderzoek van het CBS (2019b) schade vergoed krijgt is 10%. Onder slachtoffers van aan- en/of verkoopfraude in Domenie et al. (2013) heeft ruim 85% schade opgelopen. Het schadebedrag bedraagt in ruim 74% van de gevallen tussen de 1 en 100 euro.

Van slachtoffers van identiteitsfraude ondervindt ruim 60% financiële schade. Het schadebedrag ligt over het algemeen hoger dan bij aan- of verkoopfraude: in bijna 58% is de schade € 501 of meer (Domenie et al., 2013). Slachtoffers van nepboetes en wangirifraude worden in 2018 in respectievelijk ruim 12% en 4% helemaal gecompenseerd voor geleden schade (CBS, 2019b).

Tabel 11 Omvangcijfers slachtofferschap cyber- en gedigitaliseerde criminaliteit geleden schade in miljoenen euro's

	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17	'18	'19
Skimmen (PWC)												
Skimmen					118							
Nederlandse Vereniging van Banken (NVB)												
Fraude betalingsverkeer					81,8	33,3	17,3	17,9	10,2	12,9	12,6	
Fraude internetbankieren	2,1	1,9	9,8	35	34,8			3,7	0,8		3,9	
Phishing						4,7	3,9		1,1	3,8	3,8	7,9
Skimmen	31	36	19,7	38,9	29							

2.8 Discussie

In dit hoofdstuk is gekeken naar de aard en omvang van slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland (daderschap wordt in hoofdstuk 4 behandeld). Hierbij zijn diverse bronnen bekeken, zoals (academische) literatuur, slachtofferenquêtes en registratiesystemen. In de komende paragraaf worden de bevindingen met betrekking tot slachtofferschap in samenhang beschreven en bediscussieerd.

Er is relatief veel bekend over Nederlands slachtofferschap van cyber- en gedigitaliseerde criminaliteit. Zo zijn vanaf 2008 tweejaarlijks Nederlanders bevraagd via het LISS-panel over diverse vormen van slachtofferschap en via de CBS Veiligheidsmonitor is jaarlijks tussen 2012 en 2017 en vanaf 2017 tweejaarlijks slachtofferschap in kaart gebracht. Deze twee longitudinale bronnen suggereren dat 8-15% van de Nederlanders (in het jaar voorafgaand aan bevraging) slachtoffer is geweest van cyber- en/of gedigitaliseerde criminaliteit. Door de tijd lijkt er enigszins sprake te zijn van een daling in beide bronnen, hoewel deze minder sterk waar te nemen is binnen de CBS Veiligheidsmonitor. Een mogelijke verklaring is dat de CBS Veiligheidsmonitor slachtofferschap van computervirussen niet bevraagd, terwijl de omvang van deze vorm van slachtofferschap in het LISS-panel juist sterk is gedaald (van 14% naar bijna 2%).

Niet iedere vorm van cyber- of gedigitaliseerde criminaliteit maakt evenveel slachtoffers. Ook laat niet iedere vorm dezelfde ontwikkelingen zien. Het type delict dat rond 2008 de meeste slachtoffers lijkt te maken is malware. De daadwerkelijk omvang zou bovendien nog hoger kunnen liggen, omdat slachtoffers niet altijd in staat zijn om malware infecties te herkennen. Dit moet dan opgemerkt worden door een antivirusprogramma (Holt, Van Wilsem, Van de Weijer & Leukfeldt, 2020). Het aantal besmettingen lijkt echter door de tijd heen te zijn afgenomen. Een verklaring voor deze daling kan komen door betere (ingebouwde) bescherming tegen malware in computers en smartphones. Ook kan toenemend bewustzijn rondom de gevaren van malware bij Nederlandse gebruikers een rol spelen. Effectieve bescherming en bewustwording zou zich kunnen vertalen in de afname van het aantal besmettingen. Het is namelijk niet zo dat er minder aanvallen zijn met malware. Verder vraagt het LISS-panel naar besmettingen met computervirussen—een begrip dat misschien wat verouderd is. Wanneer specifiek naar malware gevraagd zou worden, zou het aantal gerapporteerde besmettingen en trends anders kunnen liggen, omdat dergelijke termen beter aansluiten op de hedendaagse beleving van hoe computers besmet raken. Ook is het wel of niet includeren van geleden schade in de vraagstelling belangrijk. Als gevraagd wordt naar slachtofferschap van computervirussen die

schade hebben veroorzaakt ligt het omvangpercentage lager dan wanneer die niet het geval is.

Onder jeugdigen bevraagd via de MZJ (Van der Laan & Beerthuizen, 2016) lijkt slachtofferschap van malware besmettingen vele malen hoger te liggen dan in de algemene populatie (iets wat ook buiten Nederland gevonden wordt; Oksanen & Keini, 2013). Een verklaring zou zijn dat gebrekkige impulscontrole bijdraagt aan risicovol onlinegedrag, iets wat beide meer voorkomt bij jongeren, wat de kans op besmettingen weer vergroot. Ook zijn jongeren vaker online dan ouderen, wat de kans op slachtofferschap ook vergroot. Een nog andere verklaring zou zijn dat jongeren meer kennis van en betrokkenheid bij technologische ontwikkelingen hebben en sneller inzien wanneer zij besmet zijn met een virus of malware, in vergelijking met een oudere leeftijdsgroep. Dan zou niet zozeer het objectieve slachtofferschap binnen deze groep hoger liggen, maar door een beter bewustzijn rapporteren zij wel vaker slachtoffer te zijn.

Slachtofferschap van hacken ligt lager dan die van malware. In tegenstelling tot malware zou het kunnen dat hacken misschien meer inspanning vereist van een dader en lastiger is om op grote schaal toe te passen. Malware daarentegen kan 'een eigen leven gaan leiden' zonder dat dit directe inspanning van een dader vereist. Dit vergroot mogelijk de kans op grootschaliger slachtofferschap. Net als bij malware wordt een hack niet altijd opgemerkt door slachtoffers. Slachtoffers weten bijvoorbeeld alleen dat zij slachtoffer zijn geworden, wanneer er openlijke schade is door een hack of wanneer zij op een andere manier geïnformeerd worden. Slachtofferschap van hacken laat door de tijd heen ook een dalende ontwikkeling zien.

Identiteitsfraude lijkt een relatief kleine groep slachtoffers te maken. Desalniettemin is het van belang om zicht te blijven houden op de omvang van dit delict, omdat identiteitsfraude grote gevolgen kan hebben voor slachtoffers. Vanwege deze beperkte omvang moet ook worden nagedacht of andere onderzoeksmethoden gebruikt dienen te worden in plaats van grootschalig surveyonderzoek. De omvang van andere vormen van online fraude, zoals bankfraude, zijn in de onderzochte periode licht gedaald.

Het delict waar in tegenstelling tot de algemeen stabiele of dalende ontwikkelingen een sterke groei te zien is, is online aan- en verkoopfraude. Zowel de CBS Veiligheidsmonitor (van bijna 3% in 2012 naar bijna 5% in 2019) als het LISS-panel (van ruim 2% in 2008 naar ruim 4% in 2018) laten een stijging in het percentage slachtoffers zien. Dit is op zich niet verwonderlijk, aangezien het gebruik van online winkelen en handel ook is toegenomen, wat meer gelegenheid creëert voor dergelijke fraude (zie bijv., Brady, Randa & Reyns, 2016). Een andere vorm van toenemende cyber- of gedigitaliseerde criminaliteit zijn DDoS-aanvallen, mogelijk door een toename in de manieren om DDoS-aanvallen uit te voeren (zoals via Internet of Things [IoT] apparaten), evenals het steeds makkelijker worden om dergelijke aanvallen uit te (laten) voeren (bijv., via cybercrime-as-a-service; Karami et al., 2016; zie ook hoofdstuk 5).

Slachtofferschap van online bedreiging en cyberpesten is de afgelopen jaren relatief stabiel gebleven. Een verklaring voor deze stabiliteit, terwijl andere gedragingen wel een groei of krimp laten zien, is dat deze twee vormen van gedrag persoonlijker zijn. Anders gezegd, er is meestal een interpersoonlijke reden of motivatie waarom iemand bedreigd of gepest wordt. Dergelijke motivatie is veel minder afhankelijk

van of wordt minder beïnvloed door allerlei technologische of maatschappelijke ontwikkelingen. Daarnaast zijn er al relatief lang kanalen beschikbaar waar online gedreigd of gepest via kan worden. E-mail, SMS, en chatprogramma's gaan al terug tot de 20e eeuw. Het zou daarom kunnen dat de initiële opkomst en groei van online bedreiging en cyberpesten heeft plaatsgevonden voor 2008 (d.w.z., het eerste jaar van observatie in dit onderzoek).

Veel informatie over slachtofferschap zijn gebaseerd op enquêtes onder slachtoffers. Deze enquêtes hebben een aantal voordelen ten opzichte van andere methoden. Zo wordt inzicht verkregen in criminaliteit die niet (noodzakelijk) bij de politie terecht komt. Aangezien uit de Veiligheidsmonitor blijkt dat minder dan 10% van slachtoffers aangifte doet, geven slachtofferenquêtes waarschijnlijk een completer beeld van de omvang van cyber- en gedigitaliseerde criminaliteit dan registraties van meldingen en aangiftes bij de politie. Dit is dan ook meteen de meest voor de hand liggende verklaring voor de discrepantie tussen justitiële cijfers van cyber- en gedigitaliseerde criminaliteit en slachtofferschap.

Een nadeel van slachtoffers vragen naar hun ervaringen is dat respondenten bepaalde gebeurtenissen niet altijd als criminaliteit herkennen (Bernaards, Monsma & Zinn, 2012), gebeurtenissen niet herinneren of eerder of later in de tijd plaatsen (Lamet & Wittebrood, 2009). Bovendien is het bepalend welke vraagstelling wordt gebruikt. Dit blijkt bijvoorbeeld uit de sterke verschillen in omvangcijfers met betrekking tot malware en wel of niet schade te hebben ondervonden.

De bronnen geven relatief weinig informatie over de aard van de delicten waarvan men slachtoffer is geworden. Een algemene beschrijving van gedrag in het item van de vragenlijst is vaak hetgeen waarop de aard bepaald dient te worden. Soms wordt doorgevraagd naar specifieke vormen van het delict, de ervaren ernst en/of de geleden schade. Veel diepgang ontbreekt (vooralsnog), wat zich reflecteert in gebrekkige kennis over specifieke cyber- en gedigitaliseerde criminaliteit (zoals ransomware en andere nieuwere vormen van dergelijke criminaliteit).

Samenvattend, over de omvang slachtofferschap van cyber- en gedigitaliseerde criminaliteit is relatief veel bekend op basis van voornamelijk slachtofferenquêtes. Wel ontbreekt diepgang wanneer het de aard betreft van slachtofferschap, zoals frequentie of ernst (in termen van schade, zowel financieel als psychologisch). Daarnaast bieden beschikbare politieregistraties vooralsnog geen of weinig inzicht in de longitudinale ontwikkeling van meldingen door slachtoffers van cyber- en gedigitaliseerde criminaliteit (naar specifiek type delict). Het is daarom aan te raden te kijken naar welke andere methoden verdere inzichten kunnen geven in de aard en omvang van slachtofferschap van cyber- en gedigitaliseerde criminaliteit. Naast enquêtes onder slachtoffers, zou ook gekeken kunnen worden naar meer officiële registraties van aantallen slachtoffers, of meer verdiepende interviews gehouden kunnen worden binnen slachtofferpopulaties.

3 Online bedreigingen in het lokaal bestuur

Auteurs[4]: *Max Boiten (Universiteit Utrecht), Maica Hopstaken (Fontys Hogeschool Tilburg), Marjolein Krijgsman (UU), Roelof Muis (Nationale Politie), Peter Mullaart (NP), Sander Prins (UU), Mirko Tobias Schäfer (UU) en Joris Veerbeek (UU)*

Samenvatting

Online kanalen zoals Facebook en Twitter bieden een laagdrempelige manier voor communicatie en het delen van meningen en informatie. Deze media kunnen echter ook gebruikt worden om bedreigingen te uiten. Onderzoek toont aan dat burgemeesters te maken hebben met een groeiend aantal bedreigingen, agressie en geweld. In dit onderzoek zetten we een eerste stap om de aanleidingen, de omvang en de verschijningsvormen van online dreigementen in kaart te brengen. De aanleidingen van bedreigingen jegens burgemeesters onderzoeken we aan de hand van een analyse van berichten in Nederlandse kranten. Ons onderzoek constateert met name drie contexten waarin bedreigingen geuit worden: (1) georganiseerde criminaliteit of motorbendes, (2) bedreigingen door burgers vanuit populistisch sentiment, en (3) bedreigingen door individuele burgers vanuit persoonlijke redenen. Op sociale media zijn daarbij met name indirecte bedreigingen uit de tweede categorie te ontdekken. Voor het in kaart brengen van de verschijningsvormen en de omvang exploreren we de mogelijkheden van automatische tekst-analyses op Twitterberichten aan burgemeesters. We vergelijken twee manieren om doodsbedreigingen automatisch op te sporen: (1) aan de hand van simpele zoektermen, en (2) aan de hand van *machine learning*. Hoewel de tweede methode subtielere vormen van bedreigingen bleek op te kunnen sporen, hebben we in dit onderzoek van de omvang van bedreigingen geen representatieve schatting kunnen maken. Onze analysemethode leverde slechts een beperkt aantal voorbeelden van concrete online bedreigingen op, en dat slechts beperkt op Twitter. Aan het slot van dit hoofdstuk suggereren we daarom dat een breed uitgezette enquête onder leden van het lokaal bestuur kan helpen meer inzicht in de problematiek en omvang van online bedreigingen te verkrijgen.

4 Dit onderzoek werd uitgevoerd door een team van onderzoekers van de Universiteit Utrecht en de Fontys Hogeschool Tilburg. Twee operationele specialisten van de Nationale Politie hebben advies gegeven op basis van hun expertise over bedreigingen en open source intelligence. Allen zijn in alfabetische volgorde opgenomen als auteurs van dit hoofdstuk.
Een overzicht van de taakverdeling geeft inzicht in de expertise en inspanning van de verschillende teamleden:
Dataverzameling: Max Boiten, Joris Veerbeek
Data-management: Sander Prins
Media-analyse (kranten): Max Boiten, Marjolein Krijgsman, Maica Hopstaken
Literatuuronderzoek: Marjolein Krijgsman, Peter Mullaart, Mirko Tobias Schäfer
Sociale media analyse: Max Boiten, Sander Prins, Joris Veerbeek
Tekstanalyse: Joris Veerbeek
Redactie: Sander Prins, Mirko Tobias Schäfer, Joris Veerbeek
Advies & domein-expertise bedreigingen & veiligheid: Roelof Muis, Peter Mullaart
Projectleiding: Mirko Tobias Schäfer

3.1 Introductie

In het hoofdstuk slachtofferschap zijn diverse vormen van cyber- en gedigitaliseerde criminaliteit aan bod gekomen. In dit hoofdstuk zal de aandacht uitgaan naar één specifieke vorm van gedigitaliseerde criminaliteit: online bedreigingen. Daarbij gaat de aandacht ook uit naar een specifieke populatie van slachtoffers, namelijk burgemeesters van Nederlandse gemeenten. Burgemeesters hebben te maken met bedreigingen als het aankomt op controversiële besluiten (opvang asielzoekers, handhaving openbare orde, enz.) en vanuit georganiseerde misdaad (plaatselijke hennepteelt, motorclubs). Onderzoek toont aan dat bijna een kwart (24%) van de 225 ondervraagde burgemeesters de afgelopen vijf jaar met een crimineel oogmerk is bedreigd, waarvan een meerderheid (62%) meerdere keren is bedreigd (Rijksoverheid, 2017, p. 21-22). Voor burgemeesters van grote steden van meer dan honderdduizend inwoners geldt zelfs dat 46% met een crimineel oogmerk is bedreigd (Rijksoverheid, 2017, p. 22). Het meest recente rapport Monitor Integriteit en Veiligheid spreekt van een continue stijging van ambtsdragers die aangeven te maken te hebben met agressie en geweld sinds 2014 (BZK, 2020). Ook in de media is er aandacht voor deze problematiek: kranten hebben in de afgelopen jaren regelmatig aandacht besteed aan bedreigingen jegens burgemeesters. Een aantal voorbeelden van deze berichtgeving zijn bedreigingen (waaronder direct aan huis) jegens de Haarlemse burgemeester Jos Wienen in 2018 met georganiseerde misdaad als vermoedelijke aanleiding, en de regelmatige bedreigingen aan het adres van de Rotterdamse burgemeester Ahmed Aboutaleb, zowel online als offline (Lammers & Edelenbosch, 2019; Binnenlands Bestuur, 2018).

Verschillende onderzoeken wijzen op de mogelijke rol van sociale media – en dan in het bijzonder van Twitter – in het faciliteren van deze bedreigingen (Bennhold & Eddy, 2020; Erhardt, 2020; Rijksoverheid, 2017). Door de laagdrempelige manier van communiceren op sociale media zou het voor burgers makkelijker zijn om frustraties en bedreigingen te uiten. Maar, zoals in het onderzoek naar de criminele beïnvloeding van het lokale openbaar bestuur terecht wordt gesteld: 'ook bedreigingen die hier worden gedaan worden als intimiderend ervaren en ze hebben veel impact op betrokkenen' (Rijksoverheid, 2017). Mogelijke gevolgen van online bedreigingen zijn de ondermijning van het openbaar gezag en de rechtsorde. In Duitsland, waar burgemeesters volgens onderzoek kampen met een 'golf van haat' op sociale media en andere kanalen, hebben burgemeesters vanwege bedreigingen van een nieuwe termijn afgezien (Bennhold & Eddy, 2020; Erhardt, 2020). Ook in Nederland is een flinke toename van verbale agressie geconstateerd, die ook via sociale media plaatsvindt (BZK, 2020).

In dit onderzoek brengen wij bedreigingen jegens burgemeesters op exploratieve wijze in kaart. Dit doen we om een inschatting te maken over de aanleidingen, verschijningsvormen, en de omvang van dreigingen die via online kanalen leden van het lokaal bestuur kunnen bereiken. Online kanalen vormen niet alleen een laagdrempelige manier van contact op te nemen met ambtsdragers, maar bieden ook de mogelijkheid om anoniem berichten te versturen. Een mogelijk effect hiervan zou een toename van bedreigingen via dergelijke wegen kunnen zijn. Met oog op het toenemende verhitte online debat omtrent populistische thema's, is het daarbij ook interessant om te kijken of deze debatten ook te relateren zijn aan bedreigingen jegens lokale ambtsdragers. We zien dit onderzoek vooral als een eerste opstap naar een brede inventarisatie van frequentie en de aard van online bedreigingen.

We concentreren ons in dit onderzoek daarbij op een tweetal analyses. Ten eerste onderzoeken we, primair om zicht te krijgen op de aanleiding en de context van online bedreigingen, hoe vaak en op welke manier Nederlandse kranten berichten over bedreigingen jegens burgemeesters. Vanuit dit contextueel kader gaan we, ten tweede, met behulp van een kwantitatieve en kwalitatieve tekstanalyse op zoek naar concrete bedreigingen op sociale media, waarbij onze focus ligt op het platform Twitter. Het doel van deze sociale media-analyse is tweeledig: de gevonden bedreigingen vormen voor ons niet alleen aanleiding om te reflecteren op de omvang en verschijningsvormen van online bedreigingen, maar ook op de mogelijkheid deze bedreigingen met automatische tekstanalyses op te sporen. We vergelijken daarbij twee manieren van automatische detectie: (1) het gebruik van een lijst met relevante zoektermen, en (2) het opsporen van bedreigingen aan de hand van algoritmes.

Bedreigingen kunnen zowel digitaal of op 'traditionele' manieren of omgevingen plaatsvinden. Uit onderzoek van Van Wilsem (2010) blijkt dat dit vaak in combinatie plaatsvindt. In deze gevallen kan er bijvoorbeeld sprake zijn van 'een verwevenheid tussen de digitale en 'fysieke' wereld' waarbij de 'voedingsbodem' van een conflict ontstaan kan zijn in een online omgeving en zich verder uitbreiden naar bedreigingen in de fysieke wereld. Andersom is dit uiteraard ook mogelijk, waarbij 'offline' bedreigingen zich uitbreiden of verplaatsen naar digitale omgevingen of middelen.' (Van Wilsem, 2010, p. 74).

Een bedreiging wordt gedefinieerd door Domenie et al. (2013) als 'het dreigen met —in de meeste gevallen—fysiek geweld of de dood tegen een persoon of zijn/haar eigendommen' (p. 28). Volgens deze definitie kan een bedreiging slechts herkend worden wanneer er sprake is van een voornamelijk expliciete dreiging. Formuleringen die niet expliciet dreigen 'met geweld, met verkrachting, met feitelijke aanranding van de eerbaarheid, met enig misdrijf tegen het leven gericht, met gijzeling, met zware mishandeling of met brandstichting' (zoals genoemd in art. 285 wetboek van strafrecht), zijn moeilijk als bedreiging te herkennen.

3.2 Methode

In dit onderzoek worden, een tweetal analyses exploratief ingezet. Deze analyses hebben uitsluitend het doel de context van het onderzoek te categoriseren. Het gaat hierbij om (1) een media-analyse van bedreigingsincidenten vanaf 2013 vanuit Nederlandse kranten en om (2) een sociale media-analyse van de tijdlijnen van alle Nederlandse burgemeesters met een Twitter-account. Voor de media-analyse zijn krantenartikelen geraadpleegd via de academische krantenbank LexisNexis, en voor de sociale media-analyse maken we gebruik van een steekproef van Twitterberichten afkomstig van online media monitoring solution OBI4wan. In wat volgt gaan we voor beide analyses nader op de dataverzameling en de analysemethode in.

3.2.1 Media-analyse

Voor de media-analyse is er met behulp van de databank LexisNexis een inventarisatie gemaakt van krantenberichten over bedreigingen jegens burgemeesters. Deze exploratieve gelegenheidssteekproef is uitsluitend ingezet als verkennend onderzoek om een helder beeld te krijgen van de context en categorisering van bedreigingen jegens burgemeesters en wethouders. De volgende analyse wordt niet ingezet om een beeld te geven van de frequentie dan wel omvang van de dreigingen, maar is

slechts bedoeld om houvast te geven aan het indelen van verdere onderzoeksresultaten en de beschrijving en context van het fenomeen 'bedreigingen jegens burgemeesters en wethouders'. Door analyses uit te voeren op de gevonden resultaten worden de verschillende verschijningsvormen van dreiging helder en kunnen aannames over deze verschijningsvormen worden geverifieerd. Labelling bestaat uit, maar beperkt zich niet tot: aard van de dreiging, online of offline dreiging, gevolgen van de dreiging en vorm van agressie die gebruikt is om de dreiging te uiten.
Er is een enkelvoudige steekproef uitgevoerd uit de verzamelde dataset via LexisNexis voor berichten van alle landelijke en regionale kranten, zowel fysiek als online, in de periode van 1 januari 2013 tot en met 16 maart 2020 waarin de zoekterm 'burgemeester bedreigd' in terugkomt. In deze query zijn dubbele resultaten gegroepeerd en zijn de resultaten gesorteerd op relevantie, om zo een dataset te creëren die een overzicht biedt van incidenten verspreid over verschillende jaren.

De artikelen die zijn gekozen om te analyseren in deze exploratieve steekproef voldoen aan (1) unieke inhoud (het incident is niet eerder te zien in de query) en (2) een titel waarin het onderwerp van dit onderzoek terugkomt. Ten gevolge van deze criteria zijn de eerste 35 berichten uit 5.221 resultaten meegenomen. Na deze eerste 35 resultaten neemt de relevantie van de resultaten sterk af en komen dubbelingen voor. Een voorbeeld van een resultaat dat niet werd meegenomen in de steekproef is het bericht 'Bedreigd door ex-burgemeester' van Tubantia (2018). De kop toont aan dat het hier niet gaat om een bedreigde burgemeester, maar om een burgemeester die zélf de dreigende is. De steekproef leverde in totaal 30 incidenten op waarbij er sprake was van een bedreiging, de overige vijf bleken niet te voldoen aan de definitie bedreiging jegens een burgemeester.[5]

3.2.2 Sociale media-analyse

Bij de sociale media-analyse wordt gebruikgemaakt van een steekproef van ca. 310.000 tweets die Nederlandse burgemeesters noemen of retweeten. De tweets betreffen de periode 1 januari 2019 tot en met 20 januari 2020 en noemen een burgemeester direct (zogenoemde @-mentions, ca. 155.000 tweets), retweeten tweets van één van de 274 burgemeester-accounts (ca. 155.000) of zijn retweets die een burgemeester-account noemen.[6] Deze data zijn middels een zoekquery, bestaande uit de Twitter-handles van de burgemeester-accounts, verkregen via OBI4wan. De sample van 310.000 tweets beslaat alle tweets die er via OBI4wan te vinden waren, en biedt dus een min of meer compleet beeld van alle publieke tweets aan en over Nederlandse burgemeesters.

5 Bij de overige vijf berichten was er sprake van een misverstand, verbale agressie die niet specifiek gericht was aan een burgemeester, of was de informatie uit het geselecteerde bericht ontoereikend om al dan niet te classificeren als bedreiging. Deze vijf berichten zijn niet meegenomen in de latere analyses over aard en aanleiding van bedreigingen jegens burgemeesters.

6 Voor de verdere analyse werden uit de 310.000 tweets degene die door Sybrand van Haersma Buma verstuurd zijn of hem noemen verwijderd (20%). Van Haersma Buma was eerder geen burgemeester maar lid van de Tweede Kamer. 20% van alle tweets verwijzen naar hem, maar dit wijkt af van ons onderwerp (bedreigingen jegens lokale ambtsdragers). Sybrand van Haersma Buma is aangesteld als burgemeester van Leeuwarden op 26 augustus 2019. Dit betekent dat hij slechts vier maanden als lokaal ambtsdrager in onze dataset aanwezig is. Daarbij is het zeer waarschijnlijk dat @-mentions en retweets t.a.v. Buma grotendeels zijn rol als politicus in de Tweede Kamer betreffen. Om die reden hebben wij ervoor gekozen tweets over en door Buma te filteren uit onze dataset.

We vergelijken twee manieren om doodsbedreigingen in onze dataset van tweets op te sporen. Ten eerste maken we gebruik van een simpele zoekopdracht, waarbij we alle tweets opsporen die het woord 'dood' (of varianten daarop) bevatten. Deze simpele baseline-methode levert veel ruis—in de vorm van vals positieven—op, hetgeen voor ons aanleiding geeft te reflecteren op de complexiteit van het opsporen van doodsbedreigingen. Ten tweede maken we gebruik van een algoritme om doodsbedreigingen op te sporen. Meer specifiek zetten we een recent ontwikkeld neuraal taalmodel (het zogeheten BERT-model) in om doodsbedreigingen in tweets te classificeren. Hiervoor hebben we een dataset samengesteld circa 3.000 dreigende tweets die—in navolging van Spitters et al. (2014)—afkomstig zijn van het Twitter-account @doodsbedreiging (verzameld via de Twitter-API). Deze dataset hebben we aangevuld met circa 30.000 tweets uit de steekproef van berichten aan burgemeesters. Alle mediumspecifieke informatie (informatie over een mention, een retweet, een quote, enz.) zijn uit de tweets verwijderd. We gebruiken een voor-getraind Nederlands taalmodel met de BERT-architectuur (De Vries et al., 2014) om dreigende tweets te laten onderscheiden van niet-dreigende tweets. Met 3.000 dreigende tweets moet het model een gevarieerde indruk krijgen van de manier waarop dreigende tweets zich in de praktijk voordoen. Het getrainde model zetten we vervolgens in op onze steekproef van tweets aan burgemeesters.

In wat volgt gaan wij nader op de resultaten in. Daarbij bespreken we eerst de resultaten van de media-analyse, en vervolgens de resultaten van de sociale media-analyses.

3.3 Resultaten

3.3.1 Resultaten media-analyse

Uit de analyse van incidenten benoemd in de krantenartikelen blijkt dat er drie vormen bedreigingen kunnen worden onderscheiden: bedreigingen jegens ambtsdragers vanuit georganiseerde criminaliteit of motorbendes, bedreigingen door burgers in samenhang met onpopulaire beslissingen, en enkele bedreigingen door individuele burgers vanuit een meer persoonlijk perspectief (zie figuur 2). Daarnaast zijn er enkele gevallen waar de vorm van bedreiging onduidelijk is. Uit de nageslagen artikelen over bedreigingen jegens burgemeesters is gebleken dat bij de meeste bedreigingen onduidelijk was of de bedreiging digitaal of niet-digitaal is geuit.[7] Opvallend is het aantal keer dat een 'verward' persoon de aanleiding is geweest van een bedreiging. Dit type aanleiding is in onze dataset vrijwel altijd te linken aan bedreigingen om persoonlijke redenen. In bijlage 3 tabel B3.3 en B3.4 wordt duidelijk hoe deze thema's en aanleidingen zijn herleid uit de artikelen.

Niet altijd zijn bedreigingen duidelijk te plaatsen in een van de drie genoemde thema's; deze zijn als 'onduidelijk' gekenmerkt. Dit omdat er vaak een nadere toelichting ontbreekt: de burgemeester wil of kan geen nadere toelichting over het incident doen in de media. De onduidelijkheid komt dan voort uit de onbekendheid met de aard en inhoud van de dreiging jegens de burgemeester, tenzij deze ter terechtzitting komt. Uit figuur 3 wordt daarnaast duidelijk dat in de meeste gevallen burgemeesters (extra) bewaking krijgen of dat zij moeten onderduiken

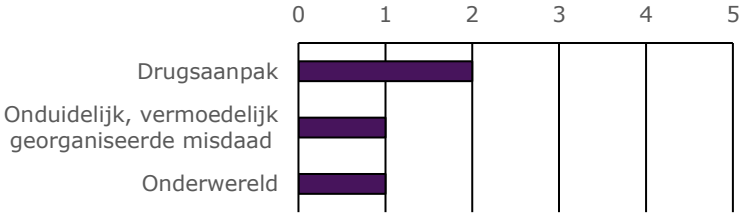
7 In onze beperkte steekproef zien we negen offline bedreigingen, zes online bedreigingen en bij tien gevallen is onduidelijk op welke manier de dreiging geuit werd.

na een bedreiging. De totstandkoming van deze labels rondom de gevolgen en getroffen maatregelen zijn te raadplegen in bijlage 3 tabel B3.4.

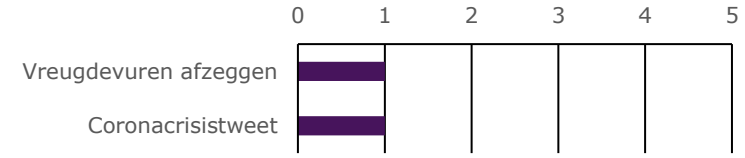
Uit de geanalyseerde krantenartikelen blijkt dat sommige omroepen of kranten een eigen onderzoek onder gemeentebesturen hebben uitgevoerd. Zo deed NH Nieuws een onderzoek waaruit bleek dat de meeste bedreigingen face-to-face of via sociale media gebeuren, en in mindere mate via e-mail (Lammers & Edelenbosch, 2019).

Figuur 2 Aanleidingen van incidenten onderverdeeld in de thema's

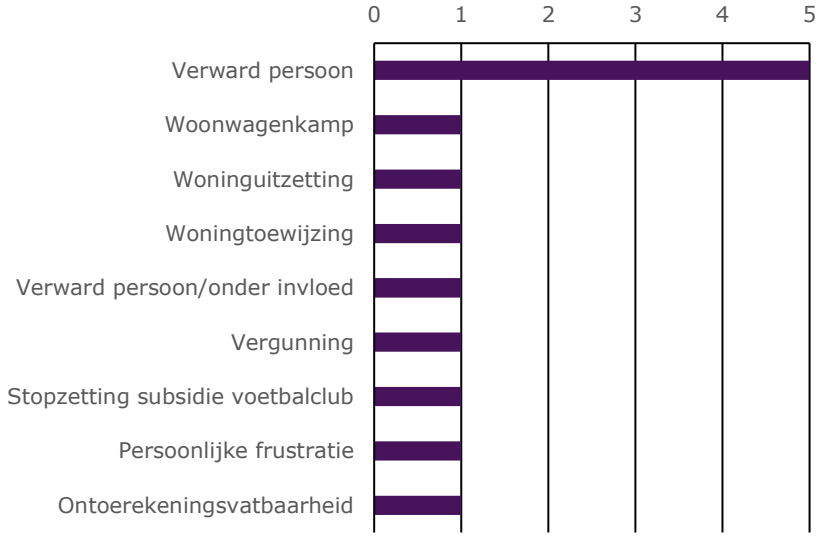
Aantal incidenten georganiseerde misdaad (N=4)



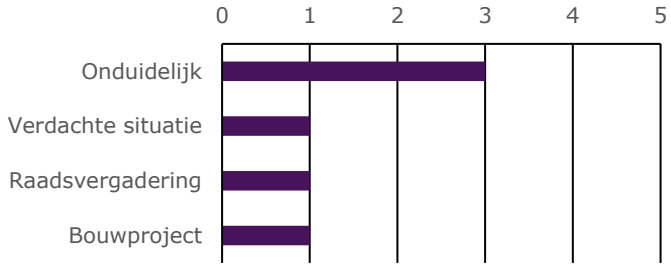
Aantal incidenten rondom maatschappelijk thema (N=2)



Aantal incidenten rondom persoonlijke redenen (N=13)

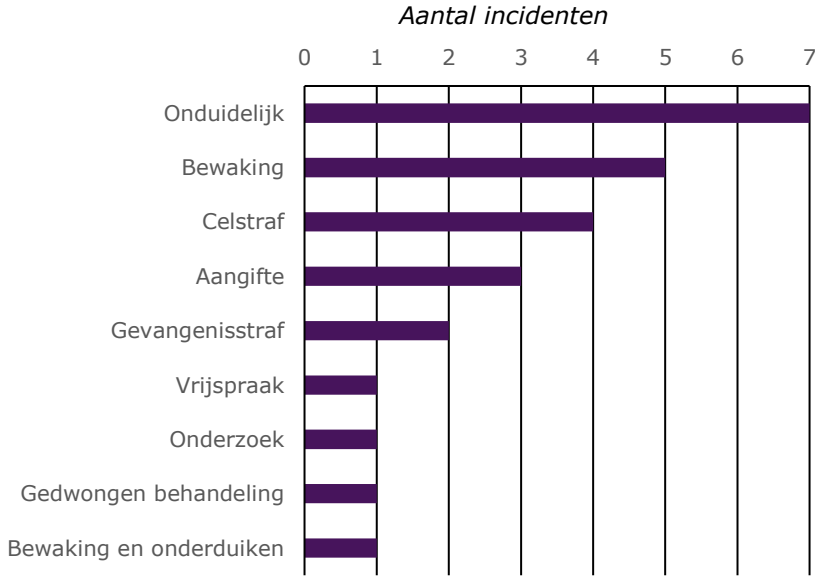


Aantal incidenten onduidelijk (N=6)



Andere dreigingen die in het persoonlijke thema passen hebben een motivatie die sterk lijkt op die van Henk K., zoals de dreiging aan het adres van de burgemeester van Vlaardingen Annemiek Jetten. De verdachte zou filmpjes op Facebook hebben geplaatst, waarin hij dreigde haar te gijzelen. Volgens de Arnhemmer zouden zij en de politie er verantwoordelijk voor zijn dat hij drie weken in een isoleercel heeft gezeten (Binnenlands Bestuur, 2019).

Figuur 3 Gevolgen en getroffen maatregelen naar aanleiding van de bedreiging(en)



De bovengenoemde krantenberichten geven al een blik op de soorten van offline en online bedreigingen. Waar het online bedreigingen betreft, wordt er in de artikelen gesproken over SMS, sociale media, en e-mail om bedreigingen te versturen. Opvallend daarbij is dat de bedreigingen uit de georganiseerde misdaad via SMS verstuurd werden. Bedreigingen in de context van controversieel beleid zijn vooral via sociale media te vinden. Uit bijlage 3 tabel B3.2 wordt duidelijk wat voor bedreigingen het label online en offline hebben gekregen.

3.3.2 Resultaten sociale media-analyse

Het opsporen van doodsbedreigingen aan de hand van zoektermen
De resultaten van de sociale media-analyse aan de hand van trefwoorden tonen aan dat een klein aantal doodsbedreigingen jegens burgemeesters te vinden zijn.

Het gaat dan bijvoorbeeld om berichten als: '@xxx ga dood' of '@xxx Wat jij moet doen is lekker dood gaan, vuile vieze hond. Lekker makkelijk reageren als je alleen de verhalen leest:'. Deze twee tweets spreken de betreffende personen direct aan, maar zijn geen directe doodsbedreiging. Het voorbeeld in figuur 4 laat zien dat het niet altijd makkelijk is om een directe bedreiging in de tekst te herkennen. Wettelijk is hier geen sprake van een doodsbedreiging. Het lijkt dus wel een ondermijnende uitspraak te zijn, maar niet noodzakelijk een strafbare.

Figuur 4 Voorbeeld met gebruik van het woord 'dood' in dreigende context

De hierboven geciteerde tweets zijn drie van 292 tweets waar het woord 'dood' in terugkomt. Uit deze drie voorbeelden blijkt al dat het moeilijk is in te schatten of het hier daadwerkelijk om een directe doodsbedreiging gaat. Het lijkt echter meer op het uiten van emoties. Het blijkt dat vrijwel alle tweets met een letterlijke doodsbedreiging of uitgesproken wens van tegenspoed voor ambtsdragers inmiddels van Twitter verwijderd zijn. We vermoeden dat of de bedreigde persoon zelf, dan wel een andere gebruiker de betreffende tweets bij Twitter heeft gerapporteerd, waarna deze vervolgens is verwijderd.

De overgrote meerderheid van de tweets gebruiken het woord 'dood' echter in een andere context; vaak gaat het om jagers die 'dieren doodschieten'. Drie veelvoorkomende thema's konden wij in onze steekproef onderscheiden:

1 Het doden van dieren, vooral in samenhang met jagers of jagen.
   a 'Wat een onnodig dierenleed dankzij dit soort prutsers. Na drie keer schieten (van dichtbij!) en twee keer slaan is de haas nóg niet dood. Kennelijk heb je weinig vaardigheden nodig om jezelf jager te noemen.'
   b 'Jagers gaan inderdaad het veld in omdat ze het leuk vinden om een dier dood te schieten. Wat is daar mis mee? Het is vanwege historie legaal. Je moet niet zeggen dat je jaagt omdat je de wildstand graag beheert. Jagen mits genoeg wild is niets mis mee.'

2 Het verwijt dat moslims ongelovigen willen doden.
   a 'Het is allemaal het gevolg van jarenlanks linksstemmend hersenloos volk. Nederland is dood. Hollandistan is een feit. QUOTE @xxx: @xxx @xxx Ja mag van de burgemeesters van #Nederland. Nederlanders verkrachten, vermoor-

den, neersteken, lastig vallen, uitschelden, bedreigen, stenen gooien, in elkaar trappen, lawaai maken, onderdrukken. Maar flyeren foei. @xxx @xxx'

b 'Dus Oemmah.. homohaat,jodenhaat, vrouwen onderdrukking en ongelovige dood is voor jouw geen probleem.. dus: over neonazi s gesproken! Pegida neemt daar stelling tegen wat is daar mis mee? QUOTE @xxx: Volgens de geweld verheerlijkende moslims van Oemmah, doet de @[gemeente xxx] @[burgemeester xxx] aan hun zelfs toezeggingen en beloond daarmee het moslimgeweld van 26.05.2018 tegen #Pegida en #Politie‼ Wanneer dit waar is, hebben ze in #xxx zeer binnenkort een enorm probleem https://t.co/xxx'

3 Dingen die dood zijn, zowel letterlijk als figuurlijk.

c '@xxx Ongelooflijk dat XXX niks wou organiseren. Nachtleven is al compleet dood hier. En er kan zelfs geen subsidie van af.... triest @[gemeente xxx] @xxx @xxx @xxx'

Alleen deze voorbeelden tonen al aan dat het op basis van de (deel)zinnen als 'dood maken' niet mogelijk is om onderscheid te maken tussen dreigende posts en 'normale' posts. Voor het herkennen van een werkelijke bedreiging hebben we een structuur nodig zoals een dader, een slachtoffer, een tijd of locatie en een actie (bijv., dood maken).

Maar zelfs wanneer we een dergelijke structuur zouden kunnen opsporen, zijn er ook berichten waarin de dreiging meer indirect van aard is, zoals in figuur 5. Het bericht representeert een afkeer jegens een ambtsdrager, maar er blijkt niet noodzakelijk uit het bericht dat de auteur ook van plan is om de dreiging waar te maken. Deze indirecte bedreigingen zijn vaak te vinden op sociale media, zoals Twitter en Facebook. Sommige formuleringen zijn dus eenvoudig, zoals 'val dood', maar wanneer de formuleringen complexer worden, zijn deze dus veel moeilijker als zodanig te identificeren. Daarbij kan ook de context en de relatie tussen de dreigende en de bedreigde persoon een betekenisvolle rol spelen. Bij een bedreiging in de vorm van 'wat ziet je kindje schatting uit' kan—in veel gevallen—alleen de bedreigde persoon bepalen dat het bericht daadwerkelijk een bedreiging is.

Figuur 5 Indirecte bedreiging in een Tweet

Machine learning

Bij het zoeken van de doodsbedreigingen en ondermijnende tweets aan de hand van een woordenlijst bleek de (tekstuele) context waarin de desbetreffende termen voorkomen van cruciaal belang. Louter zoeken op trefwoorden zoals 'dood' levert bijzonder veel ruis op, waarbij het overgrote merendeel niet als ondermijnend geclassificeerd kan worden. Een deel hiervan zou ondervangen kunnen worden door meer specifieke regels op te stellen. Een tweet zou dan alleen als doodsbedreiging tellen wanneer 'dood' wordt gebruikt met 'ik' of 'we' als onderwerp, en een persoon

als lijdend voorwerp. Dat is ook één van de strategieën die onderzoekers van de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO) hebben gebruikt in een poging doodsbedreigingen te classificeren (zie Spitters et al., 2014). Het opstellen van dergelijke regels is echter bijzonder tijdsintensief, en de opbrengst beperkt, omdat er altijd weer tweets zullen zijn die van dergelijke strikte patronen afwijken—niet in de laatste plaats omdat het taalgebruik op sociale media veelal afwijkt van formeel Nederlands taalgebruik.

Dat de betekenis van teksten afhankelijk is van de context, en talige fenomenen zich niet eenduidig laten ondervangen in strikte regels, is precies ook de reden dat computerwetenschappers die zich bezighouden met de automatische verwerking van taal zich in toenemende mate zijn gaan concentreren op het ontwikkelen van neurale taalmodellen die juist de contextuele afhankelijkheid van betekenis exploiteren. Dergelijke modellen worden getraind op miljarden teksten, waarbij de computer steeds woorden die zijn weggelaten in de tekst moet invullen. Naarmate het model meer teksten ziet, wordt het steeds beter in het voorspellen van deze woorden, en krijgt het dus steeds beter een beeld van de context waarin bepaalde woorden worden gebruikt. Omdat dergelijke modellen bij de verwerking van elk individueel woord ook alle andere woorden in de zin verdisconteren, zijn ze in theorie in staat om het woord 'steken' in de zin 'ik ga je steken' te onderscheiden van 'we hebben steken laten vallen'—zonder daarvoor expliciete regels voor te formuleren. Nadat een taalmodel is getraind op miljarden teksten, kan het gebruikt worden om allerlei talige taken uit te voeren, zoals het beantwoorden van vragen, het classificeren van sentiment, het herkennen van naamwoorden in een zin, enzovoorts. Daarvoor hoeft het model alleen nog voor beperkte tijd op een specifieke dataset getraind te worden. Dit proces noemt men het finetunen van een taalmodel.

Voor dit onderzoek hebben we, zoals we in de methode kort uiteen hebben gezet, een Nederlandstalig BERT-model gefinetuned op een dataset van doodsbedreigingen. Om de accuraatheid van ons model te testen, hebben we een deel van de dataset apart gehouden. De resultaten op deze testset suggereren dat neurale modellen veel potentie bieden voor het classificeren van dreigende tweets: van alle dreigende tweets die het model als zodanig heeft geïdentificeerd (precision), is 94% daadwerkelijk een dreigende tweet, en van alle dreigende tweets in de testset (recall), heeft het model 95% correct geïdentificeerd. Dat is, vergeleken met andere vergelijkbare pogingen om zinnen te classificeren, een bijzonder hoog resultaat. Daarbij lijkt het model zelfs in staat impliciete vormen van dreigementen correct te classificeren. Zo heeft het model het bericht 'bewaar die lag maar want het zal je laatste worden ... dikke kanker flikker je bent nog gladder dan glijmiddel' correct als dreigend geïdentificeerd—ondanks de (vele) spel- en grammaticafouten.

Tegelijkertijd moeten deze resultaten in zekere zin met argusogen worden bekeken, omdat onze dataset synthetisch—aan de hand van twee aparte datasets—is samengesteld, en niet het resultaat is van (semi-)handmatige labeling. Dat laatste is echter wel een cruciale voorwaarde voordat een model op grote schaal ingezet kan worden—anders weten we immers niet hoe accuraat het model op 'echte' data is.

Wanneer we het BERT-model vervolgens loslaten op de steekproef van tweets aan burgemeesters, wordt vooral het beeld bevestigd dat het aantal dreigende tweets in de steekproef beperkt is. Van alle 201.168 unieke berichten zijn er 'slechts' 880 berichten (0,41%) door het model als dreigend geclassificeerd. En van die 880 berichten lijkt, bij een handmatige inspectie, een evenzeer beperkt deel daadwerkelijk ondermijnend dan wel dreigend te zijn. tabel 12 toont de tweets die het BERT-

model met de grootste waarschijnlijkheid als dreigend heeft geclassificeerd. Enkele tweets zijn inderdaad dreigend, of in ieder geval ondermijnend, zoals het eerdergenoemde bericht 'ga dood', 'ga aub dood', en ook minder voorkomende varianten als 'de eerste de beste idioot die dat mijn kind aandoet, sla ik zijn/haar kop zacht' en 'ik hoop dat je familie uitsterft aan kanker'. Maar het merendeel is wellicht grof ('je kanker moeder', 'ik ga je aanklagen ratten'), maar niet zozeer dreigend of ondermijnend.

Tabel 12 De tweets die volgens het BERT-model met de grootste waarschijnlijkheid als dreigend heeft geclassificeerd

Tweet
je zal zo n vader hebben. Sybrand ga aub dood graf farizeeër.
Ik ga stuk hier [huilende smiley]
MIJN GOD KIJK DIE MALLOOT
man ga golfen
ga dood
Dat ha ik ekris fan hun krigen mar der wol no net in fugel mear yn
Ik ga stuk mannen!
op sterven na dood over jaar heeft je opgegeten
Ik ga jullie aanklagen ratten
Ik ga weer neuken ! vrouwen = maand per jaar in de krieg zitten!
HIER WORD IK ZOOOO BOOS VAN
als ik dood wil betaal ik dat graag zelf!
Je kanker moeder
zo ich habe das nicht gewust gaat voor u niet op
gaat klappen gaat klappen gaat klappen en weet wel wanneer hij weg gaat echt
WAAROM HOOR IK JULLIE NIET OVER DE GEVAREN VAN G? HEBBEN JULLIE GEEN KINDEREN? LEES DIT ARTIKEL!
hoor alleen maar ik ik ik ik ik ik ik man man
Leer eerst ff schieten en richten en ga dan pas op jacht
ga je deze agent net zo flowen als je bij jelle deed of laat je dit zomaa voorbij gaan
IK DOE ER EEN GROTE SCHEP STRONT BOVENOP !
Je kanker hoeremoeder kanker hoerezoon. Ik hoop dat je familie uitsterft aan kanker
JA EN ALS JE NU KIJK HOE DE WERELD IS VOL VAN HAAT DAN VREES IK HET ERGSTE
das nie helemaal waar maar nul op de straat ga ik met je mee.
Ik ga mijn ogen open houden
Die van mij gaat spontaan dood bij het zien van dat stuk vreten!!
Ik bel je mogge ff harrie
EMILE ROEMER wanneer gaan we stappen ouwe tijger haha weet je nog vroeger xx groeten daar he pik
o mijn god nou doe ik het weer dit is nou een echte hamas lover
JA GELUKKIG WERK IK NIET BIJ POLITIE R'DAM!
suc-6 met je de kogel kwam weer van !
neem je zn aansteker voor me mee
We leven blank gaan we omdraaien mijn honden mijn sigaretten enz.
Ik ga denk ik binnenkort op de kermis staan
De eerste de beste idioot die dat mijn kind aandoet, sla ik zijn/haar kop zacht

Daarmee laten de resultaten van dit experiment, aan de ene kant, zien dat neurale taalmodellen in staat zijn om subtielere en minder voorkomende varianten van bedreigende en ondermijnende berichten op te sporen, en (in potentie) veel beter werken dan simpele trefwoord analyses. Aan de andere kant moeten er nog behoorlijk wat stappen gezet worden vooraleer een dergelijk model daadwerkelijk ingezet kan worden, waarbij het grootste deel van het werk zit in de zorgvuldige samen-

stelling van een voldoende diverse set (be)dreigende en ondermijnende berichten die evenzeer representatief zijn voor de populatie, door middel van handmatige labeling.

3.4 Conclusie

Er is sprake van bedreigingen jegens burgemeesters en andere leden van het lokaal bestuur. Deze bedreigingen worden in toenemende mate via online kanalen geuit. In de kranten werd verslag gedaan van deze verschillende bedreigingen. In ons onderzoek maken we een onderscheid tussen drie verschillende contexten waarin bedreigingen worden geuit: (1) bedreigingen binnen een context van zware criminaliteit (georganiseerde misdaad, motorbendes, enz.), (2) het populistische sentiment, en (3) bedreigingen door individuele burgers gemotiveerd door hun persoonlijke omstandigheden.

De bedreigingen vanuit de zware criminaliteit en door individuele burgers vanuit persoonlijke redenen waren echter niet terug te zien in onze analyse van sociale media. Dat kan drie oorzaken hebben: (1) de bedreigingen waren door ons onderzoekers niet als dreiging te herkennen, (2) de dreigingen waren inmiddels verwijderd, (3) of sociale media blijken vanwege hun publieke kwaliteit geen geschikt medium voor directe bedreigingen. Voor leden van georganiseerd misdaad lijkt het ook contraproductief als hun dreiging jegens een ambtsdrager openbaar wordt; publieke kennis over de bedreiging beperkt de ambtsdrager in het naleven van de eisen van de criminelen, en dus kunnen criminelen vanuit deze redenering een voorkeur voor directe communicatiekanalen hebben, zoals SMS, e-mail, of messenger-diensten zoals WhatsApp. Maar bedreigingen kunnen ook op een manier geformuleerd zijn dat ze alleen voor de bedreigde persoon als bedreiging te herkennen zijn.

Uit de exploratieve analyse van Twitter komt een aantal voorbeelden van online bedreigingen jegens politici en ambtsdragers in het lokaal bestuur naar voren. Deze analyse is dan ook niet representatief, en kan niet meer leveren dan een exploratieve verkenning van een tot nu toe onvoldoende in kaart gebracht fenomeen. Het onderzoek kan dus geen sluitende informatie leveren over de omvang van het probleem rondom online bedreigingen jegens burgemeesters. Uit de analyse van kranten en sociale media blijkt dat online kanalen, zoals Twitter, wél gebruikt worden voor bedreigingen. Deze bedreigingen blijken zich meestal voor te doen in de context van populistisch sentiment. Dat betreft doorgaans emotionele reacties op gevoelige onderwerpen zoals de Zwarte Pieten-discussie, de komst van asielcentra en bijvoorbeeld het boerenprotest omtrent de stikstofproblematiek. Vooral de hashtag #boerenprotest op Twitter levert een reeks indirecte bedreigingen op die representatief zijn voor onze classificatie van dreigingen in de context van populistisch sentiment (zie exemplarisch figuur 6). Dreigingen in de context populistische acties zoals #boerenprotest treffen vermoedelijk vaker prominente politici, bijv. leden van de Tweede Kamer. Deze personen staan prominenter in het nationale politieke debat en worden met de maatregelen geïdentificeerd.

In dit onderzoek werd slechts gekeken naar een beperkte steekproef van sociale mediaberichten, enkel afkomstig van Twitter. Zelfs in het geval van toegang naar een grotere steekproef van Twitter of de mogelijkheid om Twitter in real-time te onderzoeken naar bedreigingen, bestaat er nog steeds een grote kans dat bedreigingen ofwel niet worden herkend, ofwel op Twitter niet aan te treffen zijn. Ook

zijn er nog andere populaire sociale media-platformen zoals Facebook, YouTube en Instagram. Uit het krantenonderzoek bleek een voorbeeld waar bedreigingen op een Facebookpagina geuit werden jegens lokale ambtsdragers. Naast de sociale media-platformen kunnen berichtendiensten, zoals WhatsApp, Telegram of Signal, gebruikt worden voor bedreigingen. En ook platformen zoals Reddit, 4chan en 8chan kregen recent media-aandacht omdat daders hun acties hier hebben aangekondigd. Deze voorbeelden hebben dan een terroristisch achtergrond, zoals de aanslag in Christchurch.

Figuur 6 Voorbeeld voor indirecte dreiging vanuit populistisch sentiment

We vergeleken in dit onderzoek twee manieren om doodsbedreigingen in Twitter op te sporen: aan de hand van simpele trefwoorden, en aan de hand van een algoritme. Een logische vervolgstap is om mogelijkheden voor automatische detectie te verkennen. Hoewel er slechts een zeer beperkt aantal bedreigende tweets in de dataset te vinden waren, bleek de inzet van het automatische BERT-model niet alleen minder ruis op te leveren, maar ook subtieler vormen van bedreigingen te kunnen herkennen. Bovendien staat automatische detectie toe om grotere hoeveelheden berichten langs te gaan. De winst hier is dat—mits goed gebouwd—dit het ook mogelijk maakt om verkennend te werken. De grootste uitdaging hiervoor is om een voldoende diverse set (be)dreigende en ondermijnende berichten te verzamelen om de modelkeuzes te informeren. Op die manier zouden we kunnen werken richting een model dat zelf nieuwe dreigende taal kan herkennen, en met input van de onderzoekers verder kan leren.

Meer inzicht in de frequentie en omvang van de problematiek kan worden vergaard door een breed uitgezette enquête onder leden van het lokaal bestuur. Op deze manier wordt getroffenen de mogelijkheid geboden hun ervaringen te delen en informatie te verstrekken over de aard van de bedreiging, het kanaal dat gebruikt werd om de bedreiging te sturen, de context waarin de bedreiging geuit werd en de reactie van de bedreigde ambtsdrager en haar organisatie.

Er is sprake van een groot aantal bedreigingen via sociale media. Bedreigingen kunnen via sociale media weliswaar gemakkelijk worden verstuurd, maar ze hebben een wel slopend effect: een ondermijning van lokaal gezag en een sluipende ontmoediging om het ambt verder uit te voeren. De drie verschillende categorieën die ons onderzoek identificeert vragen elk om een verschillende aanpak en de samenwerking met verschillende stakeholders vraagt om een maatschappelijk antwoord. De beroepsverenigingen en de politie moeten handelingsopties ontwikkelen om gepast op de bedreigingen te kunnen reageren. Sociale media-platformen zullen hun verantwoordelijkheid moeten nemen om bedreigingen snel te verwijderen. Maar ook de burger als gebruiker van sociale media zou dergelijk schofterig gedrag zelf moeten tegenspreken. De vijandelijke toon jegens volksvertegenwoordigers op sociale media is onaanvaardbaar en doet afbreuk aan het politieke debat in een open samenleving als de onze.

4 Daderschap van cyber- en gedigitaliseerde criminaliteit

Auteurs: *Take Sipma, Marinus Beerthuizen, Esther Meijer-van Leijsen en André van der Laan*

Belangrijkste bevindingen

Bronnen die inzicht geven in de omvang van Nederlands daderschap van cyber- en gedigitaliseerde criminaliteit zijn beperkt in aantal en inhoud. Daarnaast geven bronnen niet zozeer inzicht in aantallen of percentage daders binnen een populatie, maar betreffen ook geregistreerde misdrijven. In officiële statistieken wordt cybercriminaliteit vooral teruggebracht naar computervredebreuk. Gedigitaliseerde criminaliteit wordt in die statistieken ook als traditionele delicten geregistreerd, waardoor over dergelijk daderschap informatie ontbreekt.

Algemeen

Het aantal bekende verdachten of strafrechtelijke daders neemt door de tijd toe. Zo is het aantal verdachten van computervredebreuk volgens 1 bron van ruim 70 in 2008 gestegen naar bijna 430 in 2019. Deels kan deze stijging verklaard worden door hogere prioritering van cybercriminaliteit in de opsporing door de politie. Ook is in de periode 2008 tot en met 2018 het aantal strafzaken dat instroomde bij het OM betreffende cybercriminaliteit toegenomen van bijna 90 naar ruim 280, terwijl voor gedigitaliseerde criminaliteit een afname te constateren is van ruim 540 naar ruim 360. Voor strafzaken afgedaan door de rechter is een gelijke ontwikkeling te zien—van bijna 20 naar ruim 70 voor cybercriminaliteit en van bijna 370 naar ruim 170 voor gedigitaliseerde criminaliteit. Cijfers over zelfgerapporteerd daderschap onder de algehele Nederlandse bevolking ontbreken. Onder jongeren in de leeftijd 10 tot en met 22 jaar is de omvang van zelfgerapporteerd daderschap cyber- en gedigitaliseerde criminaliteit geschat tussen 8-26% in 2015.

Hacken en DDoS-aanvallen

De omvang van zelfgerapporteerd daderschap van diverse vormen van hacken onder Nederlandse jongeren bedraagt 1-18% in 2015 en 0,1-2% van de jongeren geeft aan zich schuldig te hebben gemaakt aan ten minste één DDoS-aanval.

Malware

Statistieken over daderschap van malware zijn relatief schaars. Onder jongeren is zelfgerapporteerd daderschap van het versturen van een virus 0,6-1% in 2015. Op basis van gegevens van antivirussoftware ontwikkelaars lijkt de omvang van (pogingen tot) het verspreiden van malware te zijn toegenomen.

Online bedreiging

In 2015 geeft 0-8% van jongeren aan zich schuldig te hebben gemaakt aan een vorm van online bedreiging of cyberpesten.

Online fraude

Het percentage van zelfgerapporteerd daderschap onder jongeren is 0-3% bij aan- en verkoopfraude, bijna 5% bij identiteitsfraude en ruim 10% bij virtuele diefstal.

4.1 Inleiding

Binnen de context van dit onderzoek zijn daders personen die cyber- of gedigitaliseerde criminaliteit (zeggen te) plegen (of daarvan verdacht worden). Naast het individuele aspect van daderschap komen ook de handelingen van daders (d.w.z., delicten en misdrijven) en de procedurele gevolgen (d.w.z., strafzaken) aan bod. Daderschap kan op verschillende manieren vastgesteld worden. Eén manier is via zelfrapportage, waarbij iemand zelf rapporteert dader te zijn van een delict. Ook kan iemand bij de politie een verdachte zijn van een cyber- of gedigitaliseerd delict en daarvoor door het OM vervolgd worden. Wanneer deze persoon schuldig wordt bevonden door de rechter (of officier van justitie) is er sprake van strafrechtelijk daderschap. Het werkelijke aantal daders zal echter (vermoedelijk) onbekend blijven. Net als bij slachtofferschap zullen verschillende manieren voor bepalen van daderschap tot verschillende schattingen van de omvang leiden in bronnen. Het is dus aannemelijk dat de bronnen die besproken worden ieder een ander beeld zullen schetsen van de aard en omvang van daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland. Zie voor een overzicht van de methodiek die gehanteerd wordt in dit hoofdstuk bijlage 2.

4.2 Cyber- en gedigitaliseerde criminaliteit in het algemeen

In de volgende paragraaf worden resultaten besproken die betrekking hebben op algemene cyber- en gedigitaliseerde criminaliteit. Hiermee wordt bedoeld dat er uitspraken worden gedaan over het collectief van gedragingen van cyber- en gedigitaliseerde criminaliteit, zonder uitsplitsingen naar specifieke vormen van gedragingen (zoals bijvoorbeeld DDoS-aanvallen of online bedreiging). Ook wordt hier cyber- en gedigitaliseerde criminaliteit besproken die door methodologische beperkingen niet uitgesplitst kan worden. Specifieke vormen worden in latere paragrafen besproken. Omdat in het hoofdstuk over slachtofferschap de specifieke gedragingen al zijn geïntroduceerd, zijn de paragrafen over specifieke gedragingen ingeleid met een verkorte beschrijving. Voor de uitgebreidere introductie per gedraging, zie hoofdstuk 2.

Om zicht te krijgen op de totale omvang van daderschap cyber- en gedigitaliseerde criminaliteit worden verschillende bronnen geraadpleegd. De omvangcijfers uit deze bronnen zijn gebaseerd op opsporingszaken, misdrijven, verdachten en strafzaken afkomstig uit politie- en OM-registraties. Verder biedt de Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ; Van der Laan & Beerthuizen, 2016) inzicht in zelfgerapporteerd daderschap onder jongeren tussen de 10 en 22 jaar. Het meten van zelfgerapporteerd daderschap van cyber- en gedigitaliseerde criminaliteit is (vooralsnog) niet gedaan bij een representatieve steekproef van de volwassen of gehele Nederlandse bevolking. Deze gegevens geven de omvang weer op verschillende niveaus van het trechtermodel (zie figuur 1). De uitkomsten uit de verschillende bronnen zijn gepresenteerd in tabel 13 en worden vervolgens per type bron in de tekst besproken.

4.2.1 Politieregistraties: opsporingsonderzoeken en misdrijven

Niet alle specifieke vormen van cyber- en gedigitaliseerde criminaliteit zijn als zodanig terug te vinden in politieregistraties. De enige standaardclassificatie van cybercriminaliteit die de politie kent is computervredebreuk (of F90 cybercrime), welke niet erg informatief is betreffende specificiteit van een delict. Zo is niet

duidelijk of er sprake is van hacken, ransomware of een DDoS-aanval. Om deze reden wordt computervredebreuk onder de noemer algemene cybercriminaliteit besproken. Daarnaast zijn er ook gegevens over het aantal opsporingsonderzoeken van cybercriminaliteit in het algemeen. Uit gegevens van het CBS (2020b) blijkt dat het aantal geregistreerde misdrijven computervredebreuk is toegenomen van 1.070 misdrijven in 2010 tot bijna 4.820 misdrijven in 2019 (zie tabel 13). Het aantal misdrijven varieert echter door de tijd. Zo worden in 2012 4.620 misdrijven geregistreerd, terwijl in het opvolgende jaar 2013 nog maar bijna 2.540 misdrijven worden geregistreerd. Het aantal opgehelderde misdrijven blijft met rond de 200 misdrijven per jaar relatief stabiel (met hier en daar enige uitschieters).

Vergelijkbare statistieken van geregistreerde misdrijven worden ook via open data van de politie gerapporteerd[8], maar dan onder de algemene noemer cybercrime (d.w.z., registratiecode F90). Beide bronnen zich baseren zich op het Basis Voorziening Informatie (BVI) en verschillen voornamelijk in gehanteerde terminologie en iets in aantallen. Om deze redenen rapporteren we niet beide cijferreeksen.

De jaarverantwoording van de politie bespreekt in hoeverre doelen zijn behaald die in de Veiligheidsagenda 2015-2018 zijn geformuleerd, zoals het aantal gerealiseerde complexe opsporingsonderzoeken naar cybercriminaliteit (Politie, 2019). Tussen 2015 en 2018 is het aantal gerealiseerde complexe opsporingsonderzoeken naar cybercriminaliteit gestegen van ruim 20 naar ruim 40 (zie tabel 13). Deze opsporingsonderzoeken zijn door Team High Tech Crime uitgevoerd en, vanaf 2018, ook door acht cybercrimeteams binnen de regionale eenheden. Deze eenheden richten zich op opsporen, preventie, verstoren, signaleren en adviseren op het gebied van cybercriminaliteit. De opsporingsonderzoeken kunnen het gevolg zijn van meldingen van cyber- en gedigitaliseerde criminaliteit (brengwerk), maar betreffen ook onderzoek op eigen initiatief (haalwerk). De opsporingsonderzoeken richten zich onder andere op hacken, DDoS-aanvallen, cybercrime-as-a-service, en het verwijderen van servers die gebruikt werden voor bulletproof hosting (het voor opsporingsdiensten afschermen van data). De verantwoording bevat geen lijst van alle type delicten die zijn onderzocht. Productiecijfers zijn onderhevig aan registratiepraktijken en beleidsprioriteiten. De stijging in het aantal opsporingsonderzoeken kan deels wijzen op een reële stijging, maar ook dat de cybercriminaliteit een hogere prioritering van de politie heeft gekregen.

4.2.2 Verdachtenregistraties (OM en politie)

Om verdachten te registreren wordt tot 2010 door de politie gebruikgemaakt van het Herkenningsdienstsysteem (HKS). Ruiter en Bernaards (2012) rapporteren dat in het HKS ruim 70 verdachten computervredebreuk zijn geregistreerd in 2008 (zie tabel 13). In 2009 is dit iets minder dan 70 verdachten. Vanaf 2010 is landelijk overgeschakeld op de Basisvoorziening Handhaving (BVH), wat een mogelijk trendbreuk kan veroorzaken. Uit CBS-gegevens blijkt dat bijna 250 personen verdacht waren van computervredebreuk in 2010 (CBS, 2020b). Dit aantal blijft in de daaropvolgende jaren tussen de 200 en 300, tot er in 2018 520 verdachten van computervredebreuk zijn geregistreerd. In 2019 daalt het aantal weer tot bijna 430. Dit aantal is gebaseerd op zaken waarbij door aangifte opnemende politieambtenaar sprake zou zijn van computervredebreuk.

8 https://data.politie.nl

Tabel 13 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit algemeen

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Politieregistraties												
Aantal geregistreerde misdrijven computervredebreuk			1.070	2.025	4.620	2.535	2.045	2.225	1.875	2.320	2.945	4.815
Aantal opgehelderde misdrijven computervredebreuk			195	225	265	255	195	165	170	185	380	220
Aantal geregistreerde verdachten computervredebreuk (HKS)	74	69										
Aantal geregistreerde verdachten computervredebreuk			245	265	300	295	235	195	215	260	520	425
Politie jaarverantwoording 2018												
Aantal complexe opsporingsonderzoeken cybercriminaliteit								21	34	43	43	
Aantal verdachten (OM) cybercriminaliteit								124	171	227	299	
Aantal verdachten (politie) cybercriminaliteit								172	177	215	364	
RAC-min												
Instroomstrafzaken OM												
Cybercriminaliteit	85	79	68	87	125	108	160	140	184	233	281	
Gedigitaliseerde criminaliteit	541	777	663	661	688	655	606	497	469	466	363	
Gedigitaliseerde zedencriminaliteit	395	451	500	426	545	590	552	447	421	420	326	
Andere gedigitaliseerde criminaliteit	146	326	163	235	143	65	54	50	48	46	37	
Instroom strafzaken afgedaan door rechter met schuldigverklaring												
Cybercriminaliteit	17	31	33	26	38	43	40	61	62	76	72	
Gedigitaliseerde criminaliteit	366	536	444	407	358	320	307	256	254	230	172	
Gedigitaliseerde zedencriminaliteit	259	293	320	253	269	278	270	231	228	214	159	
Andere gedigitaliseerde criminaliteit	107	243	124	154	89	42	37	25	26	16	13	
Monitor Zelfgerapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap cybercriminaliteit												
10- en 11-jarigen								6,7%				
12- tot en met 17-jarigen								16,5%				
18- tot en met 22-jarigen								21,9%				
Zelfgerapporteerd daderschap gedigitaliseerde criminaliteit												
10- en 11-jarigen								3,5%				
12- tot en met 17-jarigen								13,1%				
18- tot en met 22-jarigen								8,5%				
Zelfgerapporteerd daderschap cyber- en gedigitaliseerde criminaliteit												
10- en 11-jarigen								7,8%				
12- tot en met 17-jarigen								24,7%				
18- tot en met 22-jarigen								25,8%				

Uit de jaarverantwoording van de politie blijkt dat op basis van OM-registraties het aantal verdachten meer dan twee keer zo groot is geworden tussen 2015 en 2018 (van ruim 120 tot bijna 300 verdachten; Politie, 2019). Het aantal verdachten op basis van politieregistraties ligt iets hoger, namelijk ruim 170 in 2015 en ruim 360 in 2018. Het verschil tussen registraties van het OM en van de politie in het aantal verdachten wordt in het rapport niet toegelicht. In de jaarverantwoording van de politie is bovendien niet gespecificeerd van welke type delicten personen worden verdacht. Hierdoor is inzicht krijgen in welke gedragingen allemaal onder de noemer cybercriminaliteit vallen niet mogelijk. Verder is het uit deze rapportage niet duidelijk of deze cijfers gebaseerd zijn op verdachten die zijn opgespoord door de speciale cybercrimeteams, of ook door overige eenheden van de politie.

4.2.3 Instroom van strafzaken bij het OM en ZM (RAC-min)

In deze paragraaf bespreken we zaken met cyber- en gedigitaliseerde criminaliteit die in de periode 2008 tot en met 2018 bij het OM zijn ingestroomd. In deze vervolgingsfase heeft het OM meerdere mogelijkheden om strafzaken tegen een verdachte af te doen, zoals aanbieden van een transactie of strafbeschikking, doorsturen naar de rechterlijke macht of seponeren (via een beleids- of technisch sepot). Deze statistieken komen uit RAC-min (zie voor de methodologie bijlage 2).

Volgens het OM-registratiesysteem RAC-min zijn in de periode 2008 tot en met 2018 ruim 1.500 strafzaken betreffende cybercriminaliteit ingestroomd bij het OM (zie tabel 13). De instroom komt in 2008 tot en met 2011 niet boven de 100 strafzaken per jaar uit, maar is over de loop der jaren toegenomen tot ruim 280 strafzaken in 2018. Betreffende gedigitaliseerde criminaliteit zijn in dezelfde periode bijna 6.400 strafzaken ingestroomd, hoewel hier grofweg sprake is van een (niet-jaarlijkse) daling van ruim 540 strafzaken in 2008 tot ruim 360 strafzaken in 2018. De meeste strafzaken gedigitaliseerde criminaliteit gaan om zedenmisdrijven (zoals grooming of kinderpornografie) en dit gaat zeker op voor de latere jaren van observatie. Om deze cijfers in perspectief te plaatsen ten opzichte van de totale instroom strafzaken bij het OM, de totale instroom betreft in de periode 2008 tot en met 2018 jaarlijks tussen de 170.000 en 258.000 strafzaken (Choenni, Van der Braak & Platenburg, 2019). Het aantal strafzaken cyber- en gedigitaliseerde criminaliteit zijn dus slechts een fractie van de totale instroom met minder dan 1%.

Het aantal strafzaken cybercriminaliteit dat door de rechter in eerste aanleg is afgedaan met een schuldigverklaring ligt lager dan de totale instroom bij het OM. In de periode 2008 tot en met 2018 zijn er door de rechter bijna 500 strafzaken afgedaan met een sanctie (of schuldigverklaring zonder straf). Over de gehele linie is er sprake van een stijging van bijna 20 strafzaken in 2008 tot jaarlijks meer dan 60 strafzaken in de periode 2015 tot en met 2018. Voor gedigitaliseerde criminaliteit gaat het in de periode 2008 tot en met 2018 om bijna 3.700 strafzaken, met een enigszins dalende trend van bijna 370 strafzaken in 2008 naar ruim 170 strafzaken in 2018. Net als bij de instroom van strafzaken bij het OM gaan de door de rechter afgedane strafzaken voornamelijk over zedenmisdrijven. In de latere jaren komen andere vormen van gedigitaliseerde criminaliteit, zoals fraude, amper voor.

De (strafrechtelijke) ernst van feiten in strafzaken kan worden afgelezen aan de strafdreiging of indirecter aan de opgelegde sanctie. Wanneer gekeken wordt naar deze indicatoren van ernst van deze strafzaken is er overwegend sprake van een 'verzwaring' door de tijd heen (zie tabel 14). Voor zowel de strafzaken met cybercriminaliteit als met gedigitaliseerde criminaliteit is de gemiddelde maximale straf-

dreiging (in jaren vrijheidsstraf) toegenomen. Voor cybercriminaliteit ligt deze strafdreiging gemiddeld rond de vier jaar in 2008 tot en met 2014, in de jaren daarna is deze toegenomen tot een gemiddelde strafdreiging van vijf jaar. Voor gedigitaliseerde criminaliteit ligt deze boven de 5,5 jaar in 2008 en neemt toe tot 7,5 jaar in 2018.

Ook lijkt het percentage strafzaken met een onvoorwaardelijke vrijheidsstraf te zijn toegenomen. Voor strafzaken met cybercriminaliteit ligt dit percentage op hoogstens ruim 30% in de jaren 2008 tot en met 2014, waarna deze toeneemt in de jaren daarna. Voor gedigitaliseerde criminaliteit ligt in 2008 dit percentage op 47% en stijgt grofweg jaarlijks tot 83% in 2018. Bij de gemiddelde opgelegde straf is voor strafzaken met cybercriminaliteit een minder duidelijk patroon te zien, waar de pieken en dalen in celdagequivalenten relatief verspreid zijn over de hele periode 2008 tot en met 2018. Bij gedigitaliseerde criminaliteit is de gemiddelde straf wel toegenomen van iets meer dan 300 celdagequivalenten in 2008 en 2009 tot rond en boven de 400 in 2015 tot en met 2018.

4.2.4 Cyber- en gedigitaliseerde criminaliteit onder jongeren

Politie en justitiegegevens zijn afhankelijk van beleids- en opsporingsprioriteiten en van activiteiten van de betreffende instanties. Zelfrapportage van daderschap is een justitie-onafhankelijke bron die inzicht kan geven in de omvang van daderschap van cyber- en gedigitaliseerde criminaliteit. Voor de totale populatie van Nederlanders is (vooralsnog) geen representatief zelfrapportage bron beschikbaar, maar voor minderjarigen en jongvolwassenen is die er wel.

Op basis van de MZJ uit 2015 blijkt dat, met variatie naar leeftijd, 7-22% van 10- tot en met 22-jarigen aangeeft een vorm van cybercriminaliteit te hebben gepleegd in het jaar voorafgaand aan deelname (zie tabel 13). Bij cybercriminaliteit is deze prevalentie het laagst bij de 10- en 11-jarigen en het hoogst bij de 18- tot en met 22-jarigen. Voor gedigitaliseerde criminaliteit is deze prevalentie 4-13%[9]. Bij deze vorm van criminaliteit is de prevalentie het hoogst bij 12- tot en met 17-jarigen. Wanneer beide vormen van online criminaliteit samengenomen worden, is de prevalentie bijna 8% bij 10- en 11-jarigen en voor 12-jarigen en ouder rond de 25%.

Deze cijfers staan in contrast met officiële registratiecijfers betreffende een schatting van de omvang (zie bijvoorbeeld Van der Laan & Beerthuizen, 2018). Hoewel een dergelijk contrast altijd optreedt wanneer prevalentie via zelfrapportage met officiële registratie vergeleken wordt, lijkt dit contrast groter voor cyber- en gedigitaliseerde criminaliteit (28-31% zelfrapportage versus 0,01% registratie) in vergelijking met traditionele criminaliteit (35-37% zelfrapportage versus 1% registratie; Van der Laan, Beerthuizen & Weijters, 2016).

9 De prevalentiepercentages van gedigitaliseerde criminaliteit wijken af van die in Van der Laan & Beerthuizen (2016), omdat het item 'zich voordoen als iemand anders op internet' niet langer wordt meegenomen in de schaal gedigitaliseerde criminaliteit. Dit item wordt te onduidelijk geacht om definitief crimineel gedrag mee vast te kunnen stellen (zie ook bijlage 2).

Tabel 14 Aardcijfers daderschap cyber- en gedigitaliseerde criminaliteit algemeen

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
RAC-min												
Strafzaken cybercriminaliteit afgedaan door de rechter met schuldverklaring												
Gemiddelde maximale strafdreiging (in jaren)	4,29	3,55	3,18	3,90	4,08	3,51	4,02	5,40	4,94	4,93	5,06	
Gemiddelde oplegde straf (celdagequivalenten)	78	218	287	100	111	98	285	310	327	250	172	
Percentage onvoorwaardelijke vrijheidsstraffen	n<5	32%	20%	n<5	19%	18%	28%	46%	47%	37%	34%	
Strafzaken gedigitaliseerde criminaliteit afgedaan door de rechter met schuldverklaring												
Gemiddelde maximale strafdreiging (in jaren)	5,63	5,93	5,80	6,29	6,07	6,05	6,37	6,68	6,77	7,18	7,56	
Gemiddelde oplegde straf (celdagequivalenten)	323	306	360	373	403	383	361	460	390	470	420	
Percentage onvoorwaardelijke vrijheidsstraffen	47%	56%	52%	61%	62%	71%	77%	77%	81%	80%	83%	

4.3 Hacken

Met hacken wordt kortweg bedoeld dat op onrechtmatige wijze toegang wordt verkregen tot een digitale omgeving. Dit kunnen e-mail boxen, systemen voor online bankieren, afgesloten netwerken op werk en nog veel meer zijn. Vaak wordt bij de term hacken gedacht aan technische methoden om dit te bewerkstelligen, zoals het gebruikmaken van zwakheden in digitale infrastructuren. Dit is echter niet noodzakelijk. Er kan bijvoorbeeld ook gebruikgemaakt worden van brute force technieken (d.w.z, het herhaald uitproberen van talloze wachtwoorden) of het verkrijgen van iemands wachtwoord via social engineering (bijvoorbeeld dat een dader zich voordoet als een werknemer van een bank tegenover een klant van hen wiens gegevens hij wilt bemachtigen).

4.3.1 Politieregistraties: verdachten van hacken

Afgaand op de tekstuele informatie in politieregistraties is het mogelijk om te kijken naar verdachten van specifiek hacken, in plaats van de meer algemene termen computervredebreuk of cybercrime. In het textmining onderzoek van Tollenaar et al. (2019) blijkt dat bij bijna 20% van de ruim 3.710 hacking registraties uit 2016 een verdachte kon worden gekoppeld.

4.3.2 Hacken onder jongeren

In de MZJ 2015 wordt naar drie gedragingen gevraagd die hacken betreffen of gerelateerd zijn aan hacken—hacken ongespecificeerd, hacken met vervolgens manipuleren van gegevens in de binnengedrongen omgeving, en het veranderen van iemands wachtwoord. De binnen te dringen omgevingen die genoemd worden bij de vraagstelling zijn computers, e-mailaccounts en socialenetwerksites. Hacken (ongespecificeerd) is de meest voorkomende vorm van deze drie items met ongeveer 6-18% prevalentie, afhankelijk van de leeftijd van de respondent (zie tabel 15). 10- en 11-jarigen rapporteren dit gedrag het minst, jongvolwassenen het meest. Dit item is ook de meest voorkomende vorm van zelfgerapporteerde cybercriminaliteit binnen de MZJ. De prevalenties van hacken met manipulatie en het veranderen van iemands wachtwoord liggen dichter bij elkaar, respectievelijk 1-5% en 1-7%. Ook hier is enige variatie merkbaar tussen de leeftijdscategorieën. Gezien dat deze twee items inhoudelijk verwant aan elkaar zijn, is het niet verwonderlijk dat de prevalenties dicht bij elkaar liggen.

4.4 DDoS-aanvallen

Distributed Denial of Service (DDoS-)aanvallen zijn gecoördineerde aanvallen op computers of systemen met als doel deze onbruikbaar te maken. Zo kunnen privécomputers niet meer op internet of worden websites van banken en overheidsinstellingen onbruikbaar gemaakt. DDoS-aanvallen maken vaak gebruik van een clandestien netwerk van gehackte computers en apparaten om zo hun doelen te overladen.

Tabel 15 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit hacken

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Textmining politieregistraties (BVH)												
Percentage registraties met verdachte van totale aantal registraties hacken									19,40%			
Monitor Zelfgerapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap hacken												
10- en 11-jarigen								5,6%				
12- tot en met 17-jarigen								12,0%				
18- tot en met 22-jarigen								18,1%				
Zelfgerapporteerd daderschap hacken met manipulatie												
10- en 11-jarigen								1,4%				
12- tot en met 17-jarigen								3,7%				
18- tot en met 22-jarigen								5,1%				
Zelfgerapporteerd daderschap wachtwoord veranderen												
10- en 11-jarigen								1,2%				
12- tot en met 17-jarigen								6,6%				
18- tot en met 22-jarigen								5,8%				

Tabel 16 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit DDoS-aanvallen

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Rechtspraak.nl (via CPB)												
Aantal rechtszaken DDoS-aanvallen								1				
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap DDoS-aanval												
10- en 11-jarigen								0,1%				
12- tot en met 17-jarigen								2,1%				
18- tot en met 22-jarigen								1,1%				

4.4.1 DDoS-aanvallen in officiële registraties

In de literatuur wordt relatief weinig gerapporteerd over de omvang van daderschap van DDoS-aanvallen. Op basis van vonnissen van rechtspraak.nl blijkt volgens het Centraal Planbureau (CPB, 2016) dat er in 2015 slechts één rechtszaak betrekking had op DDoS-aanvallen (zie tabel 16). Omdat op rechtspraak.nl een selectie van zaken wordt gepubliceerd zijn dit (waarschijnlijk) niet alle rechtszaken.

4.4.2 DDoS-aanvallen onder jongeren

In de MZJ 2015 is binnen de schaal van cybercriminaliteit één item opgenomen over het uitvoeren van een DDoS-aanval op een website of e-mailbox. Het aantal jonge-ren dat aangeeft een dergelijke aanval te hebben uitgevoerd is beperkt met 0,1%-2% van de bevraagden (zie tabel 16). Bij 10- en 11-jarigen komt het delict vrijwel nooit voor met een prevalentie van 0,1% en bij 12-jarigen en ouder is dit grofweg 1-2%.

4.5 Malware

Onder malware worden alle vormen van software verstaan die als doel hebben om een computer of systeem te beschadigen. Hoewel het programmeren van malware op zichzelf niet noodzakelijk een strafbaar feit is, is de distributie van malware dat wel, omdat er dan (pas) schade kan optreden.

4.5.1 Gedetecteerde malware aanvallen

Gegevens over de omvang daderschap malware binnen de justitiële keten zijn schaars. Een andere bron om zicht te krijgen op de omvang van daderschap van malware in Nederland zijn gepubliceerde statistieken door betrokken bedrijven. Dit kan worden beschouwd als de geobserveerde criminaliteit (zie figuur 1). Deze statis-tieken zijn echter niet altijd even betrouwbaar. Het aantal infecties is een moment-opname en bedrijven die de gegevens rapporteren hebben een belang bij de om-vang van hun statistieken (Politie, 2012). Zo hebben antivirus-bedrijven baat bij een hogere mate van infecties om het belang van hun product te onderstrepen. Daar-naast zijn lagere cijfers van belang voor softwareontwikkelaars, omdat hogere cij-fers kwetsbaarheden kunnen blootgeven en hun product daarmee minder aantrek-kelijk maken. Desalniettemin kunnen deze statistieken enig inzicht bieden in trends van malware.

Enige omvangstatistieken in absolute zin zijn afkomstig van Akamai (2017; 2018). Het aantal aanvallen op webapplicaties afkomstig uit Nederland lijken te zijn toe genomen. Waar Akamai ongeveer 23 miljoen web application attacks afkomstig uit Nederland detecteerde in 2017, zijn dat er bijna 94 miljoen in 2018 (zie tabel 17). Dit is bijna 12% van het totale aantal aanvallen wereldwijd in 2018.

Gegevens uit andere bronnen betreffen alleen de relatieve omvang van malware aanvallen uit Nederland, maar rapporteren dat dit aandeel relatief groot is. In 2009 hoort Nederland met 2% van het totale aantal aanvallen tot de landen waar de meeste web application attacks vandaan komen (Symantec, 2010). In het tweede kwartaal van 2018 komt bijna 26% van de wereldwijd geblokkeerde web based attacks (door Kapersky) uit Nederland (ENISA, 2019). Alleen uit de VS komen meer aanvallen (bijna 46%). In het geval van ransomware zit Nederland in de top 10 met 3% van de aanvallen (ENISA, 2017).

Tabel 17 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit malware

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Rechtspraak.nl (via CPB)												
Aantal rechtszaken malware								5				
Akamai												
Web application attacks vanuit Nederland (x 1.000.000)										23	94	
Textmining politieregistraties (BVH)												
Percentage registraties met verdachte van totale aantal registraties ransomware									25,0%			
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap virus versturen												
10- en 11-jarigen								0,6%				
12- tot en met 17-jarigen			0,7%					1,1%				
18- tot en met 22-jarigen								0,6%				

Nederland is echter niet terug te vinden in de top met het hoogste percentage inwoners met geïnfecteerde computers, wat kan betekenen dat een groot deel van de uit Nederland afkomstige aanvallen op buitenlandse computers zijn gericht. De aanvallen vanuit Nederlandse botnet C&C-servers lijken voornamelijk in Noorwegen en Zweden slachtoffers te maken (Level 3, 2015).

Het grote aantal in Nederland gehoste aanvallen betekent overigens niet noodzakelijk dat het ook Nederlandse daders betreft; het betekent dat de gebruikte systemen zich in Nederland bevinden (Akamai, 2018). Een mogelijk verklaring voor Nederland als aantrekkelijk land om aanvallen vanuit te sturen zijn het relatief grote aantal botnet C&C-servers, besmette URL's en spamservers (zie box 3) en een relatief snel en robuust internetnetwerk (Level 3, 2015).

Box 3 Dreigingsniveau daderschap

Naast gegevens over de omvang van de daders of misdrijven, zijn gegevens gepubliceerd over mogelijke dreiging van daderschap. Deze gegevens zijn gebaseerd op statistieken van cybersecurity bedrijven, die minder betrouwbaar kunnen zijn dan statistieken uit wetenschappelijke literatuur (zie ook paragraaf 2.5.2). Het merendeel van de hier beschreven informatie is terug te lezen in rapporten van de European Union Agency for Network and Information Security (ENISA). Deze organisatie geeft jaarlijks een rapport uit over het online dreigingslandschap in Europa.

Spam is wereldwijd de meest prevalente vorm van cyberdreiging en wordt gebruikt om malware en besmette URL's te verspreiden. Volgens McAfee (2015a) bevindt 3% van spamdomeinen zich in Nederland en Nederland behoort daarmee tot de top 4 landen wereldwijd. In het tweede kwartaal van 2017 is nog steeds 2% van de spam afkomstig uit Nederland (10e wereldwijd), maar in het derde kwartaal in 2017 en in het tweede kwartaal van 2018 is Nederland niet meer terug te vinden in de top 10 (ENISA, 2017; 2018).

Het aantal besmette URL's, die onder andere aan de hand van spam kunnen worden verspreid, zijn relatief vaak afkomstig uit Nederland. Deze besmette URL's worden onder andere gebruikt voor phishing. In het tweede kwartaal van 2017 is 20% van het totale aantal besmette URL's gehost in Nederland (ENISA, 2017). Alleen uit de VS komen meer besmette URL's (32%). Eerdere gegevens laten lagere percentages zien. In 2015 komt 2% van de besmette URL's uit Nederland (TrendLabs, 2015), en in 2012 is ruim 2% van de phishing websites afkomstig uit Nederland (Symantec, 2012).

Nederland behoort tevens tot de landen met de meeste botnets control and command (C&C) servers. Botnet C&C-servers zijn servers die spam, malware, DDoS-aanvallen of besmette advertenties verspreiden. In 2016 kan 4% van de wereldwijde botnet C&C-servers in Nederland worden gelokaliseerd (ENISA, 2016). Rapporten van McAfee (2015a; 2015b; 2016a; 2016b; 2016c; 2016d; 2017a; 2017b; 2018a; 2018b; 2018c) laten soortgelijke cijfers zien: tussen 2014 en 2018 behoort Nederland tot de top 6 landen met meeste botnet C&C-servers (3-6% van het wereldwijde aantal botnet C&C-servers).

4.5.2 Malware in officiële registraties

Tollenaar et al. (2019) schatten dat er ruim 1.930 meldingen van ransomware in politieregistraties terug te vinden zijn in 2016 (zie hoofdstuk 3), waarvan in 25%

van de gevallen minimaal één verdachte is geregistreerd. Verder zijn in 2015 vijf rechtszaken over malware terug te vinden op rechtspraak.nl (CPB, 2016).

4.5.3 Malware onder jongeren

Er wordt naar één malware-gerelateerde gedragingen gevraagd in de MZJ, namelijk het versturen van virussen. Dit item is ook al in de 2010 meting bevraagd. In 2010 wordt door 0,7% van 12- tot en met 17-jarigen gerapporteerd dat zij in de twaalf maanden voorafgaand aan deelname een virus hadden opgestuurd naar iemand anders (zie tabel 17). In 2015 is de prevalentie van dit item ruim 1% voor deze leeftijdsgroep. Voor de andere leeftijdsgroepen komt dit percentage niet boven de 1% in 2015.

4.6 Online bedreiging, cyberpesten en verspreiding seksueel beeldmateriaal

Online bedreiging betreft het uiten van intenties om een ander persoon iets aan te doen via een onlinekanaal, zoals e-mail of WhatsApp, vaak met een gewelddadige intentie. Cyberpesten betreft een breed scala aan kwetsende gedragingen, die niet noodzakelijk strafrechtelijk vervolgbaar zijn. Verspreiding van seksueel beeldmateriaal betreft het zonder toestemming op of via internet verspreiden van seksueel beeldmateriaal van het slachtoffer.

4.6.1 Politieregistraties

Gedigitaliseerde delicten, zoals online bedreiging, zijn moeilijk terug te vinden in registraties, omdat ze doorgaans worden geclassificeerd onder het traditionele delict, in dit geval bedreiging. Aangezien ook andere databronnen over daderschap ontbreken, zijn er relatief weinig gegevens bekend over de omvang van online bedreiging onder de hele populatie bekend en is het (nog) niet mogelijk ontwikkelingen door de tijd in kaart te brengen.

4.6.2 Online bedreiging en cyberpesten onder jongeren

Binnen de MZJ 2015 worden twee modi operandi bevraagd van online bedreiging, namelijk via e-mail, SMS of chatbox, en daarnaast via social media. Het item met de meer gedateerde media is ook voor het jaar 2010 bevraagd. Toen heeft ruim 2% van de 10- en 11-jarige respondenten aangegeven dit gedaan te hebben tegenover bijna 7% van de 12- tot en met 17-jarigen (zie tabel 18). In 2015 is de prevalentie voor deze leeftijdsgroepen respectievelijk bijna 3% en 8%. Bij de toen nieuw bevraagde jongvolwassenen is de prevalentie ruim 5%. De prevalentie van het item online bedreigen via social media laat een vergelijkbare prevalentie zien van 2-8%, afhankelijk van de leeftijd van de respondenten.

Tabel 18 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit online bedreiging

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap bedreigen via texting												
10- en 11-jarigen			2,1%					2,5%				
12- tot en met 17-jarigen			6,5%					7,7%				
18- tot en met 22-jarigen								5,4%				
Zelfgerapporteerd daderschap bedreigen via social media												
10- en 11-jarigen								2,0%				
12- tot en met 17-jarigen								8,4%				
18- tot en met 22-jarigen								4,9%				
Zelfgerapporteerd jeugdig daderschap verspreiding seksueel beeldmateriaal minderjarigen												
10- en 11-jarigen								0,0%				
12- tot en met 17-jarigen								4,4%				
18- tot en met 22-jarigen								1,6%				
Jeugd en Cybersafety (10- tot en met 18-jarigen)												
Zelfgerapporteerd daderschap cyberpesten (K&V, 2013)				4,7%								
Zelfgerapporteerd daderschap cyberpesten (K&S, 2012)				3,8%								
Roddelen				3,0%								
Uitschelden en/of bedreigen				2,5%								
Buitensluiten				1,4%								
Het op internet plaatsen van vervelende foto's of filmpjes.				0,9%								
Toesturen van vervelende foto's of filmpjes				1,0%								

Ook wordt binnen de MZJ 2015 gevraagd of jongeren in het afgelopen jaar wel-eens seksueel beeldmateriaal van minderjarigen hebben verstuurd. Echter, bij de vraagstelling is het niet zeker of dit met of zonder toestemming van de afgebeelde personen is gebeurd. Wel is het verspreiden van seksueel beeldmateriaal van minderjarigen per definitie strafbaar. Dat gezegd hebbende, sexting komt relatief vaak voor onder jongeren (zie bijv., De Graaf, Bultnick, Van den Brink, Coehoorn, Van den Borne & Meijer, 2019) en hoeft niet noodzakelijk een intentioneel schadelijk kenmerk te hebben. De ernst en impact van het item zoals bevraagd in de MZJ isdaarmee moeilijk te bepalen. In ieder geval rapporteert geen van de bevraagde 10- en 11-jarigen in het afgelopen jaar dergelijk beeldmateriaal verstuurd te hebben. Bij 12- tot en met 17-jarigen ligt deze prevalentie op bijna 4% en bij jongvolwassenen ligt deze prevalentie op bijna 2% (zie tabel 18).

Een ander onderzoek onder jongeren is Jeugd en Cybersafety (Kerstens & Stol, 2012). In dit onderzoek zijn jongeren tussen de 10 en 18 jaar bevraagd naar verschillende online gedragingen, waaronder daderschap van cyberpesten. In totaal geeft bijna 4% van de bevraagde jongeren aan zich in de afgelopen drie maanden schuldig te hebben gemaakt aan één van de voorgelegde vormen van cyberpesten. Kerstens en Veenstra (2013), die op basis van dezelfde data onderzoek hebben gedaan naar criminologische verklaringen van cyberpesten, rapporteren een hoger cijfer van bijna 5%. Als we kijken welke vormen van cyberpesten het meeste voorkomen zijn dat roddelen (3%), uitschelden/bedreigen (bijna 3%) en buitensluiten (ruim 1%). Het op vervelende foto's of filmpjes op internet plaatsen (0,9%) of het toesturen (1%) komt het minder voor (zie tabel 18).

4.7 Online fraude

Bij fraude bevoordeelt een dader zich onder valse voorwendselen ten koste van het slachtoffer. Uit paragraaf 2.7 blijkt dat slachtofferschap van online fraude in veel verschillende vormen voorkomt. Hoewel hierbij uiteraard daders bij betrokken zijn, zijn er slechts gegevens beschikbaar van daderschap van identiteitsfraude, phishing, online aan- en verkoopfraude en virtuele diefstal. Bovendien zijn deze gegevens beperkt en is het niet mogelijk om trends in daderschap van online fraude weer te geven.

4.7.1 Online fraude in officiële registraties

Het aantal registraties van online aan- en verkoopfraude in het BVH telt bijna 33.900 (zie hoofdstuk 2; Tollenaar et al., 2019). Bij ruim 60% van deze registraties wist de politie ten minste één verdachte op te sporen. Het CPB (2016) rapporteert daarnaast dat er in 2015 zeventien rechtszaken over phishing en twee rechtszaken over identiteitsfraude terug te vinden waren op rechtspraak.nl.

4.7.2 Online fraude onder jongeren

Twee vragen binnen de MZJ 2015 hebben betrekking op online aan- en verkoop-fraude via internet. De prevalentie van beide vormen van fraude is erg laag, on-geacht de leeftijd van de respondenten. Zo worden beide vormen van fraude door 10- en 11-jarigen helemaal niet gerapporteerd en is de prevalentie aankoopfraude bij de oudere groepen rond de 1% (zie tabel 19). Voor verkoopfraude komt de prevalentie niet eens boven de 1% uit voor de oudere groepen.

Tabel 19 Omvangcijfers daderschap cyber- en gedigitaliseerde criminaliteit online fraude

	'08	'09	'10	'11	'12	'13	'14	`15	`16	`17	`18	`19
Rechtspraak.nl (via CPB)												
Aantal rechtszaken phishing								17				
Aantal rechtszaken identiteitsfraude								2				
Textmining politieregistraties (BVH)												
Percentage registraties met verdachte van totale aantal registraties online aan- en verkoopfraude									60,4%			
Monitor Zelfgrapporteerde criminaliteit (MZJ)												
Zelfgerapporteerd daderschap aankoopfraude												
10- en 11-jarigen								0,0%				
12- tot en met 17-jarigen								0,9%				
18- tot en met 22-jarigen								1,2%				
Zelfgerapporteerd daderschap verkoopfraude												
10- en 11-jarigen								0,0%				
12- tot en met 17-jarigen								0,2%				
18- tot en met 22-jarigen								0,3%				
Jeugd en Cybersafety												
Zelfgerapporteerd daderschap online aan- en verkoopfraude				3,1%								
Zelfgerapporteerd daderschap online aankoopfraude				2,6%								
Zelfgerapporteerd daderschap online verkoopfraude				1,0%								
Zelfgerapporteerd daderschap identiteitsfraude				4,5%								
Zelfgerapporteerd daderschap virtuele diefstal				10,2%								

In het Jeugd en Cybersafety onderzoek is zelfgerapporteerd daderschap van online aan- en verkoopfraude gemeten onder jongeren tussen de 10 en 18 jaar (Kerstens & Stol, 2012). Uit dit onderzoek blijkt dat ruim 3% van de jongeren aangeeft zich schuldig te hebben gemaakt aan online aan- en/of verkoopfraude. Als we aan- en verkoopfraude opsplitsen, blijkt dat bijna 3% van de jongeren aankoopfraude pleegt en 1% verkoopfraude. In het Jeugd en Cybersafety onderzoek is ook gevraagd naar daderschap van andere vormen van online fraude. Bijna 5% van de bevraagden geeft in de twaalf maanden voor deelname aan zich schuldig te hebben gemaakt aan identiteitsfraude (Kerstens & Jansen, 2016) en ruim 10% aan virtuele diefstal (Kerstens & Stol, 2012).

4.8 Discussie

In dit hoofdstuk is gekeken naar wat er bekend is over de aard en omvang van daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland (in hoofdstuk 2 is slachtofferschap behandeld). Net als bij slachtofferschap is gekeken naar verschillende bronnen en de afzonderlijke resultaten worden in deze paragraaf in samenhang besproken en bediscussieerd.

In tegenstelling tot slachtofferschap is er relatief weinig bekend over hoeveel Nederlanders zich schuldig maken aan cyber- en gedigitaliseerde criminaliteit. Waar er bij slachtofferschap bronnen zijn die frequent Nederlands slachtofferschap bevragen, is daderschap gebaseerd op incidentele metingen of longitudinale bronnen met beperkingen. De eerste cijfers uit de door ons aangehaalde bronnen stammen al uit 2008 (binnen het kader van dit onderzoek; over eerdere jaren zijn ongetwijfeld ook inzichten bekend). Dit betekent dat in meer dan tien jaar tijd over de omvang van daderschap relatief weinig is gepubliceerd.

De oudste cijfers binnen dit onderzoek, verkregen uit RAC-min op basis van relevante wetsartikelen en het HKS, laten qua verdachten en strafrechtelijk daderschap een beperkte omvang zien. Voor cybercriminaliteit gaat het om enkele tientallen strafzaken en verdachten per jaar, terwijl voor gedigitaliseerde criminaliteit het om enkele honderden strafzaken gaat. Afgezet tegen de vele tienduizenden strafzaken en verdachten die het OM jaarlijks behandelt (bijv., Choenni et al., 2019), gaat het dus slechts om een fractie van het totaal. Door de tijd heen neemt het aantal strafzaken en verdachten met cybercriminaliteit wel toe, maar de omvang blijft beperkt. Deze stijging zou kunnen komen door een werkelijke stijging van cybercriminaliteit. Maar, het kan ook dat de politie meer prioriteit geeft aan cybercriminaliteit, bijvoorbeeld door het verruimen van de opsporing van cybercriminaliteit van de Landelijke Eenheid naar alle regionale eenheden (Politie, 2019). Gedigitaliseerde criminaliteit volgt meer de algemene dalende misdaadtrend vanaf grofweg 2008 (bijv., Choenni et al., 2019).

Het is aannemelijk dat ten minste een deel van alle door het OM behandelde cyber- en gedigitaliseerde criminaliteit buiten zicht valt, omdat niet alle vormen van dergelijke criminaliteit via een wetsartikel te herkennen zijn. Online bedreiging en online stalking, bijvoorbeeld, zullen namelijk onder de daarvoor al langer bestaande wetsartikelen vervolgd worden. Statistieken van cybercriminaliteit zijn grotendeels terug te voeren naar computervredebreuk, een term die voor een breed scala aan verschillende cyberdelicten relevant kan zijn. Dat binnen politieregistraties het niet altijd duidelijk is of er sprake is van cyber- of gedigitaliseerde criminaliteit is al langer bekend (De Cuyper & Weijters, 2016; Leukfeldt, Veenstra, Domenie & Stol,

2012). Om relevante of specifieke strafzaken te herkennen zullen andere methoden toegepast dienen te worden, zoals textmining (zie Tollenaar et al., 2019).

Dat door de politie, het OM en de gerechtelijke macht relatief weinig strafzaken, verdachten of daders van cyber- en gedigitaliseerde criminaliteit behandeld worden komt ook uit andere bronnen naar voren. De aantallen in jaarverslagen en andere publicaties zijn tientallen of hooguit honderden per jaar. Dat er potentieel veel meer verdachten en daders zijn voor opsporing en vervolging, wordt onder andere duidelijk uit bronanalyse met innovatieve technieken. In 2016 alleen al waren er honderdduizenden registraties van cyber- en gedigitaliseerde criminaliteit in Nederlandse systemen van de politie, waaronder aangiften en meldingen (Tollenaar et al., 2019; zie ook het hoofdstuk over slachtofferschap). Echter, lang niet bij alle registraties was een verdachte gekoppeld of bekend, wat een verklaring kan zijn voor de relatief lage aantallen cyber- en gedigitaliseerde criminaliteit verder in de strafrechtketen. Ook statistieken van misdrijven van computervredebreuk in andere bronnen laten eenzelfde beeld zien (CBS, 2020b). Uit zelfrapportage blijkt ook een veel grotere omvang van (jeugdig) daderschap dan het percentage daders dat uiteindelijk terecht komt in de strafrechtketen (Van der Laan & Beerthuizen, 2016; Kerstens & Stol, 2012: Kerstens & Jansen, 2016).

Wat betreft dreigingsniveau scoort Nederland relatief hoog in internationale lijsten. Botnet C&C-servers, malicious websites, spam en aanvallen met ransomware komen relatief vaak uit Nederland, zeker rekening houdend met de beperkte omvang van Nederland. Daar staat wel tegenover dat Nederland relatief hoog scoort op het gebied van cyberveiligheid (Gehem et al., 2015; Munnichs, Kauw & Kool, 2017; NCSC, 2017).

De zoektocht naar inzichten in de aard en omvang van cyber- en gedigitaliseerde criminaliteit heeft een aantal bronnen opgeleverd. Echter, deze beperkte aantallen bronnen zijn lastig in perspectief te plaatsen. Het betreft vaak één bron op één meetmoment, waardoor trends door de tijd heen (vooralsnog) niet in kaart kunnen worden gebracht. Registratiebronnen die wel inzichten door de tijd heen geven hebben zo hun eigen beperkingen, waardoor groei (en krimp) van de omvang door de tijd heen voorzichtig geïnterpreteerd dient te worden. Zelfrapportage bronnen over daderschap van cyber- en gedigitaliseerde criminaliteit door de tijd heen zijn vooralsnog niet of in maar beperkte mate beschikbaar, en dan vooral binnen een jeugdige populatie. Ook is zelfgerapporteerd daderschap (vooralsnog) niet bevraagd onder een bredere representatieve steekproef van de gehele Nederlandse bevolking.

Betreffende de aard van cyber- en gedigitaliseerde criminaliteit in deze bronnen is er ook relatief weinig bekend. Veel verder dan een algemene beschrijving van type delicten of indirecte afleiding op basis van wetsartikelen gaan de meeste bronnen niet. Specifiek in dit hoofdstuk zijn (in alfabetische volgorde) aan bod gekomen: DDoS-aanvallen, hacken, malware, online bedreiging (en aanverwante delicten) en online fraude. Andere meer recentere delicten komen echter niet aan bod, zoals het (laten) installeren van ransomware, phishing van inloggegevens, of helpdesk- of WhatsApp-fraude. Nu is een vaker voorkomend probleem dat binnen wetenschap, justitieel beleid en praktijk er slechts gereageerd kan worden op nieuwe (cyber-) criminele ontwikkelingen, in plaats van te anticiperen en proactief te handelen (bijv., Goodman, 2015). Hierdoor is het niet mogelijk om (statistische) inzichten te geven op wat er zich momenteel of in het zeer recente verleden afspeelt.
De belangrijkste conclusie van dit hoofdstuk is daarom dat er in de bestaande literatuur relatief weinig bekend is over de aard en omvang van daderschap van

cyber- en gedigitaliseerde criminaliteit. Eén verklaring waarom er relatief weinig bekend is, is dat daderschap überhaupt moeilijk in kaart te brengen is. Alles wat via landelijke registratiesystemen bekend is betreft een fractie van alle criminaliteit (en is voornamelijk gebaseerd op meldingen van slachtoffers). Wetenschappelijk onderzoek betreft vaak een incidentele steekproeftrekking en grote enquêtes zijn schaars door kosten en vereiste inspanning. Voor deze laatste methode is het ook nog maar de vraag of veel nieuwe inzichten verkregen zullen worden, omdat cyber- en gedigitaliseerde criminelen mogelijk een specifiek en relatief kleine groep in de samenleving zijn. Een aselecte steekproef van de Nederlandse bevolking zal dergelijke criminelen mogelijk alsnog niet goed in beeld kunnen brengen (zie voor vergelijkbare problematiek met high impact crime Beerthuizen, Van Leijsen & Van der Laan, 2019). Om dit probleem tegen te gaan, hebben Weulen Kranenbarg, Holt en Van Gelder (2019), bijvoorbeeld, gebruikgemaakt van een high-risk sampling methode door 1.100 verdachten van cybercriminaliteit te benaderen. Voor onderhavig onderzoek zijn deze gegevens echter niet te gebruiken, omdat het geen representatief of volledig beeld geeft van het aantal daders binnen de totale Nederlandse bevolking. De vragenlijsten van de MZJ (Van der Laan & Beerthuizen, 2016) en Jeugd en Cybersafety (Kerstens & Stol, 2012; Kerstens & Jansen, 2016) zijn wel voorgelegd aan een aselecte steekproef, maar alleen aan jongeren en betreft vermoedelijk meer lichte cyber- en gedigitaliseerde delinquentie (gezien de zelfrapportage aard van de instrumenten; zie bijv., Farrington et al., 2003).

Kortom, op het gebied van daderschap ligt de voornaamste uitdaging in de basis— het überhaupt goed kaart brengen van daderschap. Zelfs bronnen die binnen hun eigen beperkte kader een populatie breed overzicht geven, zoals registratiebronnen van justitie, hebben te kampen met diverse problemen, zoals moeizame of onmogelijke specificatie van cyber- of gedigitaliseerd crimineel gedrag. Het is aan te raden om via alternatieve methoden verder te kijken naar daderschap van cyber- en gedigitaliseerde criminaliteit, methoden toe te passen die niet afhankelijk zijn van officiële registratieprocessen en –protocollen, of te kijken op welke manier bestaande registratiebronnen verrijkt kunnen worden.

5 Aanbieders en afnemers van cybercrime-as-a-service

Auteur: *Marinus Beerthuizen*

Samenvatting

Op onlinemarkten bieden criminelen 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. Dit fenomeen heet cybercrime-as-a-service (CAAS). Door advertenties van dergelijke diensten op onlinemarkten via geautomatiseerde methoden te observeren en te coderen (d.w.z., textmining) is het mogelijk om ontwikkelingen in deze criminaliteit weer te geven. Over het algemeen lijkt er sprake te zijn van een toename in de CAAS in de periode 2011-2017, wanneer gekeken wordt naar een aantal grote markten (bijv., AlphaBay). Echter, vanwege beperkingen in de methodiek is het moeilijk interpreteerbaar hoe groot het fenomeen nu werkelijk is.

5.1 Introductie

In dit hoofdstuk wordt een specifieke vorm van daderschap van cybercriminaliteit belicht, namelijk het aanbieden en afnemen van cybercriminele diensten. Ondanks dat bij cybercriminaliteit vaak gespecialiseerde software of kennis nodig is, is het niet noodzakelijk dat een dader deze software zelf ontwikkelt of deze kennis zelf heeft. Het gebruiken van dergelijke software kan door een relatieve leek gedaan worden of een leek kan iemand anders betalen om cyberdelicten voor hem of haar te laten plegen. Zo kan, bijvoorbeeld, ransomware aangeschaft worden of tegen betaling uitgevoerd worden door een andere partij. Dit fenomeen wordt cybercrime-as-a-service (CAAS) genoemd. Naast het installeren van ransomware op computers (zie bijv., Caballero, Grier, Kreibich & Paxxon, 2011) zijn DDoS-aanvallen veel voorkomende diensten van cybercriminaliteit (zie bijv., Karami et al., 2016). Dergelijke diensten worden onder andere aangeboden op onlinemarkten op het darkweb. Door deze markten te observeren kan informatie verkregen worden over de aard en omvang van CAAS-daderschap.

Door de ongestructureerde aard en de grote omvang van onlinemarkten zijn traditionele observatiemethoden ongeschikt. Het is onpraktisch om handmatig alle aangeboden diensten te bekijken, te scoren en te achterhalen wie de aanbieder of afnemer is. Via geautomatiseerde methoden kunnen dergelijke platformen wel efficiënt geobserveerd worden. Webscraping is een geautomatiseerde methode om in grote getalen gegevens van internet te verzamelen en te registreren. Zo wordt via het maken van zogeheten snapshots informatie van webpagina's opgeslagen, waarna de informatie bewerkt en bestudeerd wordt.

In het huidige hoofdstuk worden statistieken gepresenteerd rondom daderschap van CAAS, van zowel aanbieders als afnemers. Deze statistieken komen voort uit onderzoek naar een selectie van anonieme online markten (Van Wegberg et al., 2018[10]).

10 De auteur wil Rolf van Wegberg (TU Delft) bedanken voor het aanleveren van de gegevens voor de hier gepresenteerde statistieken. De data is toegankelijk via www.impactcybertrust.org en https://arima.cylab.cmu.edu/markets/

Eén van de inclusiecriteria van bronnen voor dit rapport is dat cyber- en gedigitaliseerde criminaliteit een Nederlands slachtoffer of dader moet kennen, of criminaliteit betreft waartegen de Nederlandse rechtshandhaving optreedt. Voor anonieme onlinemarkten is niet (altijd) te bepalen of CAAS een Nederlandse aanbieder of afnemer betreft of een Nederlands slachtoffer gaat maken. Omdat de Nederlandse politie actief is geweest (en bezig is) met verstoren van onlinemarkten, waaronder die in dit hoofdstuk besproken worden (zie, bijv., OM, 2014; Techzine, 2014; Politie, 2017; Wired, 2018), worden deze onlinemarkten relevant gevonden.

5.2 Methode

Op onlinemarkten vinden allerlei vormen van criminaliteit plaats. Om inzicht te krijgen in specifiek CAAS is het belangrijk om dit type criminaliteit te kunnen onderscheiden van andere criminaliteit. Voor een uitgebreidere beschrijving van de methodiek zie Van Wegberg et al. (2018). Wij zullen ons hier beperken tot een beknopte omschrijving.

Ten eerste zijn via webscraping gegevens verzameld van criminele advertenties op een selectie van onlinemarkten. De verzamelde gegevens betreffen onder andere een titel van de advertentie, beschrijving van de dienst of goederen, naam van de aanbieder, datum van plaatsing, enz. Deze gegevens komen van een achttal bekende onlinemarkten: Agora, AlphaBay, Black Market Reloaded (BMR), Evolution, Hydra, Pandora, Silk Road 1 (SR1) en Silk Road 2 (SR2). Niet iedere markt heeft even lang bestaan.

Ten tweede zijn deze advertenties via machine learning ingedeeld in categorieën van CAAS. Om dit te realiseren zijn handmatig 1.500 advertenties beoordeeld, om vervolgens deze beoordelingen te gebruiken om via machine learning het herkennings- en labelingproces te automatiseren.

Van Wegberg et al. (2018) maken onderscheid tussen twee vormen van CAAS—business-to-business (B2B) en business-to-consumer (B2C). De eerste betreft grootschalige aanbieding van diensten en goederen, de tweede betreft kleinschalige aanbieding van goederen die slechts eenmaal verkocht worden (bijv., beperkt bruikbare toegangsgegevens van kleine hoeveelheden accounts). De preciezere aard van de diensten en goederen moet uit de advertentieteksten gehaald worden. De statistieken in het huidige hoofdstuk beperken zich tot B2B diensten/goederen, welke te onderscheiden zijn in tien categorieën:

1 *Apps* ontwikkeld voor criminele doeleinden, zoals *keyloggers*.
2 Diensten en goederen betreffende *botnets*.
3 *Cash-out* goederen en diensten, zoals creditcard gegevens, bankgegevens en tutorials voor witwaspraktijken.
4 *E-mail* spamlijsten en benodigdheden voor phishing.
5 Microsoft Office, browser en MacOSX *exploits*.
6 *Hosting* van websites/services voor criminele doeleinden.
7 *Malware*, waaronder voornamelijk ransomware.
8 Kennis en gegevens betreffende *telefoons*, zoals manieren om beveiligingsmaatregels te omzeilen.

Sommige statistieken zijn door de auteur verwerkt. Delen van dit hoofdstuk zijn afgeleid uit Van Wegberg et al. (2018).

9 *Remote Access Trojan* software bedoeld om op afstand toegang te krijgen tot computers en dergelijke.
10 Informatie over *website* ontwikkeling, VPN verbindingen en gehackte servers.

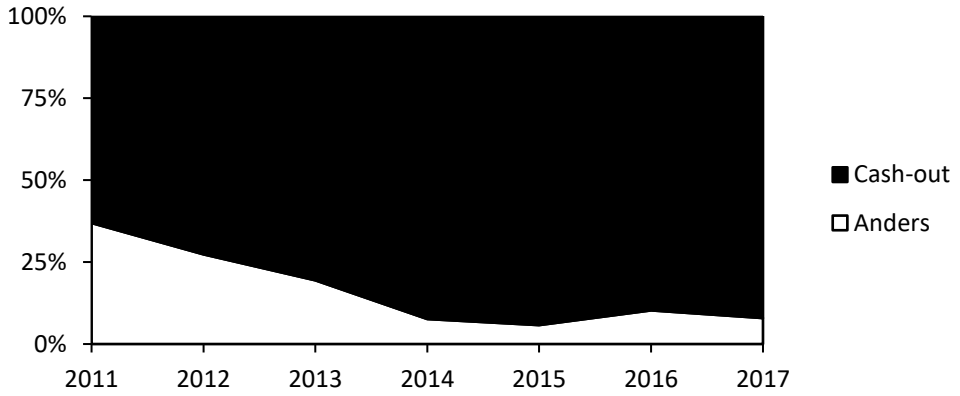
Van Wegberg et al. (2018) presenteren meerdere indicatoren van omvang van CAAS—aantallen advertenties (listings), aantallen actieve verkopers, aantallen reacties (feedback) en omzet (revenue). De variabele aantallen advertenties betreft een optelsom van geobserveerde advertenties. Actieve verkopers betreft het aantal verkopers dat op een meetmoment ten minste één advertentie heeft geplaatst in één van de tien bovengenoemde categorieën. Reacties betreft het aantal berichten dat afnemers achterlaten bij advertenties en verkopers. In deze reacties worden ervaringen en meningen over de dienst of goed openbaar gepresenteerd. Omzet is een optelsom van de geadverteerde prijzen van goederen en diensten vermenigvuldigd met het aantal feedback/reacties per aanbieding.

Wij richten ons in dit hoofdstuk op de aantallen actieve verkopers als zijnde daderschap van aangeboden CAAS en de aantallen reacties als een proxy variabele van daderschap van afgenomen CAAS. Er zijn echter geen garanties dat ieder uniek account één natuurlijk persoon betreft—een account kan door meerdere personen beheerd worden en een persoon kan ook meerdere accounts beheren. Eenzelfde probleem doet zich voor bij reacties, waar meerdere reacties door een enkel persoon achtergelaten kunnen zijn.

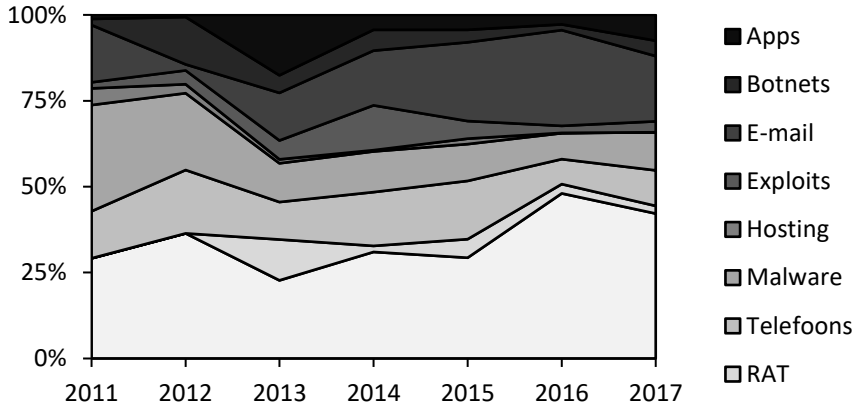
5.3 Resultaten

In figuur 7 wordt de feedback verdeling in diensten en goederen weergegeven. In 2011, toen alleen nog SR1 geobserveerd werd, betreft ongeveer twee derde van de feedback een cash-out dienst of goed. In de jaren daarna, evenals in andere markten, blijft cash-out een grote meerderheid van de feedback betreffen. Door de tijd neemt dit aandeel zelfs toe. In 2017 gaat meer dan 90% van de waargenomen feedback over een cash-out dienst of goed.

Figuur 7 Verdeling cash-out versus andere type feedback CAAS



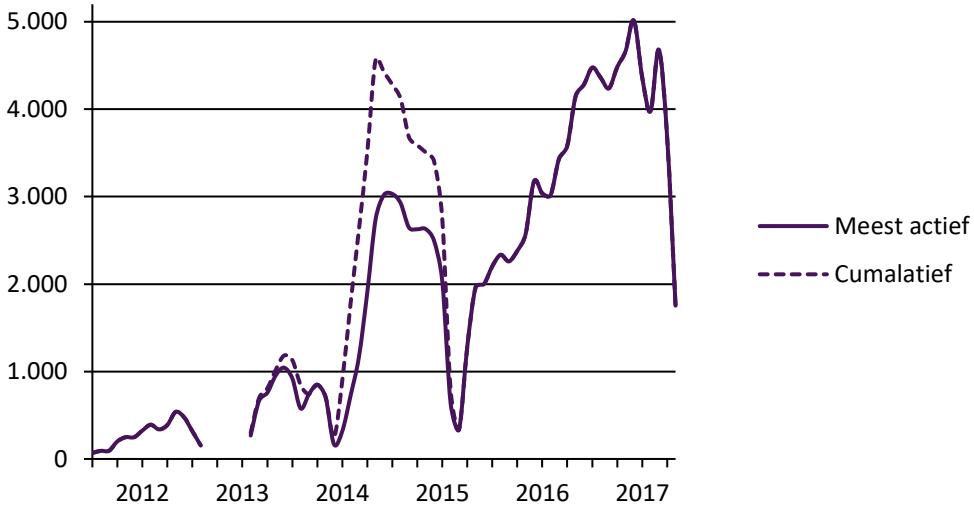
Figuur 8 Verdeling feedback type CAAS (exclusief cash-out)



In Wegberg et al. (2018) wordt het grote cash-out aandeel ook gevonden voor aantallen actieve verkopers en als onderdeel van de omzet. Deze toename kan geïnterpreteerd worden als een (verdere) toename in populariteit van cash-out diensten en goederen. Ook kan het wijzen dat later opkomende markten zich mogelijk (meer) specialiseren in cash-out diensten en goederen.

In figuur 8 wordt de feedback betreffende andere typen CAAS weergegeven (zonder cash-out). In 2011 zijn de twee grootste niet-cash-out CAAS vormen malware en website. In 2017 is website nog steeds een grote categorie, zelfs de grootste, maar malware niet meer. Op de tweede plaats is daarvoor e-mail-diensten/goederen gekomen. Een aantal categorieën komt ongeacht het jaar relatief gezien weinig voor—apps, botnets, exploits, hosting en RAT.

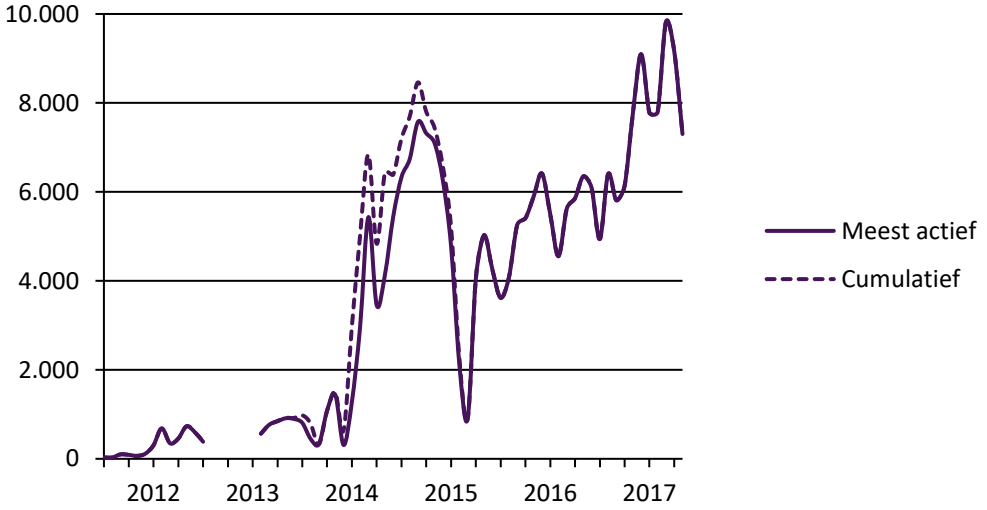
Figuur 9 Aantallen actieve verkopers CAAS



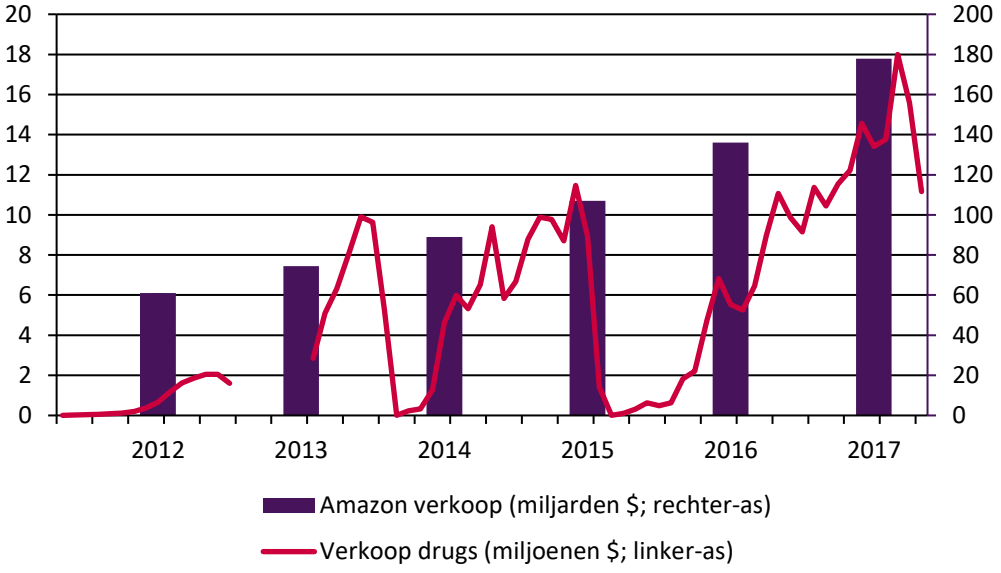
In figuren 9 en 10 zijn de aantallen actieve verkopers en de aantallen feedback weergegeven voor de geobserveerde markten. Er worden twee lijnen weergegeven —een indicatie van de meest actieve markt op het moment van observatie en een cumulatie van alle actieve verkopers verspreid over de markten. Zowel de aantallen actieve verkopers als de hoeveelheid feedback neemt toe door de tijd. Waar rond de jaarwisseling 2012 er ongeveer 500 actieve verkopers zijn en 1.000 reacties, zijn dit

op de piek eind 2017 respectievelijk 5.000 en bijna 10.000. Verder lijken de ontwikkelingen van beide indicatoren veel op elkaar—periodes met veel actieve verkopers zijn ook de periodes met veel feedback (r>0,85, p<0,001). De dippen in 2014 en 2015 voor beide indicatoren hebben ermee te maken dat toen een aantal markten ophielden te bestaan.

Figuur 10 Aantallen feedback CAAS



Figuur 11 Verkoop drugs online markten en legale verkoop Amazon



De duidelijkste ontwikkeling in aantallen actieve verkopers en feedback is een sterke toename vanaf begin 2014. Dit is een trend die ook bij andere criminele diensten en goederen waarneembaar is en ook bij legaal onlineverkeer (in figuur 11 zijn de maandelijkse en jaarlijkse verkoop weergegeven van, respectievelijk, drugs op de acht geobserveerde onlinemarkten en de algemene verkoop van Amazon online[11]).

11 Drugsstatistieken zijn verkregen via https://arima.cylab.cmu.edu/markets en de Amazon statistieken zijn verkregen via https://www.statista.com/statistics/266282/annual-net-revenue-of-amazoncom

5.4 Discussie

Het via webscraping observeren van onlinemarkten is een directe methode om inzicht te krijgen in het fenomeen CAAS. Deze directheid heeft zijn voordelen. Zo is men niet afhankelijk van de gewilligheid van daders om mee te werken aan onderzoek. Daarnaast is men ook niet afhankelijk van justitiële publicaties over aantallen verdachten en daders. Hiermee is webscraping een aanvulling op traditionelere bronnen en geeft een unieke kijk op daderschap in een 'natuurlijke' omgeving. Overigens hoeft deze methodiek zich niet te beperken tot CAAS, maar kan en wordt ook toegepast op andere criminele fenomenen (bijv., drugshandel; Christin, 2013; Soska & Christin, 2015; EMCDD/ Europol, 2017).

Er zijn echter beperkingen die interpretatie van aard en omvang bemoeilijken. Ten eerste, de huidige statistieken zijn niet noodzakelijk een volledige weergave van alle onlinemarkten. Bijvoorbeeld, Hansa is een andere populaire niet-geobserveerde markt die wel actief was tijdens de observatieperiode. Ook moet men actief blijven zoeken naar welke nieuwe markten opkomen, wanneer oude markten offline gaan. Gebeurt dit niet, dan vallen er gaten in de waargenomen ontwikkelingen.

Ten tweede, over de hoeveelheden aanbieders en afnemers is op basis van deze statistieken maar beperkt iets te zeggen. De teleenheden van daders betreffen namelijk online registraties en niet noodzakelijk een individu. Een absolute omvang van CAAS-daderschap is daarmee (vooralsnog) niet te schatten. Een account kan meerdere samenwerkende personen betreffen, of meerdere accounts kunnen beheerd worden door één persoon. Ook zijn reacties slechts een proxy variabele van het werkelijke aantal daders dat gebruikmaakt van CAAS.

Een algemene conclusie is dat er zeker een markt bestaat voor CAAS. Daarnaast kan, hoewel voorzichtig vanwege bovengenoemde beperkingen, geconstateerd worden dat binnen de geobserveerde markten sprake is van een groei. Daarbij is de meest populaire vorm van CAAS de cash-out diensten, welke voorzien in het illegaal verkrijgen van financiële middelen.

6 Conclusie en discussie

Auteurs: *Marinus Beerthuizen, Take Sipma en André van der Laan*

In het huidige rapport zijn inzichten in de aard en omvang van slachtoffer- en daderofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland uiteengezet. Daarvoor is een multimethode en –bronnen aanpak gehanteerd. Zo is er een systematische literatuurstudie uitgevoerd, aangevuld met snowball-sampling, zodat een volledig en hedendaags overzicht is verkregen over wat bekend is over de te onderzoeken fenomenen. Daarnaast zijn er in meerdere deelstudies empirische gegevens verzameld over de mate waarin cyber- en gedigitaliseerde criminaliteit geregistreerd is in traditionele bronnen van politie en justitie. Ook is informatie uit bronnen die onafhankelijk zijn van politie- en justitiële inspanningen gehaald, namelijk zelfrapportage van slachtoffer- en daderofferschap. Verder is onderzocht wat nieuwere methoden kunnen bijdragen aan de kennis over de mate waarin cyber- en gedigitaliseerde criminaliteit Nederlanders raakt. Zo zijn webscraping naar aanbieders van cybercrime-as-a-service op onlinemarkten en geautomatiseerde zoekopdrachten naar online bedreiging van openbaar bestuur besproken. In dit hoofdstuk wordt antwoord gegeven op de drie onderzoeksvragen en een discussie gevoerd over de gevonden inzichten.

6.1 Beantwoording 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?*

Onderzoeksvragen 1 en 2 betreffen de conceptualisatie en operationalisatie van hoe cyber- en gedigitaliseerde criminaliteit gerepresenteerd worden in bronnen. Omdat conceptualisatie en operationalisatie in elkaars verlengde liggen, worden beide onderzoeksvragen tegelijkertijd beantwoordt.

Iedere bron eigen kijk op slachtoffer- en daderschap cyber- en gedigitaliseerde criminaliteit
Het ligt voor de hand om slachtoffer- en daderschap op het niveau van het individu te bepalen—slachtoffers en daders. Dit is iets wat in de onderzochte bronnen ook het meest naar voren komt. Bij slachtofferschap gaat het grotendeels om zelfgerapporteerde slachtoffers, naast politieregistraties van meldingen en aangiftes. Daarnaast worden personen gezien als dader zoals met zelfrapportage of officiële registratie van daderschap (of verdachteschap) is vastgesteld. Populatieprevalenties lijken daarbij de standaard om slachtoffer- en daderschap te schatten (d.w.z., een percentage slachtoffers of daders in de onderzochte populatie). Zo meet de CBS Veiligheidsmonitor slachtofferschap in percentages 15-jarigen en ouder en de Monitor Zelfgerapporteerde Jeugdcriminaliteit meet daderschap in percentages jongeren van 10 tot en met 22 jaar. Een voordeel van dergelijke percentages uit deze bronnen is dat ontwikkelingen door de tijd goed te vergelijken zijn en representatief zijn voor de Nederlandse bevolking in die betreffende jaren. Prevalentiecijfers bieden niet direct zicht op het absolute aantal daders of slachtoffers, maar kunnen wel naar absolute cijfers vertaald worden, hoewel dit weinig gebeurd. Daarnaast zijn

er bronnen die voornamelijk absolute statistieken geven, zoals de aantallen strafzaken in RAC-min. Absolute aantallen in statistieken kunnen informatief zijn betreffende de last of druk die cyber- en gedigitaliseerde criminaliteit hebben op, bijvoorbeeld, (overheids)instanties die zich bezighouden met het vervolgen van daders of ondersteunen van slachtoffers.
Iedere bron heeft zijn eigen conceptualisering en operationalisering van de aard van cyber- en gedigitaliseerde criminaliteit. Dat geldt voor de meer algemene conceptualisatie, zoals welke gedragingen tot cyber- en gedigitaliseerde criminaliteit gerekend (kunnen) worden, als preciezere aard, zoals impact of ernst. Delicten die structureel in meerdere bronnen bevraagd zijn betreffen: hacken; DDoS-aanvallen; malware verspreiden (voornamelijk computervirussen); online bedreiging en aanverwante delicten cyberpesten en verspreiding seksueel beeldmateriaal); verschillende varianten van online fraude, zoals identiteitsfraude, phishing, bankpas- en creditcardfraude, en aan- en verkoopfraude.

Cyber- en gedigitaliseerde criminaliteit gemeten door middel van korte omschrijvingen en afleidingen uit justitiële registraties
Er zijn twee manieren waarop de aard van (dergelijke) cyber- en gedigitaliseerde criminaliteit wordt geoperationaliseerd. Namelijk, een korte omschrijving van een delict, of (indirecte) afleiding uit justitiële registratie. Bij afleiding uit justitiële registraties wordt gebruikt gemaakt van maatschappelijke kwalificaties of wetsartikelen. De maatschappelijke kwalificatie die als enige gebruikt wordt in alle geraadpleegde bronnen is die van computervredebreuk. De relevante wetsartikelen voor cyber- en gedigitaliseerde criminaliteit zijn verkregen uit eerder onderzoek (zoals Sr138a/Sr 138ab voor computervredebreuk; zie bijlage 2 voor een volledig overzicht). Dergelijke informatie geeft weinig inzicht in de aard van een specifiek delict. Voor meer details qua aard, zoals type gedragingen, zou dan in processenverbaal of rechtbankvonnissen gekeken moeten worden. Voor gedigitaliseerde criminaliteit is het mogelijk om op basis van wetsartikel onderscheid te maken tussen gedigitaliseerde zedencriminaliteit en andere vormen van gedigitaliseerde criminaliteit (waarmee dan voornamelijk fraude wordt bedoeld). Vergeleken met daderschap is voor slachtofferschap meer bekend over verschillende vormen van cyber- en gedigitaliseerde criminaliteit. Zo wordt er in slachtofferenquêtes gevraagd naar diverse vormen van online fraude, zoals phishing, fraude met bankpassen en creditcards en virtuele diefstal. Voor daderschap beperkt dit zich tot voornamelijk aan- en verkoopfraude en in mindere mate identiteitsfraude.

Dat de informatie over de aard van slachtoffer- en daderschap in veel bronnen beperkt is, is niet verwonderlijk. Bij enquêtering blijft diepgang qua aard vaak achterwege, omdat de aard vaak wordt geoperationaliseerd als korte omschrijving van een gedraging (met eventueel enkele vervolgvragen). Dat het vaak bij een korte omschrijving blijft is noodzakelijk om de vragenlijst in omvang te beperken en de begrijpelijkheid te vergroten. Ook zorgt de behoefte aan beperkte omvang en begrijpelijkheid ervoor dat een beperkt aantal items voorgelegd kan worden aan een respondent. Hierdoor kunnen ook niet alle denkbare vormen van cyber- en gedigitaliseerde criminaliteit bevraagd worden in een enkel onderzoek. Daarnaast zijn statistieken die een landelijk beeld geven vaak oppervlakkig vanuit het doel dat ze dienen: kwantitatief meten en bij voorkeur over langere tijd (‘een beetje weten over veel datapunten’). Ook zijn dergelijke registratiesystemen voornamelijk operationele systemen bedoeld voor primaire processen als opsporing en vervolging en niet bedoeld om kwantitatief onderzoek op te verrichten.

Bij slachtofferenquêtes wordt soms gevraagd naar ondervonden schade of last—hoe ernstig is het slachtofferschap of hoe ernstig is deze ervaren? Wanneer geen of weinig schade wordt ervaren, zou gesproken kunnen worden van minder ernstige criminaliteit, in vergelijking met wanneer wel veel schade is ervaren. Ook zou het wel of geen aangifte doen een implicatie kunnen zijn van ernst, hoewel andere zaken zoals ervaren schaamte of aangiftegemak daarbij ook een rol spelen. Ook op grotere schaal kunnen rapporten van banken over geleden financiële schade inzichten geven in de ernst van ondervonden slachtofferschap van skimmen of andere vormen van financiële fraude.

Eén van de kenmerken van de aard van geregistreerd daderschap waar iets meer over gezegd kan worden is strafrechtelijke ernst. Binnen registratiebronnen zijn er kenmerken die aangehaald kunnen worden voor de ernst van gedrag, namelijk de maximale strafdreiging van het zwaarste delict binnen de strafzaak en de werkelijk opgelegde straf. Dit laatste kan op twee manieren bekeken worden: in termen van celdagequivalenten en aanwezigheid onvoorwaardelijke vrijheidsstraf (de zwaarste primaire straf binnen het Nederlands rechtssysteem). Het idee is dat hoe hoger de opgelegde straf, hoe ernstiger het gedrag, evenals dat gedrag dat wordt bestraft met een vrijheidsstraf ernstiger is dan gedrag dat met een andere straf wordt afgedaan. Over het algemeen lijkt de (strafrechtelijke) ernst van strafzaken waarin cyber- en gedigitaliseerde criminaliteit behandeld worden toe te nemen in de periode 2008 tot en met 2018—straffen worden zwaarder en de maximale strafdreiging lijkt ook toe te nemen. Dit laatste kan komen doordat door de tijd heen strafzaken cyber- en gedigitaliseerde delicten steeds vaker relevante wetsartikelen betreft met een hogere strafdreiging, of dat andere ernstige offline delicten steeds vaker onderdeel gaan uitmaken van dergelijke strafzaken.

Bronnen die langere tijd structureel en frequent rapporteren, zoals justitiële registratiebronnen, bieden minder zicht op actuele ontwikkelingen. Meer inzichtelijke bronnen over slachtofferschap rapporteren minder frequent. Zo geeft de CBS Veiligheidsmonitor vanaf 2012 tot en met 2017 jaarlijkse inzichten over cyber- en gedigitaliseerde criminaliteit, maar niet over jaren daarvoor en over de jaren daarna tweejaarlijks. Het LISS-panel gaat wel iets verder terug in de tijd wat betreft het meten van cyber- en gedigitaliseerde criminaliteit, maar rapporteert niet jaarlijks. Ook zijn er bronnen die incidenteel onderzoek betreffen. Gezien de snelle ontwikkelingen binnen cybercriminaliteit kan een beperkte meetfrequentie ervoor zorgen dat nieuw opkomende gedragingen pas onderzocht worden als zij alweer op hun retour (kunnen) zijn. Het is niet zozeer dat over specifieke vormen van cyber- en gedigitaliseerde helemaal niks bekend is, maar meer dat er door de tijd heen nog wel gaten zijn vanaf 2008. Over het algemeen is er meer bekend over recentere jaren.

Samenvattend, de aard van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland is grofweg op twee manieren geconceptualiseerd en geoperationaliseerd in de bestudeerde bronnen. Ten eerste gaat het om korte omschrijvingen van type delicten waar van men slachtoffer of dader van is. Ten tweede gaat het om afleidingen uit justitiële registraties. Veel meer dan oppervlakkige informatie over de aard gaan de meeste bronnen vaak niet, ook omdat ze daarmee wel aan hun doel tegemoetkomen—frequent een globaal overzicht geven. De prevalentie van slachtoffer- en daderschap zijn voornamelijk concreet geoperationaliseerd als percentage slachtoffers en daders binnen een specifieke populatie. Enkele andere teleenheden komen ook voor in de onderzochte bronnen.

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

Er is niet één overkoepelend antwoord te geven op de vraag hoe groot slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland geschat wordt. Dit wordt duidelijk uit de uiteenlopende ranges en teleenheden betreffende slachtoffer- en daderschap die besproken zijn in dit rapport. Ter illustratie kijken wij naar 2015 en omliggende jaren, omdat meerdere bronnen deze jaren betreffen wanneer het gaat om slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in het algemeen.

Variatie in omvang naar verschillende bronnen
Rond 2015 zien wij voor slachtofferschap van cyber- en gedigitaliseerde criminaliteit uiteenlopende cijfers. De prevalentie van Nederlands slachtofferschap ligt in twee bronnen wel relatief dicht bij elkaar, namelijk 11% in 2015 volgens de CBS Veiligheidsmonitor en 8-10% in, respectievelijk, 2014 en 2016 volgens het LISS-panel. Zelfrapportage van jeugdig slachtofferschap ligt in 2015 volgens de MZJ hoger. Daar rapporteert, afhankelijk naar leeftijdscategorie, 16-37% van de jongeren slachtoffer te zijn geweest van ten minste één vorm van cyber- of gedigitaliseerde criminaliteit (hoewel dit relatief hoge percentage komt door het percentage ontvangen van een computervirus dat schade aanrichtte). Via textmining methodiek is geschat dat er een jaar later in 2016 ongeveer 136.000-318.000 politieregistraties zijn met cyber- en/of gedigitaliseerde criminaliteit.

In 2015 is de prevalentie van zelfgerapporteerd jeugdig daderschap van cybercriminaliteit 7-22% en van gedigitaliseerde criminaliteit 4-13%. Ter contrast betreft het aantal verdachten bij de politie en het OM in 2015 tussen de ruim 120 en bijna 200 individuen. Verder telt in datzelfde jaar de instroom van strafzaken met cyber- en gedigitaliseerde criminaliteit bij het OM, respectievelijk, 140 en bijna 500 zaken. Van die instroom zijn er uiteindelijk, respectievelijk, ruim 60 en bijna 260 zaken door de rechter in eerste aanleg afgedaan met een schuldigverklaring.

Variatie in omvang door de tijd heen
Bij slachtofferschap is ook variatie door de tijd heen bij prevalentie. Bij de CBS Veiligheidsmonitor varieert zelfgerapporteerd slachtofferschap van 11-13% in de periode 2012 tot en met 2019, terwijl bij het LISS-panel de prevalentie sterker varieert tussen de 8-15% in de periode 2010 tot en met 2018 (vanwege verschillen in welke delicten gemeten worden). Bij daderschap is ook variatie door de tijd heen merkbaar. Vanaf 2008 neemt het aantal politie en OM verdachten cybercriminaliteit toe van ruim 70 personen tot bijna 430 in 2019. De instroom van strafzaken met cybercriminaliteit bij het OM neemt in de periode 2008 tot en met 2018 toe van bijna 90 naar ruim 280 zaken, terwijl het aantal strafzaken met gedigitaliseerde criminaliteit (niet jaarlijks) afneemt van ruim 540 naar ruim 360. Ook laat het aantal strafzaken dat wordt afgedaan door de rechter met een schuldverklaring eenzelfde patroon zien in deze periode—van bijna 20 tot ruim 70 strafzaken betreffende cybercriminaliteit en van bijna 370 tot ruim 170 strafzaken betreffende gedigitaliseerde criminaliteit. Deze ontwikkelingen vinden plaats terwijl tegelijkertijd het aantal strafzaken in het algemeen dalend is.

Variatie in omvang naar type cyber- of gedigitaliseerd delict
Verder is er variatie naar type delict. Een veel voorkomende vorm van slachtofferschap is malware. Zo zegt 2-14% van de respondenten uit het LISS-panel een schadelijk computervirus te hebben gehad, evenals 6% van de mensen bevraagd

in het CBS ICT onderzoek. Maar dit zijn nog relatief lage percentages vergeleken met de MZJ, waar 8-27% van de jongeren aangeeft een schadelijk virus te hebben ontvangen in het voorgaande jaar en in de Eurobarometer uit 2014 loopt de zelfrapportage van slachtofferschap malware zelfs op tot 62%. Een mogelijke verklaring voor dit laatste hoge percentage is dat in de Eurobarometer niet expliciet gevraagd is of er sprake is van schade. Verder is het percentage besmette computers geschat op 24-38% in de periode 2009 tot en met 2015. De minst voorkomende vormen van slachtofferschap betreft online fraude. Zo komt uit meerdere bronnen naar voren dat minder dan 1% van de bevraagde personen slachtoffer zegt te zijn van, bijvoorbeeld, verkoopfraude, wangirifraude of identiteitsfraude. Een uitzondering hierop is aankoopfraude met zelfrapportage percentages tussen de 2-5% en waarvan het percentage slachtoffers ook nog eens toeneemt door de tijd heen.

Hacken (ongespecificeerd) is de meest voorkomende variant bij zelfgerapporteerd daderschap onder jeugdigen met 6-18% van de jongeren (hoewel hacken met manipulatie of het veranderen van iemands wachtwoord beduidend minder voorkomen met, respectievelijk, 1-5% en 1-7%). Bij dezelfde jeugdige populatie is de zelfrapportage prevalentie lager voor het versturen van virussen, uitvoeren van DDoS-aanvallen en fraude met aan- en verkoop, respectievelijk, rond de 1%, 0-2% en 0-3%. Variatie in het voorkomen naar type delict zien wij ook in politieregistraties. Hacken, ransomware en DDoS-aanvallen komen ieder afzonder naar schatting in tussen de 2.000 en 4.000 registraties voor, terwijl de geschatte aantallen registraties van afzonderlijke vormen van gedigitaliseerde criminaliteit, zoals online bedreiging en aan- en verkoopfraude, tussen de 34.000 en 120.000 registraties betreffen.

Variatie in omvang binnen trechtermodel van criminaliteit
Als laatste is er ook variatie door het trechtermodel heen (zie figuur 1). Over het algemeen laten bronnen die zich hoog in de trechter bevinden een grotere omvang zien, dan de bronnen die zich lager in de trechter bevinden. Deze discrepanties in omvang zijn in de lijn der verwachting uiteengezet in het eerste hoofdstuk, maar hebben wel als gevolg dat uitspraken over omvang apart gedaan zouden moeten worden voor de verschillende lagen van het trechtermodel. Dit wordt mooi geïllustreerd in de cijfers betreffende hacken.

Ongeveer 5% van de Nederlanders rapporteert slachtoffer te zijn geweest van hacken in 2015. Daarnaast suggereert zelfrapportage onderzoek onder jongeren dat 1-18% van de strafrechtelijk vervolgbare jongeren gehackt heeft in het jaar voorafgaande aan bevraging in 2015. Dit zou zich in absolute aantallen vertalen naar honderdduizenden slachtoffers en alleen al tienduizenden jeugdige daders. Lager in het trechtermodel suggereren bronnen in de jaren rond 2015 een kleinere omvang van hacken. Zo zijn er naar schatting via textmining slechts 3.710 politieregistraties waarin hacken ter sprake komt in 2016. Daarnaast blijkt uit politiecijfers dat er in 2015 en omliggende jaren rond de 200 verdachten van computervredebreuk worden geregistreerd. Oftewel, de geschatte omvang van hacken door het trechtermodel heen begint op honderdduizenden slachtoffers en tienduizenden daders, slinkt daarna af naar duizenden registraties bij de politie, om vervolgens te eindigen op slechts honderden verdachten.

Geen eenduidig beeld omvang slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland
Het mag duidelijk zijn—er is veel variatie in de gerapporteerde omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit. Deze variatie komt

tenminste deels voort uit de relatieve versplintering van het concept cyber- en gedigitaliseerde criminaliteit per bron. Niet iedere bron kijkt naar alle vormen van cyber- en gedigitaliseerde criminaliteit, waardoor uitspraken zich grotendeels beperken tot enkele typen individuele delicten. Ook is niet bij iedere bron bekend welke gedragingen het precies bevat, waardoor niet duidelijk is waar omvangcijfers over gaan (zoals bij de precieze inhoud van strafzaken). Daarnaast heeft ook niet iedere bron dezelfde teleenheid (zoals bijvoorbeeld de discrepantie tussen personen en strafzaken) en produceren meer innovatieve methoden teleenheden die moeilijk of niet te herleiden zijn naar de meest basale eenheid van slachtoffer- en daderschap—het individu. Ook verschilt de omvang per jaar en of gekeken wordt naar slachtoffer- of daderschap. Deze variatie maakt het niet mogelijk om een overkoepelend antwoord te geven op de vraag wat de omvang is van bekend Nederlands slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit (om nog maar niks te zeggen over de omvang van het onbekende, het zogeheten dark number).

6.2 Discussie methoden

Hoewel nieuwe methoden (zoals textmining) of bronnen (zoals onlinemarkten en sociale media) frisse blikken op criminele fenomenen kunnen bieden, is het lastig of niet mogelijk om dergelijk onderzoek empirisch te synthetiseren met, of te valideren door middel van, traditionele methoden. Immers, hoewel sommige zaken zoals onlineadvertenties wel meetbaar zijn, wijken de teleenheden dermate af van traditionele methoden dat een inhoudelijke vergelijking maken met traditioneel onderzoek moeilijk is. Daarnaast hebben deze methoden hun eigen unieke beperkingen, zowel inhoudelijk als technisch. Zo werd bij het onderzoek naar online bedreiging van burgemeesters binnen het onderzoeksproces duidelijk dat een (groot) aandeel van bedreigingen die via internet verstuurd worden onzichtbaar zijn voor het publiek. Daarnaast komt uit het onderzoek naar onlinemarkten naar voren dat, ondanks dat er sprake is van uniek meetbare accounts, er geen uitspraken gedaan kunnen worden over om hoeveel unieke aanbieders en afnemers van cybercrime-as-a-service. Omdat het beeld heerst dat nieuwe vormen van hogere technologische misdaad ook nieuwe vormen van hogere technologische methodiek vereisen voor bestudering, is het belangrijk om ook de tekortkomingen van dergelijke methoden en bronnen te beseffen. Daarbij komt dat dergelijke metingen ook alleen zin hebben als er een bekend referentiepunt is. Kort gezegd, schrijf traditionele methodieken zoals enquêtes en officiële registraties niet af.

Een beperking van het huidige onderzoek is de gebruikte methodes. Namelijk, bij de zoektocht naar literatuur is gebruikgemaakt van academische zoekmachines, aangevuld met snowball sampling. Dit laatste is noodzakelijk gebleken, omdat belangrijke publicaties niet via academische zoekmachines gevonden konden worden. Publicaties van het CBS of van het WODC zelf zijn hierin niet of moeilijk vindbaar. Maar, waar gebruikmaken van zoekmachines met een gestandaardiseerd protocol de kans op uitputtend literatuur vinden vergroot, is dat bij snowball sampling niet het geval. Het is aannemelijk dat sommige literatuur die zich buiten academische zoekmachines bevindt, maar wel relevant is voor dit rapport, niet gevonden zijn. Om te voorkomen dat belangrijke literatuur ontbreekt is daarom ook de expertise van de begeleidingscommissie ingezet. Desondanks kunnen wij geen garanties bieden dat alle relevante bestaande literatuur ook is opgenomen in dit rapport.

6.3 Afsluiting

Informatie en kennis over de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland is gefragmenteerd. Het huidige onderzoek voorziet in de behoefte dat deze kennis nu in een rapport gebundeld is. Een overkoepelend antwoord over de omvang van dergelijke criminaliteit blijft echter uit. 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, wat een belangrijke reden is waarom de beschikbare kennis gefragmenteerd is. Het is echter ook maar de vraag of uniformiteit mogelijk of wenselijk is gegeven de snelheid waarin de digitale ontwikkelingen zich voordoen. Immers, het kennisdomein is nog volop in ontwikkeling en vroegtijdig vastleggen in één concept of operationalisatie kan innovatie in de weg zitten en daarmee ook kennisverwerving belemmeren. De onduidelijkheid in welke mate verschillende bronnen hetzelfde bespreken maakt prioriteren wel lastig voor beleid en praktijk.

Het is wel duidelijk dat cyber- en gedigitaliseerde criminaliteit in Nederland een maatschappelijk probleem zijn. Jaarlijks ondervinden naar schatting honderdduizenden tot meer dan een miljoen Nederlanders enige vorm van slachtofferschap van cyber- en/of gedigitaliseerde criminaliteit. Het beeld dat dit fenomeen alleen maar groter zou zijn geworden door de tijd heen wordt echter niet door al het onderzoek ondersteunt. Sterker nog, algemeen slachtofferschap in twee longitudinale bronnen suggereert juist een relatieve stabiliteit of een daling. Daartegenover staat dat specifieke delicten, zoals online aan- en verkoopfraude, juist wel een duidelijke stijging laten zien. Ook binnen de justitiële keten is er steeds meer cybercriminaliteit in behandeling (maar niet noodzakelijk gedigitaliseerde criminaliteit, zover de bronnen hier zicht op hebben). Zo is er een duidelijk stijging in het aantal verdachten, ingestroomde aantal strafzaken en veroordelingen betreffende cybercriminaliteit.

Verder doen cyber- en gedigitaliseerde criminaliteit doen als maatschappelijke problemen niet veel onder voor traditionele criminaliteit. Waar in de CBS Veiligheidsmonitor het jaarlijks slachtofferschap van cyber- en gedigitaliseerde criminaliteit op 11-13% wordt geschat in de periode 2012 tot en met 2019, betreft dit voor traditionele criminaliteit 14-20% in dezelfde periode (CBS, 2020a). Hoewel slachtofferschap van traditionele criminaliteit wel vaker voorkomt, is het wel een afnemend fenomeen, terwijl slachtofferschap cyber- en gedigitaliseerde criminaliteit mogelijk stabiliseren. Maar ook aan de kant van (jeugdig) daderschap is duidelijk dat beide vormen criminaliteit naast elkaar bestaan. De MZJ 2015 laat zien dat de prevalentie van zelfgerapporteerd daderschap van cyber- en/of gedigitaliseerde criminaliteit 8-26% is, terwijl deze voor traditionele criminaliteit 20-37% is (Van der Laan & Beerthuizen, 2016). In een laatste opzicht waaruit blijkt dat beide vormen criminaliteit overeenkomsten hebben zijn de obstakels bij het bepalen van de aard en omvang. De genoemde zaken van fragmentarische kennis cyber- en gedigitaliseerde criminaliteit naar verschillende bronnen, type gedragingen en slachtoffer- versus daderschap komen vermoedelijk ook voor bij traditionele criminaliteit, evenals moeilijkheden met schattingen van dark numbers (zie ook Smit et al., 2019a, 2019b). Iets waar wel een duidelijk verschil in zit is de trechterwerking van de justitiële keten op de omvang van deze vormen van criminaliteit. De trechter heeft namelijk een sterker afslankend effect op de omvang van cyber- en gedigitaliseerde criminaliteit—in termen van waargenomen omvang van zelf-

gerapporteerd naar strafrechtelijk daderschap— vergeleken met traditionele criminaliteit (Van der Laan et al., 2016).

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 registreren en te meten. Hierbij moet niet alleen gedacht worden aan hoe te meten, maar ook wat te meten. Bijvoorbeeld, cyberpesten wordt soms meegenomen in het totaalbeeld cyber- en gedigitaliseerde criminaliteit. Ondanks dat het antisociaal gedrag is dat schade toebrengt bij slachtoffers (en een serieus maatschappelijk probleem is), is het niet noodzakelijk crimineel gedrag. Daarmee valt pesten buiten strafrechtelijke gedrag in het justitiële domein. Afhankelijk van de insteek van beleid, is het aan of juist af te raden dergelijk gedrag te belichten.

Voor de aanpak van cyber- en gedigitaliseerde criminaliteit is het verder belangrijk om goed de vinger aan de pols te houden betreffende nieuwe vormen van dergelijke criminaliteit, hoe deze met elkaar en met traditionele criminaliteit verweven zijn en in welke contexten die zich voordoen. Om in te kunnen spelen op 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 op alleen maar actuele criminaliteit moet zijn. Hiermee loopt men immers het risico aanpakken te ontwikkelen die mogelijk niet meer relevant zijn tegen de tijd dat ze geïmplementeerd kunnen worden, omdat de gedraging zich dan niet meer voordoet.

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 textmining (zie Tollenaar et al., 2019) of andere innovatieve technieken. Het grote gebrek bij dergelijke registratiesystemen zit hem niet in de beschikbaarheid van allerlei detailinformatie op veel meetpunten, maar op het (makkelijk) herkennen van relevante cyber- en gedigitaliseerde criminaliteit. Anders gezegd, binnen in het justitiële domein is al veel tekstuele data beschikbaar, maar nog nauwelijks ontsloten (Van der Laan & Tollenaar, 2019).

Ten tweede, blijf investeren in expertise over cyber- en gedigitaliseerde criminaliteit in de justitiële keten (zie ook Boekhoorn, 2020). 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 heben, zoals aangiftebereidheid of het potentieel internationale kenmerk van cyber- en gedigitaliseerde criminaliteit. 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 kan bijdragen aan dat het fenomeen van cyber en gedigitaliseerde criminaliteit adequaat kan worden opgepakt.

Summary

Nature and magnitude of cybercrime victimization and offending in the Netherlands'

Cybercrime is a serious issue in the Netherlands—estimations suggest that hundreds of thousands become victims of cybercriminals on a yearly basis. Hence, cybercrime is a hot topic for law enforcement and in politics. Two forms of cybercrime are distinguished. Firstly, cyber-dependent crime, in which both modus operandi and target concern information and communication technology (ICT). Examples for this first type of cybercrime are hacking and ransomware. Secondly, cyber-enabled crime, in which the modus operandi concerns ICT, but the target does not. Examples for this second type of crime are death threats via social media and online purchase and sales fraud (e.g., via Amazon).

Information on cybercrime victimization and offending in the Netherlands is available through self-report measures of victimization and offending, and registrations of law enforcement and private parties. In the current report this information is collected, clustered and presented in a coherent manner, thus providing an overview of the nature and magnitude of cybercrime victimization and offending in the Netherlands. The report concerns cybercrime from 2008 and forward.

This report contains answers to three research questions:

1 How is the nature of cybercrime victimization and offending conceptualized?
2 How are cybercrime victimization and offending operationalized?
3 What is the magnitude of cybercrime victimization and offending?

Conceptualization addresses what (experienced) behaviours and offenses are cybercrime, whereas operationalization concerns how these concepts are measured. Furthermore, the current report focusses on victimization of and offending by natural persons. Cybercrime exclusively between legal and/or state entities are beyond the primary scope. Victimization includes victimhood as experienced by individuals, and police reports of victimhood. Offending includes law enforcement registrations of suspects, offenders and crimes, as well as self-reported offending. Cybercrime is relevant when the offender and/or victim are Dutch. Moreover, cybercrime combated by Dutch law enforcement is relevant, even when there is not necessarily a Dutch offender or victim. The nature of cybercrime victimization and offending covers type, seriousness and impact, whereas magnitude concerns measures, such as percentage prevalence of victimhood or number of offenders and crimes.

This report is the result of a multi-method and multi-source approach using a systematic literature search, traditional empirical exploration of (registration) sources, and innovative methods applied to online platforms (i.e., social media and dark web forums).

Victimization

Cybercrime victimization in the Netherlands is mostly measured via self-report and police reports. The magnitude of victimization differs per type of offense, consulted source and population of interest.

8-15% of Dutch citizens victim of cybercrime, trends differ per source—relatively stable or decline

According to the Netherlands' Safety Monitor, the percentage of Dutch aged 15 years and older victimized by cybercrime declines from 12% to 11% in 2012-2017. In 2019, this percentage grows to 13%. In another study, the LISS-panel, the percentage of victimhood is initially 15% in 2010, which declines to 8% by 2018. Although both sources concern the same population, differences can occur through different methods and item questions. For instance, the Safety Monitor uses a new representative sample for each measurement, while the LISS-panel uses panel data (supplied with new respondents in case of attrition). In addition, the LISS-panel addresses computer virus infections, a steeply declining form of cybercrime victimization, whereas the Safety Monitor does not.

Cybercrime constitutes minority of police reports, though not negligible in absolute terms

Due to the limited amount of cybercrime victims reporting to the police (7-8%), only a fraction of all cybercrime victimization exists in police records. Textmining research on police reports from 2016 suggest that out 3.9 million registrations 4.000-25.000 of those concern cyber-dependent crimes, and 132.000-293.000 concern cyber-enabled crimes. Even though these numbers constitute a minority of all registrations, in absolute terms they are not negligible.

Malware most common form of cybercrime victimization

The prevalence of victimization differs per type of cybercrime and consulted source. Computer virus infections (i.e., malware) affect 2-62% of Dutch citizens, based on self-report measures. The large range is (likely) due to the inclusion or exclusion of explicit harm. When harm or damage is not included in the item description, prevalence rates are higher. Furthermore, 1-16% of Dutch citizens report hacking victimization, and 0-16% report some form of online fraud victimization. Moreover, 0-9% experience cyber harassment victimization, such as threats, bullying and distribution of private sexual images without consent. In police reports from 2016 online threats are the most common form of cybercrime, whereas hacking, ransomware and DDoS-attacks are much less prevalent. Lastly, reporting victimization to the police differs per type of cybercrime—online fraud shows higher report rates (12-22%) than hacking (2-3%).

Online threats against Dutch mayors largely hidden on social media

With social media and other online platforms, the distance between citizen and government has shrunk considerably, allowing for direct communication between the two—including harassment. On basis of an empirical study on traditional and social media, there is little found on why and how often Dutch mayors receive threats via Twitter and other online platforms. Exploratory research does suggest

three recurring themes of threats: organized crime and motorcycle gangs, dissatisfaction from individual citizens regarding governance, and other threats.

Offending

Cybercrime offending in the Netherlands is largely studied through law enforcement registrations and self-report measures. As with victimization, prevalence of offending differs per type of cybercrime and consulted source.

Limited information on cybercrime in law enforcement registrations

Only a few sources provide information on cybercrime offending in the Netherlands, often concerning estimates of number of offenders, criminal cases, registered crimes or investigations. Moreover, information on specific types of cybercrime is scarce, as law enforcement registration is mostly limited to computer trespassing. In addition, cyber-enabled crime can be registered under its traditional counterpart (e.g., online threats as "regular" threats), making them hard(er) to recognize.

Law enforcement shows limited, though increasing, numbers of cyber-dependent crime offending

Registrations by law enforcement suggest only a limited amount of cyber-dependent crime offending, though these numbers do increase over time. For instance, the number of suspects of cyber-dependent crime is approximately 70 in 2008, and increases to approximately 430 in 2019. Cyber-enabled crime, however, exhibits a decreasing trend. For example, the number of criminal cases handled by the Public Prosecution Services (PPS) goes from approximately 540 in 2008 to approximately 360 in 2018. Overall, cybercrime is less than 1% of all crime handled by law enforcement in terms of offenders and cases.

Cybercrime in criminal justice chain more serious through the years

Indicators of criminal severity suggest that cybercrime in the criminal justice chain is becoming more serious through the years—over time, judges punish cybercrime more severely and the maximum applicable punishment increases as well. For instance, in 2008-2014 the amount of cyber-dependent crime cases resulting in a mandatory prison sentence is at most approximately 30%, whereas in 2015-2018 these percentages range 34-47%. For cyber-enabled crime, these percentages go from 47% in 2008 to 83% in 2018.

Gap between self-reported cybercrime offending among youths and official registrations

Information on self-reported cybercrime offending is limited to the Dutch youth population. The prevalence of cyber-dependent offending among 10 through 22 years olds is, depending on age category, 7-22% in 2015. For cyber-enabled crime, the prevalence ranges 4-13%. Hence, a gap between tens of thousands self-reported juvenile cyber offenders and tens to hundreds of yearly officially registered offenders exists.

Cybercrime-as-a-service on the rise

Cybercrime-as-a-service (CAAS) concerns goods and services provided by cybercriminals to other criminals, who do not have the means to commit cybercrime by themselves. A textmining study on the supply of CAAS on dark web forums (e.g., AlphaBay) suggests that this phenomenon increases over time—during 2011-2017 both the number of advertisements and consumer responses regarding CAAS is up. However, due to methodological limitations, it is hard to interpret what the magnitude of CAAS on dark web forums really is.

Answering the research questions

1 How is the nature of cybercrime victimization and offending conceptualized?
2 How are cybercrime victimization and offending operationalized?

The consulted sources conceptualize and operationalize the nature of cybercrime victimization and offending in the Netherlands in two ways. Firstly, short descriptions of criminal behaviour in questionnaire items, and secondly, derivations from law enforcement registrations, such criminal codes or offence labels (i.e., computer trespassing). Operationalization of cybercrime victimization and offending usually concerns population percentages, though other measures exist, such as absolute numbers of offenders and criminal cases.

3 What is the magnitude of cybercrime victimization and offending?

There is no single answer to this question, as the ranges and units of measurement differ largely per type of offense, consulted source, and target population. For instance, in 2015, respectively, 7-22% and 4-13% of Dutch youths report to have committed a cyber-dependent or cyber-enabled offense. Meanwhile, cybercrime suspects in that same year number only between approximately 120 and 200 individuals. Moreover, youths compared to full population samples report more cybercrime victimization, cyber-dependent crime goes up, whereas cyber-enabled crime goes down, and malware infections are much more prevalent than online fraud. Hence, providing a single answer to the question of what the magnitude of cybercrime victimization and offending in the Netherlands is is (currently) not possible.

Conclusion and recommendations

For now, there is no uniformity in the conceptualization and operationalization of cybercrime. That said, it might be undesirable to obtain uniformity in the short run, as cybercriminology—as well as cybercrime itself—is still developing. Locking in too early on one concept or operationalization might hinder acquisition of knowledge later on.

It is clear that cybercrime is a serious issue in the Netherlands, with a significant amount of Dutch citizens becoming a victim every year. However, the belief that cybercrime is becoming an ever bigger problem is not necessarily supported by the data, as longitudinal sources on victimization suggest relative stability or a modest decline. Some specific cybercrimes, such as online purchase and sales fraud, do

show an increase over time. Also, the number of cyber-dependent offenders in the criminal justice chain increases as well.

Furthermore, cybercrime remains a serious issue, when compared to traditional crime. Although victimization of traditional crime is more prevalent than cybercrime, traditional victimization does show a steep decline, whereas cybercrime victimization might be stabilising.

This report contains two policy recommendations. Firstly, invest in the improvement and continued development of instruments to measure and register cybercrime victimization and offending. This does not only include how to measure, but also what to measure. Adequately reacting to novel cybercriminal developments requires policy makers to collaborate with institutions and experts that are able to detect novel forms of cybercrime in its early stages. Also, do not focus too narrowly on only novel forms of cybercrime, which may only briefly stay relevant. Within registration systems of law enforcement, development should not solely focus on expanding registration possibilities (e.g., more labels for different forms of cybercrime), but also on utilizing innovative methods on existing data. After all, law enforcement registration already does contain large amounts of detailed data (e.g., written police reports).

Secondly, keep investing in cybercrime expertise in the criminal justice chain. This report shows that cybercrime victimization is much more prevalent than criminal justice statistics suggest. This gap exists in part due to circumstances that the criminal justice chain cannot control, such as victim willingness to report. However, this gap is also in part due to controllable circumstances, such as available cybercrime expertise. Lack of cybercrime expertise in law enforcement might result in inadequate handling of victims' police reports, resulting in reports not progressing through the criminal justice chain, or being unrecognizable as cybercrime when progressing through the chain. Moreover, limited expertise might result in the misappraisal of severity, which could hinder detection and prosecution of cybercrime. Investing in cybercrime expertise in law enforcement will likely contribute to effective means of combating cybercrime in the Netherlands.

Literatuur

American Psychological Association (2008). Reporting standards for research in psychology: Why do we need them? What might they be? *American Psychologist,* 63, 839-851.

Akamai (2017). *Q2 2017 report*. Online via: https://blogs.akamai.com/index.html

Akamai (2018). *Summer SOTI web-attacks.* Online via: https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M.J.G. van, Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Berlijn: Springer.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. In *Proceedings of the 17th Workshop on the Economics of Information Security* (WEIS). Cambridge: Harvard University.

Beerthuizen, M.G.C.J., Leijsen, E.M.C. van, & Laan, A.M. van der (2019). *Risico- en beschermende factoren in de kindertijd en vroege adolescentie voor latere high impact crime in de latere adolescentie en jongvolwassenheid*. Den Haag: WODC. Cahier 2019-5.

Beerthuizen, M.G.C.J., Wartna, B.S.J., Verweij, S., & Tollenaar, N. (2015). *De misdrijf-straf index: Op weg naar een maat voor de ernst van delicten afgeleid van de afdoening van strafzaken.* Den Haag: WODC. Memorandum 2015-3.

Bennhold, K., & Eddy, M. (2020). *'Politics of Hate' takes a toll in Germany well beyond immigrants.* Online via: www.nytimes.com/2020/02/21/world/europe/germany-mayors-far-right.html

Boekhoorn, P. (2020). *De aanpak van cybercrime door regionale eenheden van de politie.* Den Haag: SDU/Politie & Wetenschap.

Bernaards, F., Monsma, E., & Zinn, P. (2012). *High tech crime: Criminaliteitsbeeld-analyse 2012*. Woerden: KLPD.

Binnenlands Bestuur (2018). *Burgemeester Aboutaleb ernstig bedreigd.* Online via: www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/burgemeester-aboutaleb-ernstig-bedreigd.9591209.lynkx

Binnenlands Bestuur (2019). *Steun voor bedreigde burgemeesters*. Online via: www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/steun-voor-bedreigde-burgemeesters.9607479.lynkx

Brady, P.Q., Randa, R., & Reyns, B.W. (2016). From WWII to the World Wide Web: A research note on social changes, online 'places', and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice, 32*(2)*,* 129-147.

BZK (2020). *Monitor Integriteit en Veiligheid 2020*. Online via: www.rijksoverheid.nl/documenten/rapporten/2020/07/02/monitor-integriteit-en-veiligheid-2020

Caballero, J., Grier, C., Kreibich, C., & Paxxon, V. (2011). Measuring pay-per-install: The commodization of malware distribution*.* In *Proceedings of the 20th USENIX Security Symposium*. Berkeley: USENIX.

CBS (2016). *ICT, kennis en economie 2016*. Den Haag: CBS.

CBS (2019a). *Internet; toegang, gebruik en faciliteiten*. Online via: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?fromstatweb

CBS (2019b). *Digitale veiligheid & criminaliteit 2018*. Den Haag: CBS.

CBS (2020a). *Veiligheidsmonitor 2019*. Den Haag: CBS.

CBS (2020b). *Geregistreerde criminaliteit; soort misdrijf, regio.* Online via: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1595585232679
Choenni, R., Braak, S.W. van den, & Platenburg, P.F.M. (2019). *Criminaliteit en Rechtshandhaving 2018*. Den Haag: WODC/RvdR/CBS. Cahier 2019-3.
Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*.* In *Proceedings of the World Wide Web Conference 2013*. Genève: IWWWCC.
Cooper, H., L.V. Hedges, and J.C. Valentine. 2009. *The handbook of research synthesis and meta-analysis* (*2nd ed)*. New York: Russell Sage Foundation.
CPB (2016). *Risicorapportage Cyberveiligheid Economie 2016*. Den Haag: CPB.
CPB (2018). *Risicorapportage Cyberveiligheid Economie 2018*. Den Haag: CPB.
Cuyper, R.H. de, & Weijters, G. (2016). *Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices*. Den Haag: WODC. Memorandum 2016-1.
Domenie, M.M.L., Leukfeldt, E.R., Toutenhoofd-Visser, M.H., & Stol, W.P. (2009). *Werkaanbod cybercrime bij de politie: Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercrime*. Leeuwarden: NHL Hogeschool Leeuwarden.
Domenie, M.M.L., Leukfeldt, E.R., Wilsem, J.A. van, Jansen, J., & Stol, W.P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving*. Den Haag: Boom Lemma.
Eeten, M.J.G. van, Asghari, H., Bauer, J.M., & Tabatabaie, S. (2011). *Internet service providers and botnet mitigation: A fact-finding study on the Dutch market*. Delft: TU Delft.
EMCDD/Europol (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy.* Lissabon/Den Haag: EMCDD/Europol.
Engelen, F., Roels, J., & Heij, V. de (2015). *Monitor Zelfgerapporteerde Jeugdcriminaliteit: Hoofdonderzoek 2015. Onderzoeksdocumentatie.* Heerlen: CBS.
ENISA (2016). *ENISA threat landscape report 2015*. Heraklion: ENISA.
ENISA (2017). *ENISA threat landscape report 2016*. Heraklion: ENISA.
ENISA (2018). *ENISA threat landscape report 2017*. Heraklion: ENISA.
ENISA (2019). *ENISA threat landscape report 2018*. Heraklion: ENISA.
Erhardt, C. (2020). *Kommunalpolitiker: Bedrohungen sind an der Tagesordnung: Umfrage-Ergebnisse.* Online via: https://kommunal.de/Kommunalpolitiker-umfrage-2020
Eurobarometer (2012). *Special Eurobarometer 390 cyber security*. Köln: GESIS.
Eurobarometer (2015). *Special Eurobarometer 423 cyber security*. Köln: GESIS.
Farrington, D.P., Jolliffe, D., Hawkins, J.D., Catalano, R.F., Hill, K.G., & Kosterman, R. (2003). Comparing delinquency careers in court records and self-reports. *Criminology, 41*(3)*,* 933-958.
Gehem, M., Usanov, A., Frinking, E., & Rademaker, M. (2015). *Assessing cyber security: A meta-analysis of threats, trends, and responses to cyber attacks*. Den Haag: The Hague Centre for Strategic Studies (HCSS).
Goodman, M. (2015). *Future Crimes*. New York: Doubleday.
Graaf, H. de, Bultinck, M., Brink, F. van den, Coehoorn, I., Borne, M. van den, Meijer, S. (2019). *Seks onder je 25e*. Utrecht: Rutgers/Soa AIDS Nederland/GGzE.
Gudkova, D., Vergelis, M., Shcherbakova, T., & Demidova, N. (2017). *Spam and phishing in Q3 2017.* Online via: https://securelist.com/spam-and-phishing-in-q3-2017/82901/

Holt, T.J., Wilsem, J. van, Weijer, S. van de, & Leukfeldt, E.R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2)*,* 187-206.
Jong, L., Leukfeldt, E.R., & Weijer, S. van de (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime. *Tijdschrift voor Veiligheid, 17*(1-2), 66-78.
Karami, M., Park, Y., & McCoy, D. (2016). Stress testing the booters: Understanding and under-mining the business of DDoS services*.* In *Proceedings of the 25th International Conference on World Wide Web* (pp. 1033-1043). Genève: IWWWCC.
Kerstens, J., & Jansen, J. (2016). The victim-perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-line victimization and perpetration. *Deviant Behavior, 37*(5), 585-600.
Kerstens, J., & Stol, W.P. (2012). *Jeugd en cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren*. Den Haag: Boom Lemma.
Kerstens, J., & Veenstra, S. (2013). Cyberpesten vanuit een criminologisch perspectief. *Tijdschrift voor Criminologie, 55*(4), 375-393.
Laan, A.M. van der, & Beerthuizen, M.G.C.J. (2016). Jeugdige zelfgerapporteerde daders. In A.M. van der Laan & Goudriaan (red.), *Monitor Jeugdcriminaliteit 2015* (pp. 23-50). Den Haag: WODC/CBS. Cahier 2016-1.
Laan, A.M. van der, & Beerthuizen, M.G.C.J. (2018). *Monitor Jeugdcriminaliteit 2017: Ontwikkelingen in de geregistreerde jeugdcriminaliteit in de jaren 2000 tot 2017.* Den Haag: WODC. Cahier 2018-1.
Laan, A.M. van der, Beerthuizen, M.G.C.J., & Weijters, G. (2016). Jeugdige daders van online-criminaliteit*. Cahiers Politiestudies*, 41, 145-168.
Laan, A.M. van der, & Blom, M. (2011). Zelfgerapporteerde daders. In A.M. van der Laan & M. Blom (red.), *Jeugdcriminaliteit in de periode 1996-2010* (pp. 23-50). Den Haag: WODC/CBS. Cahier 2011-2.
Laan, A.M. van der, & Goudriaan, H. (2016). *Monitor Jeugdcriminaliteit. Ontwikkelingen in de jeugdcriminaliteit 1997 tot 2015.* Den Haag: WODC. Cahier 2016-1.
Laan van der, A.M., & Tollenaar, N. (2019). Zelflerend algoritme vindt cybercrime in registraties. *Secondant*. Online via: https://ccv-secondant.nl/platform/article/zelflerend-algoritme-vindt-cybercrime-in-registraties
Laan, A.M. van der, & Tollenaar, N. (nog te verschijnen). Textmining for cybercrime in registrations of the Dutch police. In M. Weulen Kranenbarg & E.R. Leukfeldt (red.), *Cybercrime in context: The human factor in victimization, offending, and policing (Vol. Crime and justice in digital society)*. Cham: Springer.
Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers*. Den Haag: Sociaal en Cultureel Planbureau.
Lammers, J., & Edelenbosch, M. (2019). *Noord-Hollandse burgemeesters veelvuldig bedreigd.* Online via: https://ww.nhnieuws.nl/nieuws/236843/Noord-Hollandse-burgemeesters-veelvuldig-bedreigd
Leukfeldt E.R., Domenie M.L.L., & Stol, W. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische Uitgevers.
Leukfeldt, E.R., Veenstra, S., Domenie, M., & Stol, W. (2012). *De strafrechtketen in een gedigitaliseerde samenleving.* De Bilt/Leeuwaarden: PAC/NHL.
Leukfeldt, E.R., Kentgens, A., Prins, E., & Stol, W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor de intake van delicten met een digitale component*. Den Haag: Boom Lemma Uitgevers.
Level 3 (2015). *Safeguarding the internet*. Broomfield: Level 3.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children.* Londen: EU Kids Online Network.
McAfee (2015a). *McAfee Labs Threats Report: May 2015*. Santa Clara: McAfee.
McAfee (2015b). *McAfee Labs Threats Report: November 2015*. Santa Clara: McAfee.
McAfee (2016a). *McAfee Labs Threats Report: December 2016*. Santa Clara: McAfee.
McAfee (2016b). *McAfee Labs Threats Report: June 2016*. Santa Clara: McAfee.
McAfee (2016c). *McAfee Labs Threats Report: March 2016*. Santa Clara: McAfee.
McAfee (2016d). *McAfee Labs Threats Report: September 2016*. Santa Clara: McAfee.
McAfee (2017a). *McAfee Labs Threats Report: April 2017*. Santa Clara: McAfee.
McAfee. (2017b). *McAfee Labs Threats Report: June 2017*. Santa Clara: McAfee.
McAfee. (2018a). *McAfee Labs Threats Report: December 2018*. Santa Clara: McAfee.
McAfee. (2018b). *McAfee Labs Threats Report: June 2018*. Santa Clara: McAfee.
McAfee. (2018c). *McAfee Labs Threats Report: September 2018*. Santa Clara: McAfee.
Montoya, L., Junger, M., & Hartel, P. (2013). How 'digital' is traditional crime? Presentatie op de *2013 European Intelligence and Security Informatics Conference* (EISIC).
Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*. Den Haag: Rathenau Instituut.
NBIP (2017). *DDoS data rapport 2017.* Ede: Stichting Nationale Beheersorganisatie Internet Provider.
NBIP (2018). *DDoS data rapport 2018.* Ede: Stichting Nationale Beheersorganisatie Internet Provider.
NBIP (2019). *DDoS data rapport 2019*. Ede: Stichting Nationale Beheersorganisatie Internet Provider.
NCSC (2015). *Cybersecuritybeeld Nederland 2015*. Den Haag: NCSC.
NCSC (2017). *Cybersecuritybeeld Nederland 2017*. Den Haag: NCSC.
NCSC (2019). *Cybersecuritybeeld Nederland 2019*. Den Haag: NCSC.
NOS (2019). *Gevaarlijke hacktool offline na grote politieactie, hackers opgepakt*. Online via: https://nos.nl/artikel/2312554-gevaarlijke-hacktool-offline-na-grote-politieactie-hackers-opgepakt.html
NU.nl (2020). *Tag cybercrime*. Online via www.nu.nl/tag/cybercrime
NVB (2016). *Jaarverslag 2015*. Amsterdam: Nederlandse Vereniging van Banken.
NVB (2017). *Jaarverslag 2016*. Amsterdam: Nederlandse Vereniging van Banken.
NVB (2018). *Jaarverslag 2017*. Amsterdam: Nederlandse Vereniging van Banken.
NVB (2019). *Jaarverslag 2018*. Amsterdam: Nederlandse Vereniging van Banken.
Oksanen, A. & Keipi, T. (2013). Young people as victims of vrime on the internet: A population-based study in Finland. *Vulnerable Children & Youth Studies, 8(4)*, 298–309.
Openbaar Ministerie (2014). *Undercover onderzoek naar illegale marktplaatsen op internet.* Online via: www.om.nl/@32626/undercover-onderzoek/
PandaLabs (2009). *Annual report 2009.* Bilbao/Madrid: Panda Security.
PandaLabs (2011). *Annual report 2011*. Bilbao/Madrid: Panda Security.
PandaLabs (2012). *Annual report 2012.* Bilbao/Madrid: Panda Security.
PandaLabs (2013). *Annual report 2013*. Bilbao/Madrid: Panda Security.
PandaLabs (2014). *Annual report 2014*. Bilbao/Madrid: Panda Security.
PandaLabs (2015). *Annual report 2015*. Bilbao/Madrid: Panda Security.
Politie (2012). *High tech crime: Criminaliteitsbeeldanalyse 2012*. Driebergen: KLPD.

Politie (2017). *Ondergrondse Hansa Market overgenomen en neergehaald.* Online via: www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html
Politie (2019). *Jaarverantwoording 2018*. Driebergen: KLPD.
Politie (2020). *Meer misdrijven in 2019, daders steeds jonger.* Online via: www.politie.nl/nieuws/2020/januari/15/cijfers.html
PwC (2013). *2013-update onderzoek omvang van identiteitsfraude & maatschappelijke schade in Nederland*. Amsterdam: PwC.
PwC & VU (2014). *Cybercriminaliteit tegen Nederlandse organisaties: Een digitale dreiging.* Amsterdam: PwC/Vrije Universiteit Amsterdam.
Rijksoverheid (2017). *Eindrapportage criminele beïnvloeding van het lokale openbaar bestuur, en Monitor agressie en geweld 2018.* Online via: www.rijksoverheid.nl/documenten/rapporten/2017/10/05/rapport-criminele-beinvloeding-van-het-lokale-openbaar-bestuur
Ruiter, S., & Bernaards, F. (2012). Verschillen crackers van andere criminelen? Een vergelijking op basis van Nederlandse verdachtenregistraties. *Tijdschrift voor Criminologie, 55*(4), 342-359.
Sipma, T., & Leijsen, E.M.C. van (2019). *Slachtofferschap van online criminaliteit: Prevalentie, risicofactoren en gevolgen.* Den Haag: WODC. Cahier 2019-18.
Smit, P., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, Bongers, F. (2018a). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van criminaliteit te meten. Deel 1: Hoofdrapport.* Den Haag: WODC. Cahier 2018-21a.
Smit, P., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, Bongers, F. (2018a). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van criminaliteit te meten. Deel 2: Technisch rapport.* Den Haag: WODC. Cahier 2018-21b.
Spitters, M., Eendebak, P.T., Worm, D.T., & Bouma, H. (2014). Threat detection in tweets with trigger patterns and contextual cues. In *2014 IEEE Joint Intelligence and Security Informatics Conference* (pp. 216-219). Piscataway: IEEE.
Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *Proceedings of the 22nd USENIX Security Symposium* (pp. 33-48). Berkeley: USENIX.
Symantec (2010). *Internet threat security report 2009 (Vol. 14)*. Mountain View: Symantec.
Symantec (2012). *Symantec intelligence report: October 2012*. Mountain View: Symantec.
Symantec (2017). *Internet threat security report: Ransomware 2017*. Mountain View: Symantec.
Symantec (2018). *Internet threat security report (Vol. 23)*. Mountain View: Symantec.
Symantec (2019). *Internet threat security report (Vol. 24)*. Mountain View: Symantec.
Techzine (2014). *Nederlandse politie heeft Silk Road 2.0 servers in beslag genomen.* Online via: www.techzine.nl/nieuws/88597/nederlandse-politie-heeft-silk-road-2-0-servers-in-beslag-genomen.html
Tollenaar, N., Rokven, J.J., Macro, D., Beerthuizen, M.G.C.J., & Laan, A.M. van der (2019). *Predictieve textmining in politieregistraties*: *Cyber- en gedigitaliseerde criminaliteit*. Den Haag: WODC. Cahier 2019-2.
TrendLabs. (2015). *A rising tide: New hacks threaten public technologies*. Tokyo: Trend Micro.

Tubantia (2018). *Taakstraf voor ex-voorzitter Wiezo voor bedreiging burgemeester Robben.* Online via: www.tubantia.nl/wierden/taakstraf-voor-ex-voorzitter-wiezo-voor-bedreiging-burgemeester-robben~a91bb37f/
Unuchek, R., Sinitsyn, F., Parinov, D., & Liskin, A. (2017). *IT threat evolution Q2 2017.* Online via: https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/
Verburg, I. (2011). *Monitor Zelfgerapporteerde Jeugdcriminaliteit: Steekproef-trekking, nonresponsanalyse en weging* (BPA nr. 06-10-SOO). Den Haag: CBS.
Volkskrant (2020). *Voor hackers en phishers is het coronavirus een buitenkansje*. Online via: www.volkskrant.nl/wetenschap/voor-hackers-en-phishers-is-het-coronavirus-een-buitenkansje~b7b8b2dd/
Vries, W. de, Cranenburgh, A. van, Bisazza, A., Caselli, T., Noord, G. van, & Nissim, M. (2019). *BERTje: A Dutch BERT Model*. arXiv preprint arXiv:1912.09582.
Wegberg, R. van, Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganán, C., Klievink, B., Christin, N., & Eeten, M. van (2018). Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets. In *Proceedings of the 27th USENIX Security Symposium* (pp. 1009-1026). Berkeley: USENIX.
Weulen Kranenbarg, M., Holt, T.J., & Gelder, J.L. van (2019). Offending and victimization in the digital age: Correlates of cybercrime and traditional-only offending, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40-55.
Wilsem, J. van (2010). Digitale en traditionele bedreiging vergeleken. *Tijdschrift voor Criminologie 52*(1), 73-87.
Wilsem, J. van (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115-127.
Wilsem, J. van, Meulen, N. van der, & Kunst, M. (2013). Je geld kwijt, en dan? Financiële schade bij slachtoffers van onterechte bankafschrijvingen. *Tijdschrift voor Criminologie, 55*(4), 360-374.
Wired (2018). *Operation Bayonet: Inside the sting that hijacked an entire dark web drug market.* Online via: www.wired.com/story/hansa-dutch-police-sting-operation/
Zebel, S., De Vries, P., Giebels, E., Kuttschreuter, M., & Stol, W. (2012). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*. Enschede: Universiteit Twente/NHL Hogeschool/Politieacademie/Open Universiteit.

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter	
Prof. dr. Wouter Stol	NHL Hogeschool/Politieacademie
Leden	
Dr. Marleen Weulen Kranenbarg	Vrije Universiteit/NSCR
Dr. Maarten Cruyff	Universiteit Utrecht
Ton Eijken	ministerie van Justitie en Veiligheid; DSenJ

Bijlage 2 Methoden

Literatuurstudie

Het doel van de literatuurstudie is om een overzicht te bieden van de aard en omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit in Nederland. Literatuur over slachtofferschap en literatuur over daderschap is volgens dezelfde systematische zoektocht verzameld, gebaseerd op richtlijnen voor meta-analyses en reviews (American Psychological Association, 2008; Cooper, Hedges & Valentine, 2009). Het is belangrijk heldere inclusiecriteria te formuleren en transparante, repliceerbare zoekstrategieën te hanteren.

Inclusiecriteria

In deze studie zijn wetenschappelijke publicaties in peer-reviewed tijdschriften, evenals boekhoofdstukken en beleidsrapportages meegenomen. Verder zijn alleen publicaties vanaf 2008 meegenomen. Het belangrijkste criterium is dat een kwantificatie van de omvang van slachtoffer- en/of daderschap van cyber- en/of gedigitaliseerde criminaliteit in de Nederlandse context in de publicatie gerapporteerd wordt. Publicaties die alleen de aard van dergelijke criminaliteit onderzoeken zijn niet meegenomen (bijv., studies die alleen ingaan op juridische of technische aspecten van cyber- en/of gedigitaliseerde criminaliteit).

Zoekstrategie

De zoektocht om relevante studies te lokaliseren is tweeledig. Ten eerste zijn databases van wetenschappelijke literatuur doorzocht met vooraf opgestelde zoektermen (zie tabel B2.1). Dit leverde vooral wetenschappelijke literatuur op. Daarnaast is snowball sampling toegepast—literatuurlijsten van relevant bevonden studies doorzoeken naar nieuwe resultaten. Dit leverde voornamelijk vakpublicaties op.

Online databases

Er zijn meerdere databases gebruikt: JSTOR, SCOPUS, ScienceDirect en Web of Science. Om te bepalen welke zoektermen relevant zijn om deze databases mee te doorzoeken, is eerst een exploratieve zoektocht gedaan. Een zoekterm met daarin verschillende specifieke type delicten[12] leverde 8.378 resultaten op in Web of Science en 291.231 in JSTOR. Om de resultaten realistisch doorzoekbaar te houden is bepaald om losse delicten niet te specificeren in de zoektermen, maar alleen de algemene term 'cybercrim*' te gebruiken. De asterisk zorgt ervoor dat alle woorden die beginnen met de term (bijv., cybercrime en cybercrimineel) meegenomen worden, zonder dat deze apart gespecificeerd moeten worden.

Om te specifiëren dat studies die een kwantificatie rapporteren relevant zijn, zijn de volgende zoektermen ook toegevoegd: 'prevalence', 'incidence', 'costs' en 'harm'. Daarnaast betreft het huidige onderzoek cyber- en gedigitaliseerde criminaliteit in Nederland. Daarom dient ook ergens in de publicatie verwezen te worden naar

12 (cybercrim* OR cybersecurity OR gedigitaliseerde criminaliteit OR ransomware OR DDoS OR hack* OR malware OR ((online OR cyber OR internet) AND (harassment OR fraud)))

Nederland of Nederlanders. In JSTOR en ScienceDirect worden publicaties gelokaliseerd door de volledige tekst van de publicatie te doorzoeken. In dat geval is gekozen om de termen 'Netherlands', 'Dutch' of 'Holland' toe te voegen. In Web of Science en SCOPUS wordt alleen het topic (d.w.z., titel, abstract en trefwoorden) of het abstract doorzocht. Aangezien Nederland niet noodzakelijk in het abstract genoemd wordt, terwijl het wel in het artikel genoemd kan worden, zijn voor deze databases geen geografische zoektermen gebruikt. Om Nederlandstalige literatuur in kaart te brengen, zijn alle 203 wetenschappelijke artikelen tussen 2008 en 2018 in het Tijdschrift voor Criminologie beoordeeld op de inclusiecriteria. De gebruikte zoektermen zijn gepresenteerd in tabel B2.1.

Tabel B2.1 Zoektermen databases

Database	Zoektermen	Zoekvelden	*N* Hits
JSTOR	((cybercrim*) AND (prevalence OR incidence OR costs OR harm)) AND (Netherlands or Dutch or Holland)	Alle velden	186
JSTOR	(cybercrim*) AND (prevalence OR incidence OR costs OR harm)	Abstract	4
SCOPUS	(cybercrim*) AND (prevalence OR incidence OR costs OR harm)	Titel, abstract en keywords	190
SD	((cybercrime) AND (prevalence OR incidence OR costs OR harm)) AND (Netherlands or Dutch or Holland)	Volledige tekst	52
WoS	(cybercrim*) AND (prevalence OR incidence OR costs OR harm)	Onderwerp	50
WoS	(cybercrim*) AND (Netherlands or Dutch or Holland)	Onderwerp	19

SD = Science Direct, WoS = Web of Science

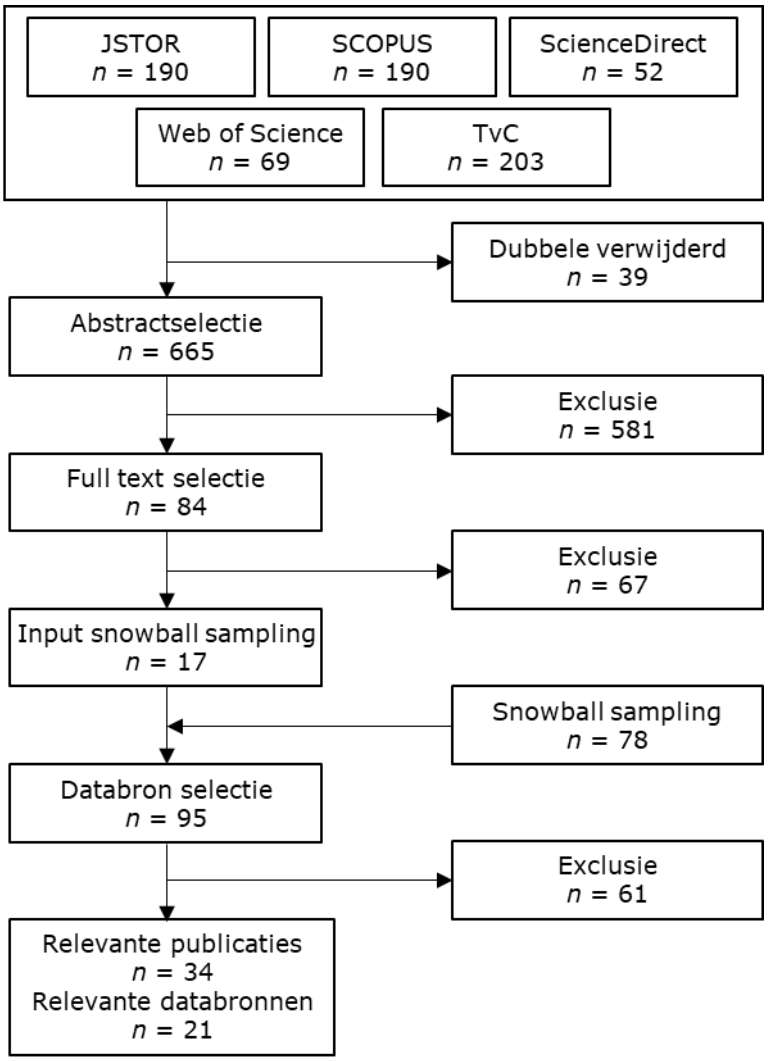
De zoektocht via internationale databases leverde 462 unieke studies op (zie figuur B2.1). Vervolgens is in twee stappen bepaald of ze aan de inclusiecriteria voldoen. Ten eerste is op basis van het abstract ingeschat of een studie relevant is en wanneer geen abstract beschikbaar is, gebeurt dit op basis van titel. Ter illustratie is de publicatie 'Investigating internet crimes' wel meegenomen, maar 'Encyclopedia of applied ethics (2nd edition) niet. Na deze evaluatie zijn 386 van de 462 niet relevant bevonden, met voornaamste reden dat het niet Nederlands slachtoffer- of daderschap ging of dat er geen kwantificatie is gerapporteerd. De abstracts van studies gevonden via Web of Science zijn dubbel gecodeerd om interbeoordelaars-betrouwbaarheid te berekenen (n=69). De inclusieselectie op basis van de abstracts was goed (κ=0,73). Daarna is in de volledige tekst gekeken of er daadwerkelijk een omvangschatting is gerapporteerd over slachtoffer- en/of daderschap van cyber- en/of gedigitaliseerde criminaliteit in Nederland. Veertien studies zijn uiteindelijk relevant bevonden. Bij het Tijdschrift voor Criminologie zijn zeven studies relevant bevonden.

Snowball sampling

De zoektocht via online databases heeft relatief weinig resultaten opgeleverd om een aantal redenen. Ten eerste betreft het vooral Engelstalige literatuur, waarbij in weinig gevallen gerapporteerd is over cyber- en/of gedigitaliseerde criminaliteit in Nederland. Daarnaast is in een groot deel van de geëxcludeerde publicaties geen kwantificatie gepresenteerd. Ten derde, als de publicaties wel gebruikmaken van kwantitatieve onderzoeksmethoden, dan betreft dit vaak verdiepende analyses (zoals verklarende analyses van oorzaken en gevolgen slachtoffer- of daderschap). Een eenvoudige omvangschatting wordt dan niet altijd gegeven.

Nederlandstalige en vakpublicaties zijn ondervertegenwoordigd in deze zoektocht, terwijl deze studies juist relevant kunnen zijn voor deze literatuurstudie. Om beter zicht te krijgen op de Nederlandstalige en vakliteratuur, is gebruikgemaakt van snowball sampling. Dit houdt in dat literatuurlijsten van eerder gevonden studies worden doorgenomen om nieuwe relevante literatuur te vinden. Aangezien eerder gevonden literatuur voornamelijk wetenschappelijke studies betreft, zal deze methode hoogstwaarschijnlijk nauwelijks vakpublicaties opleveren. Om deze vakpublicaties op systematische wijze toch te lokaliseren zijn een aantal recente vakpublicaties vooraf geselecteerd, en vervolgens zijn diens literatuurlijsten doorgenomen (namelijk, CBS, 2019b, 2020b; CPB, 2018; Munnichs et al., 2017; McAfee, 2018; Sipma & Van Leijsen, 2019; Symantec, 2019; Tollenaar et al., 2019). Het betreft rapporten van Nederlandse instanties die zich bezighouden met cyber- en gedigitaliseerde criminaliteit. Daarnaast zijn een aantal rapporten toegevoegd van private partijen die gespecialiseerd zijn in cybersecurity.

Figuur B2.1 Resultaten systematische zoekstrategie



Tabel B2.2 Gebruikte databronnen in literatuur

Databron	Korte beschrijving	Actor	Referenties
Akamai	Via Akamai antivirussoftware opgespoorde web application attacks vanuit Nederland en op Nederlandse systemen	S/D	Akamai (2017, 2018)
CBS Veiligheidsmonitor	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking van 15 jaar en ouder	S	CBS (2020b)
CBS Digitale Veiligheid & Criminaliteit	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking van 12 jaar en ouder	S	CBS (2019b)
CBS, ICT-gebruik huishoudens en personen	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking van 12 jaar en ouder	S	CBS (2016)
Centraal Meld- en Informatiepunt Identiteitsfraude en –fouten	Meldingen van slachtoffers van identiteitsfraude	S	PwC (2013)
Domenie et al. (2013)	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking	S	Domenie et al. (2013)
EU Kids online	Slachtofferenquete onder representatieve steekproef van jongeren van 9 tot en met 16 jaar in verschillende Europese landen, waaronder Nederland	S	Livingstone et al. (2011)
Eurobarometer	Slachtofferenquête onder representatieve steekproef van bevolking 15 jaar en ouder in verschillende Europese landen, waaronder Nederland	S	Eurobarometer (2012; 2015)
Jeugd en Cybersafety	Slachtoffer- en daderenquête onder representatieve steekproef van Nederlandse scholieren tussen 11 en 18 jaar	S/D	Kerstens & Stol (2012); Kerstens & Jansen (2016); Kerstens & Veenstra (2013)
LISS-panel	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking van 15 jaar en ouder	S	Sipma & Van Leijsen (2019)
NBIP	Meldingen van DDoS aanvallen	S	NBIP (2017; 2018; 2019)
NVB	Gegevens van Nederlandse Vereniging van Banken	S	NVB (2016; 2017; 2018; 2019)
PandaLabs	Via Panda antivirussoftware opgespoorde geïnfecteerde computers	S	PandaLabs (2009; 2011-2015)
Politieregistraties	Registraties van aangiften	S	NCSC (2015)
Politieregistraties	Registraties van misdrijven	D	CBS (2020b)
Politieregistraties	Registraties van opsporingsonderzoeken	D	Politie (2019)
Politieregistraties	Registraties van verdachten	D	CBS (2020b); Politie (2019); Ruiter & Bernaards (2013)
Politieregistraties	Textmining van politieregistraties	S/D	Tollenaar et al. (2019)
PwC Slachtofferenquête	Slachtofferenquête onder representatieve steekproef van Nederlandse bevolking	S	PwC (2013)
Rechtspraak.nl	Vonnissen van rechterlijke uitspraken	D	CPB (2016)
Van Eeten et al. (2011)	Onderzoek naar geïnfecteerde apparaten met Nederlands IP-adres. Gegevens zijn afkomstig van de volgende providers: Bbned, KPN, Online, Solcon, Tele2, UPC, XS4All, ZeelandNet en Ziggo.	S	Van Eeten et al. (2011)

Geselecteerde literatuur

De systematische literatuurzoektocht levert uiteindelijk 95 relevante publicaties op. Hoewel deze studies kwantificaties van cyber- en gedigitaliseerde criminaliteit rapporteren, blijkt bij nadere inspectie 61 studies geen relevante kwantificaties te bevatten. Dit heeft een aantal oorzaken. Ten eerste betreft een deel alleen cijfers van aard of ernst van cybercriminaliteit en geen landelijke omvang (bijv. Leukfeldt, Domenie en Stol, 2013). Ten tweede betreffen het cijfers over bedrijven of organisaties als slachtoffer, in plaats van Nederlandse natuurlijke personen (bijv. PwC & VU, 2014). Ten derde hebben sommige indicatoren betrekking op de dreiging van cybercriminaliteit in plaats van daadwerkelijke criminaliteit (bijv. ENISA, 2019). Deze studies leveren desalniettemin een indicatie van de mogelijke omvang van cyber- en gedigitaliseerde criminaliteit en zijn daarom besproken in diverse boxjes in hoofdstuk 3 en 5. Ten vierde zijn studies niet geïncludeerd, omdat ze geen unieke omvangcijfers presenteerden. Deze studies verwijzen naar een databron die al in een andere studie besproken is (bijv., Van Wilsem, 2011). Alleen studies met unieke informatie zijn geselecteerd. Studies die bijvoorbeeld omvangcijfers rapporteren, maar deze één-op-één uit andere rapportages halen, zijn niet meegenomen om overlap tegen te gaan. De databron waarnaar wordt geciteerd is tenslotte al via de snowball sampling geïncludeerd.

Tot slot hebben enkele studies gebruikt gemaakt van de Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ), die als eigen bron is opgenomen in dit rapport (zie verderop in deze bijlage). Omdat omvangstatistieken terug te brengen zijn naar databronnen in plaats van naar studies, worden deze statistieken per databron gepresenteerd in hoofdstuk 2 en 4. Zie tabel B2.2 voor een overzicht van de databronnen en de studies waarmee we ze hebben gelokaliseerd.

Codeerschema

Nadat publicaties met relevante databronnen gelokaliseerd en geselecteerd zijn, zijn publicaties gecodeerd op basis van een aantal indicatoren. Aangezien elke publicatie meerdere statistieken over omvang kan bevatten, worden per statistiek kenmerken gecodeerd. Dit bevat de statistiek zelf, met eventueel een betrouwbaarheidsinterval of standaarddeviatie, en kenmerken over de operationalisatie. Het doel hiervan is om verschillende statistieken te groeperen op basis van hun operationalisatie en/of conceptualisatie om een zo volledig mogelijk, maar tegelijkertijd gestructureerd, beeld te geven van de omvang van slachtoffer- en daderschap van cyber- en gedigitaliseerde criminaliteit.

Monitor Zelfgerapporteerde Jeugdcriminaliteit

De Monitor Zelfgerapporteerde Jeugdcriminaliteit (MZJ) is zelfrapportage onderzoek onder Nederlandse jongeren dat eens in de vijf jaar wordt uitgevoerd. Het gaat om jongeren in de leeftijd van 10 tot en met 22 jaar (waarbij de jongvolwassenen pas sinds de 2015 meting zijn toegevoegd). In de MZJ is aandacht voor slachtoffer- en daderschap van criminaliteit, waaronder ook cyber- en gedigitaliseerde criminaliteit. Het betreft dan slachtoffer- en daderschap in de twaalf maanden voorafgaand aan afname. In dit rapport wordt in mindere mate verwezen naar de 2010 meting (Van der Laan & Blom, 2011) en in meerdere mate naar de 2015 meting (Van der Laan & Beerthuizen, 2016). Dit omdat in de 2015 slachtoffer- en daderschap bevragingen

zijn toegevoegd met betrekking tot cyber- en gedigitaliseerde criminaliteit. In 2010 zijn er in totaal 3.030 jongeren bevraagd en in 2015 3.188 jongeren. Er zijn wegingsfactoren meegeleverd om de steekproef nationaal representatief te laten zijn voor de Nederlandse jeugdpopulatie op basis van leeftijd, sekse, herkomst, opleidingsniveau, stedelijkheidsgraad en landsdeel (Verburg, 2011; Engelen, Roels & De Heij, 2015).

Cyber- en gedigitaliseerde criminaliteit in de MZJ

Zelfgerapporteerd slachtofferschap van cyber- en gedigitaliseerde criminaliteit in het afgelopen jaar is gemeten aan de hand van zes items, waarvan er twee betrekking hebben op cybercriminaliteit en vier op gedigitaliseerde criminaliteit (zie tabel B2.3). Deze vragen zijn alleen gesteld in de 2015 meting. De wetsartikelen uit het Wetboek van Strafrecht waarop de delicten betrekking hebben, zijn weergegeven in de laatste kolom. Per item is aan de jongeren gevraagd of zij dit hebben meegemaakt in de afgelopen twaalf maanden. Wanneer zij aangeven dat dit het geval is, dan wordt per item de prevalentie op 'ja' gezet. Anders op 'nee'. Totaalscores voor cyber- en gedigitaliseerde criminaliteit apart en samen worden gebaseerd op dat ten minste één van de relevante items op 'ja' staat. Prevalentie wordt weergegeven met weging naar bovengenoemde kenmerken.

Tabel B2.3 Vraagstelling slachtofferschap MZJ

Delictsomschrijving	Vraagstelling	Wetsartikel
Cybercriminaliteit		
Virus	Is je computer, laptop, tablet of smartphone in de afgelopen 12 maanden weleens door een virus vastgelopen, kapot gegaan of gecrasht?	Sr 161sexies Sr 350a
Hacken	Heeft iemand met kwade bedoelingen in de afgelopen 12 maanden weleens ingebroken of ingelogd op een computer, e-mailaccount, website of profielsite (zoals Facebook of Twitter) van jou?	Sr 138ab
Gedigitaliseerde criminaliteit		
Online pesten	Ben je in de afgelopen 12 maanden weleens via internet getreiterd of gepest?	NVT
Online bedreiging	Ben je in de afgelopen 12 maanden weleens via internet bedreigd?	Sr 285
Seksueel beeldmateriaal verspreid	Heeft iemand in de afgelopen 12 maanden weleens seksueel getinte foto's of filmpjes van jou online gezet?	Sr 139e Sr 240b
Online aan- of verkoopfraude	Ben je in de afgelopen 12 maanden weleens opgelicht bij het kopen of verkopen van spullen of diensten via internet, bijvoorbeeld omdat de spullen of diensten niet werden geleverd of omdat iemand niet betaald heeft?	Sr 326c

Zelfgerapporteerd daderschap van cyber- en gedigitaliseerde criminaliteit in het afgelopen jaar is gemeten aan de hand van tien items in de 2015 meting, waarvan er vijf betrekking hebben op cybercriminaliteit en vijf op gedigitaliseerde criminaliteit (zie tabel B2.4)[13]. In de 2010 meting zijn slechts twee gedragingen bevraagd (namelijk, virus versturen en bedreigen via texting). Per item is eerst gevraagd of de jongere dit delict ooit heeft gepleegd, en zo ja, hoe vaak in de afgelopen twaalf maanden. Indien iemand ten minste één keer een delict gepleegd

13 Er zijn een tweetal items die wel bevraagd zijn in de MZJ2010 en MZJ2015, maar vanwege trivialiteit (voor het item illegaal downloaden van films, software, enz.) en onduidelijkheid van vraagstelling (voor het item voordoen als iemand anders op internet) achterwege gelaten worden.

heeft in het afgelopen jaar wordt de prevalentie van die persoon op 'ja' gezet. Anders op 'nee'. Totaalscores voor cyber- en gedigitaliseerde criminaliteit apart en samen worden gebaseerd op dat ten minste één van de relevante items op 'ja' staat. Prevalentie wordt weergegeven met weging naar bovengenoemde kenmerken.

Tabel B2.4 Vraagstelling daderschap MZJ

Delictsomschrijving	Vraagstelling	Wetsartikel
Cybercriminaliteit		
Virus versturen*	Heb je weleens met opzet via internet of per e-mail virussen rondgestuurd naar andere computers?	Sr 161sexies Sr 350a
Hacken	Heb je weleens ingelogd op een computer, e-mailaccount of sociale netwerksite van iemand anders zonder dat diegene hiervan wist?	Sr 138ab
Hacken met manipulatie	Heb je weleens op iemand anders zijn computer of profiel ingelogd en hier gegevens in veranderd of gewist zonder dat diegene daarvan wist?	Sr 138ab
Wachtwoord veranderen	Heb je weleens iemand zijn wachtwoord veranderd zodat diegene niet meer kon inloggen?	Sr 138ab
DDoS-aanval uitvoeren	Heb je weleens geprobeerd een website of een e-mailbox plat te leggen door enorme hoeveelheden informatie daarnaar toe te sturen?	Sr 138b
Gedigitaliseerde criminaliteit		
Bedreigen via texting*	Heb je weleens via een sms, e-mail of in een chatbox iemand een bericht gestuurd met de bedoeling hem of haar bang te maken?	Sr 285
Bedreigen via social media	Heb je weleens via andere sociale media zoals WhatsApp, Facebook, Twitter, Instagram of Snapchat iemand een bericht gestuurd met de bedoeling hem of haar bang te maken?	Sr 285
Artikel niet opsturen	Heb je weleens iets verkocht via internet, het geld gekregen van de koper, maar het artikel nooit opgestuurd?	Sr 326c
Geld niet overmaken	Heb je weleens iets gekocht en ontvangen via internet, maar nooit betaald?	Sr 326c
Seksueel beeldmateriaal van minderjarige verspreiden	Heb je weleens via internet of je telefoon seksueel getinte foto's of filmpjes verspreid van iemand anders terwijl diegene nog geen 18 jaar was?	Sr 139e Sr 240b

* Deze twee items zijn de enige twee bevragingen van cyber- en gedigitaliseerde criminaliteit in de 2010 meting; alle andere items komen alleen in de 2015 meting voor.

RAC-min

RAC-min is een systeem dat een proces-verbaal kan volgen tot dagvaarding en veroordeling en gaat over alle strafzaken die het Openbaar Ministerie (OM) in behandeling neemt. Naast informatie over hoe het OM ingestroomde strafzaken afdoet, bevat het ook gegevens over de berechting in eerste aanleg. De teleenheid binnen dit systeem is de strafzaak en in dit onderzoek wordt als tijdseenheid het jaar waarop de zaak instroomt bij het OM gehanteerd.

Cyber- en gedigitaliseerde criminaliteit in RAC-min

Strafzaken met daarin cyber- en gedigitaliseerde criminaliteit zijn geselecteerd op basis van wetsartikelen die relevant zijn voor deze twee vormen van criminaliteit. Sinds de invoering van de wetten computercriminaliteit zijn er wetsartikelen geschreven om verschillende vormen van cybercriminaliteit (en in mindere mate gedigitaliseerde criminaliteit) te vervolgen. In sindsdien uitgevoerd onderzoek zijn aanvullende wetsartikelen gevonden waarbij logischerwijs verondersteld kan worden dat het gros van vervolgde delicten onder dit wetsartikel cyber- of gedigitaliseerde criminaliteit zijn (Leukfeldt, Kentgens, Prins & Stol, 2015). Bijvoorbeeld, wetsartikel Sr 240b betreffende kinderpornografie. Waar eerst fysiek beeldmateriaal verkregen diende te worden, gaat de hedendaagse verspreiding veelal via internet. Daarmee wordt verondersteld dat delicten vervolgd onder wetsartikel Sr 240b (grotendeels) gedigitaliseerde criminaliteit zijn. Een selectie van cyber- en gedigitaliseerde delicten op basis van wetsartikelen is al eerder toegepast in (jeugd) onderzoek en monitoring (bijv., Van der Laan & Beerthuizen, 2018; Zebel, De Vries, Giebels, Kuttschreuter & Stol, 2012). De relevante wetsartikelen zijn weergegeven in tabel B2.5.

Tabel B2.5 Wetsartikelen cyber- en gedigitaliseerde criminaliteit

Wetsartikel	Korte omschrijving
Cybercriminaliteit	
Sr 138a	Hacking (alleen vooraf 24 juli 2010)
Sr 138ab	Hacking
Sr 138b	Belemmeren toegang/gebruik geautomatiseerd werk
Sr 139c	Aftappen of opnemen van gegevens
Sr 139d	Opname-, aftap- of afluisterapparatuur plaatsen
Sr 139e	Bezitten of verspreiden afgetapte gegevens
Sr 161sexies	Intentioneel vernielen van geautomatiseerd werk
Sr 161septies	Onbedoeld vernielen van geautomatiseerd werk
Sr 350a	Intentioneel vernielen van gegevens op geautomatiseerd werk
Sr 350b	Onbedoeld vernielen van gegevens op geautomatiseerd werk
Gedigitaliseerde criminaliteit	
Sr 231a	Identiteitsfraude met biometrische gegevens
Sr 232	Vervalsen digitale betaalmiddelen
Sr 240b	Kinderpornografie
Sr 248e	Grooming
Sr 273/1/2	Bekendmaking/heling bedrijfsgeheim
Sr 273d	Schending telecommunicatiegeheim
Sr 317/2	Afpersing onder dreiging vernieling digitale gegevens
Sr 326c	Misbruik publicatie telecommunicatiedienst

De omvangstatistieken betreft het absolute aantal strafzaken dat binnenstroomt bij het OM. Hierbij wordt voor cybercriminaliteit geen onderscheid gemaakt naar type delict, omdat de wetsartikelen dermate uniform geacht worden qua inhoud, dat een opsplitsing niet relevant is. Voor gedigitaliseerde criminaliteit wordt wel onderscheid gemaakt tussen twee vormen: gedigitaliseerde zedencriminaliteit (wetsartikelen Sr 240b en Sr 248e) versus overige wetsartikelen (voornamelijk fraude-gerelateerde wetsartikelen Sr 231a en Sr 232; de overige wetsartikelen komen hoogstens enkele keren per jaar voor).

Voor statistieken betreffende de ernst van cyber- en gedigitaliseerde criminaliteit wordt gebruikgemaakt van strafdreiging en bestraffing indicatoren. Per jaar is de gemiddelde maximale strafdreiging in jaren vrijheidsstraf, de gemiddelde opgelegde straf en het percentage strafzaken met een onvoorwaardelijke vrijheidsstraf bepaald van alle strafzaken waarin cyber- en gedigitaliseerde criminaliteit voorkwamen. Voor de gemiddelde straf is de procedure zoals uiteengezet in Beerthuizen et al. (2015) grotendeels gevolgd, wat resulteert in een zogeheten celdagequivalent. Er wordt hier alleen naar strafzaken met meerderjarige daders gekeken, omdat de deze procedure niet gevalideerd is voor strafzaken tegen minderjarigen. Ook is er geen duidelijkheid over hoe opgelegde straffen tegen minderjarigen zich verhouden tegenover straffen tegen meerderjarigen, wanneer gepleegde delicten vergelijkbaar zijn. Voor het percentage strafzaken met een onvoorwaardelijke vrijheidsstraf beperken wij ons ook tot meerderjarigen, omdat vrijheidsstraffen bij minderjarigen veel minder vaak voorkomen.

Bijlage 3 Online bedreigingen in het lokaal bestuur

Tabel B3.1 Overzicht artikelen

Aanleiding	Thema's	Link
AZC in de gemeente	Maatschappelijk, populistisch sentiment	www.rtlnieuws.nl/node/914766
AZC in de gemeente	Maatschappelijk, populistisch sentiment	www.gelderlander.nl/ede/van-de-knaap-wil-dood-op-borden-in-otterlo~aac0a090/
AZC in de gemeente	Maatschappelijk, populistisch sentiment	www.ad.nl/groene-hart/aangifte-burgemeester-gouda-om-bedreigingen~a3981341/
AZC in de gemeente	Maatschappelijk, populistisch sentiment	www.ad.nl/binnenland/man-vast-voor-online-bedreigen-burgemeester-den-bosch~a6382d64/
AZC in de gemeente	Maatschappelijk, populistisch sentiment	www.dvhn.nl/drenthe/Burgemeester-Hoogeveen-met-de-dood-bedreigd-21171000.html
Clubhuis motorclub sluiten	Georganiseerde misdaad	www.1limburg.nl/jos-som-nooit-overwogen-te-stoppen-vanwege-bedreigingen
Clubhuis motorclub sluiten	Georganiseerde misdaad	www.volkskrant.nl/nieuws-achtergrond/loco-burgemeester-emmen-na-bedreiging-ondergedoken-in-engeland~b336aaa6/
Coronacrisis-tweet	Maatschappelijk, populistisch sentiment	www.gelderlander.nl/veenendaal/oud-burgemeester-veenendaal-met-de-dood-bedreigd-na-tweet-over-coronahysterie~aae898f3/?referrer=https://www.google.com/
Drugsaanpak	Georganiseerde misdaad	www.bd.nl/waalwijk-heusden-e-o/bedreigers-burgemeester-jan-hamming-stopten-na-serieus-gesprek-met-de-politie~aa5be4c2/?referrer=https://www.google.com/
Drugsaanpak	Georganiseerde misdaad	www.nrc.nl/nieuws/2015/12/19/ik-laat-me-niet-van-mijn-koers-brengen-1567990-a797581
Drugsaanpak	Georganiseerde misdaad	www.ad.nl/binnenland/brabantse-burgemeester-70-bedreigd-door-criminelen-drugsgeld-levert-enorm-rendement-op~a89c2af0/
Drugsaanpak	Georganiseerde misdaad	www.1limburg.nl/duizenden-smsjes-verstuurd-zaak-bedreiging-burgemeester
Drugsaanpak	Georganiseerde misdaad	www.ad.nl/gouda/doodsbedreiging-laat-mij-niet-koud~a89fb795/
Officieel onduidelijk, vermoedelijk georganiseerde misdaad	Georganiseerde misdaad	www.nhnieuws.nl/nieuws/236843/Noord-Hollandse-burgemeesters-veelvuldig-bedreigd
Onderwereld	Georganiseerde misdaad	https://eenvandaag.avrotros.nl/item/en-toen-was-de-burgemeester-het-beu-luc-winants-blikt-terug-op-bedreigingen-en-scheldpartijen/
Onduidelijk	Onduidelijk	www.nhnieuws.nl/nieuws/236925/burgemeester-ouder-amstel-deed-dit-jaar-al-meerdere-keren-aangifte-van-belediging
Onduidelijk	Onduidelijk	www.ad.nl/amersfoort/burgemeester-metz-van-soest-herhaaldelijk-bedreigd~a7f1a114/
Onduidelijk	Onduidelijk	www.noordhollandsdagblad.nl/cnt/dmf20181126_68148095/burgemeester-koggenland-ernstig-bedreigd?utm_source=google&utm_medium=organic
Ontoerekeningsvatbaarheid	Persoonlijk	www.omroepzeeland.nl/nieuws/106621/Geen-cel-maar-gedwongen-opname-voor-bedreiger-Aboutaleb
Persoonlijke frustratie	Persoonlijk	www.rtvutrecht.nl/nieuws/1884430/verdachte-van-bedreiging-burgemeester-de-bilt-vrijgesproken.html

Aanleiding	Thema's	Link
Vergunning	Persoonlijk	www.ad.nl/den-haag/werkstraf-geeist-tegen-bloemenverkoper-die-dreigde-burgemeester-charlie-aptroot-dood-te-schieten~a92e0677/
Vergunning	Persoonlijk	www.tubantia.nl/wierden/taakstraf-voor-ex-voorzitter-wiezo-voor-bedreiging-burgemeester-robben~a91bb37f/?referrer=https://localfocus2.appspot.com/5c1c9b0feba8f
Verward persoon	Persoonlijk	www.omroepgelderland.nl/nieuws/2140918/Ik-kom-je-vermoorden-Zaltbommel-wordt-al-1-5-jaar-bedreigd
Verward persoon	Persoonlijk	www.ed.nl/laarbeek/bedreigde-burgemeester-van-der-meijden-blij-met-alle-steun~a257a5b4/
Verward persoon	Persoonlijk	www.lc.nl/friesland/Celstraf-voor-bedreiging-burgemeester-Klaas-Agricola-24931613.html?harvest_referrer=https%3A%2F%2Fwww.google.com%2F&harvest_referrer=https%3A%2F%2Ftoestemming.ndcmediagroep.nl%2F%3Ftoken%3Db25dc27e-3b1c-417d-87bf-10df2d14e4fd
Verward persoon	Persoonlijk	www.telegraaf.nl/nieuws/2745477/bedreiger-burgemeester-van-zanen-vrijgelaten
Verward persoon	Persoonlijk	www.rijnmond.nl/nieuws/188027/63-jarige-voor-de-rechter-om-bedreiging-burgemeester-Nissewaard
Verward persoon	Persoonlijk	www.bd.nl/home/boxtelaar-staat-terecht-voor-bedreigen-boxtelse-burgemeester~a2bea9fe/
Verward persoon	Persoonlijk	www.omroepgelderland.nl/nieuws/2432998/Man-voor-rechter-om-bedreigen-van-burgemeester-Renkum-en-politie
Vreugdevuren afzeggen	Maatschappelijk, populistisch sentiment	www.binnenlandsbestuur.nl/bestuur-en-organisatie/nieuws/steun-voor-bedreigde-burgemeesters.9607479.lynkx

Tabel B3.2 Online/offline

Label	Definitie	Voorbeeld
Online dreiging	Dreigingen die de burgemeester op een digitale manier ontving. Op één na zijn al deze dreigingen via sociale media zoals maar niet beperkt tot Facebook, Twitter of Whatsapp geuit. De uitzondering is een dreiging die werd geuit als reactie onder een artikel op een nieuwssite.	'Een 48-jarige man moet donderdag voor de rechter verschijnen voor het bedreigen van burgemeester Agnes Schaap van Renkum. Hij zou filmpjes op Facebook hebben geplaatst, waarin hij dreigde haar te gijzelen. Volgens de Arnhemmer zouden zij en de politie er voor verantwoordelijk zijn dat hij drie weken in een isoleercel heeft gezeten.'
Offline dreiging	Offline dreigingen nemen plaats in de fysieke wereld. Voorbeelden van deze dreigingen zijn: autobranden, dreigingen die de door de burgemeester aan den lijve zijn ondervonden, brieven, telefoontjes of politiemeldingen.	'De dreigtelefoontjes komen van een man die in de regio bekend staat als 'de bommenman'. Volgens de burgemeester dreigde de man met explosieven en nam hij de woorden 'ik kom je vermoorden' regelmatig in zijn mond.'

Tabel B3.3 Aanleiding voor dreigingen

Label	Definitie	Voorbeeld
Verward persoon	Deze dreigingen komen meestal voort uit persoonlijke frustratie, met als uniek kenmerk dat de verdachte specifiek aangemerkt is als verward persoon. De dreiging lijken op losse flodders, niet per se gericht aan de persoon achter de titel 'burgemeester'.	'[De advocaat] benadrukte dat de tekstboodschappen die de Boxtelaar vorig jaar verstuurde verkeerd zijn begrepen. Dat geldt ook voor wat hij zou hebben gezegd tijdens een bijna drie kwartier durend telefoongesprek met een leerplichtambtenaar. (…) De Boxtelaar zou hebben gezegd of geschreven dat hij 'de ergste horror zou doen uitkomen'. Ook repte hij over een lijk in een kofferbak.'
AZC in de gemeente	Dreigingen die voortkomen door een directe beslissingen van een burgemeester. Burgers zijn ontevreden over een AZC en botvieren de frustratie aan het adres van de burgervader.	In een brief aan RTV Oost die vandaag door de zender is gepubliceerd staat dat de afzender 'geen vluchtelingen in Rijssen wil hebben'. Als burgemeester Hofland 'wel deze vluchtelingen opneemt gaat hij dood' staat er te lezen. Ook zijn gezin en het stadhuis zijn dan niet veilig, meldt de onbekende briefschrijver die heeft ondertekend met 'IS'.
Drugsaanpak	Dreigingen die voortkomen naar aanleiding van de drugsaanpak in een gemeente. Vaak moeilijk te herleiden.	'Burgemeester Jan Boelhouwer van Gilze en Rijen kreeg vier keer te maken met serieuze bedreigingen van criminelen. (…) Hij pleit voor harde maatregelen tegen het massaal witwassen van drugsgelden in vastgoed.
Vergunning	Dreigingen die komen uit onvrede van burgers omdat ze een vergunning niet krijgen.	'Werkstraf geëist tegen bloemenverkoper die dreigde burgemeester Charlie Aptroot dood te schieten. (…) De verdachte man had al langere tijd een geschil met de gemeente over het aantal parkeerplekken bij zijn bloemenkiosk. In een rechtszaak in maart vorig jaar werd de man vrijgesproken van de bedreigingen.'
Clubhuis motorclub sluiten	De aanpak van burgemeesters tegen dreigingen vanuit motorclubs wordt beantwoord door bedreiging.	'Som werd het afgelopen jaar enkele maanden zwaar beveiligd, nadat hij een pand van de Hells Angels op de Markt van Kerkrade sloot. Voor zijn huis stond 24-uur politiebewaking. Op verzoek van politie en justitie moest hij zelfs enkele dagen op een ander adres verblijven. Som zegt daarover: 'Heel vervelend, zit niemand op te wachten.'
Onderwereld	Dreigingen uit de 'onderwereld'. Veel andere dreigingen vallen op het eerste gezicht onder dit label, maar hebben een verdere specificatie waardoor ze onder een specifiek label vallen. Onder het label 'Onderwereld' valt alleen het artikel waar deze term letterlijk te vinden is als aanleiding voor de dreiging.	'De criminelen kwamen steeds dichterbij: er kwamen bedreigingen en er stond wel eens iemand te wachten als Winants 's avonds thuiskwam. Anderen kwamen doodleuk op bezoek in het gemeentekantoor. 'Mensen die je even iets komen vertellen', omschrijft hij ze. Namen noemt hij niet. 'Ze vertellen je fijntjes wat hun afkomst is, dat ze zaken komen doen. Nou, dan ben je bij mij aan het verkeerde adres.'
Officieel onduidelijk, vermoedelijk georganiseerde misdaad.	De bron van de dreigingen wordt door de politie verborgen gehouden. Wel zijn er aanwijzingen te vinden in het beleid van de burgemeester uit welke hoek de dreigingen komen.	'Sommige dingen kan ik niet vertellen. Niet dat ik veel weet. Informatie over de bedreiging komt terecht bij de hoofdofficier van justitie en die maakt, in overleg met de politie, een beoordeling en treft maatregelen die hij nodig vindt. Ik krijg die informatie niet.'

Label	Definitie	Voorbeeld
Coronacrisis tweet	Een burger was het niet eens met het standpunt van de burgemeester.	'Burgemeester Wouter Kolff van Dordrecht heeft aangifte gedaan tegen een Papendrechter die hem dit weekeinde met de dood bedreigde. De man zei bij een bericht op Facebook dat hij de voormalig burgemeester van Veenendaal wilde doodschieten.'
Vreugdevuren afzeggen	Naar aanleiding van het afzeggen van de vreugdevuren werd de burgemeester bedreigd door burgers.	'Het verbieden van de vreugdevuren rond de jaarwisseling heeft tot veel beledigingen en twee bedreigingen geleid', stelt de woordvoerder van burgemeester Jetten desgevraagd. 'De burgemeester heeft op aanraden van politie en justitie aangifte gedaan.'
Ontoerekeningsvatbaarheid		'Volgens deskundigen heeft de Spijkenisser waanstoornissen waar hij niet aan te behandelen valt. Hijzelf ontkent dat. Omdat hij naar eigen zeggen al zestien jaar wordt gestalkt door de politie en mensen hem bespioneren en bestelen, stuurde de man in april een dreigmail naar de burgemeester. ,,Vandaag of morgen vermoord ik er een paar of hak ik er een paar in stukken'', dreigde hij in de richting van de ambtenaren.'
Persoonlijke frustratie	Burgers voelen zich tekort gedaan door de burgemeester en/of het openbaar bestuur uiten hun frustratie in de vorm van dreigingen aan het adres van de burgemeester. Er is hier geen sprake van een verward persoon.	'De man probeert al jaren een plekje te bemachtigen op het woonwagenkamp in Maartensdijk, maar volgens hem wordt dat door de gemeente gedwarsboomd. (…) Volgens ambtenaren zou hij hebben verteld dat hij vroeger iemand had neergestoken. Ook zou hij hebben gezegd dat hij iemand te pakken wilde nemen. De burgemeester, een wethouder of een raadslid. Volgens de ambtenaren voldoende om melding te maken van het gesprek.'

Tabel B3.4 Aard van dreigingen

Label	Definitie
Persoonlijk	Onder dit overkoepelende label vallen de aanleidingen: Ontoerekeningsvatbaarheid, Persoonlijke frustratie, Vergunning en Verward persoon
Georganiseerde misdaad	Onder dit overkoepelende label vallen de aanleidingen: Clubhuis motorclub sluiten, drugsaanpak, officieel onduidelijk, vermoedelijk georganiseerde misdaad en onderwereld
Maatschappelijk/ populistisch sentiment	Onder dit overkoepelende label vallen de aanleidingen: AZC in de gemeente, Coronacrisis-tweet en vreugdevuren afzeggen

Tabel B3.5 Gevolgen en maatregelen

Label	Definitie	Voorbeeld
Bewaking	De burgemeester in kwestie kreeg (een vorm van) beveiliging als gevolg van dreigingen.	'Als de burgemeester 's avonds naar zijn niet nader te noemen onderduikadres gaat – slapen in de eigen woning aan een gracht in de binnenstad zit er al een tijdje niet meer in – leveren de mannen hem daar af. Nee, een echt hechte band krijgt hij niet met ze want om de zoveel tijd wordt de een voor de ander ingewisseld. 'Dat is standaard beleid', weet Jos Wienen (58), burgemeester van Haarlem. Dit is hem ook nog eens door justitie verteld, trouwens ook door collega-burgemeesters die onderwerp zijn geweest van persoonlijke beveiliging.'
Gevangenisstraf	Gevangenisstraf ten gevolge van de dreiging. De verdachte werd dus veroordeeld.	'Burgemeester Joyce Langenacker van Ouder-Amstel deed dit jaar een aantal keer aangifte wegens zware beledigingen aan haar adres'
Taakstraf	Taakstraf ten gevolge van de dreiging. De verdachte werd dus veroordeeld.	'Sinds zijn scheiding is ondernemer Henk K. (52) verbitterd. Als een ambtenaar het zomerfeest Wiezo, waarvoor hij zich het vuur uit de sloffen liep, dwarsboomt, bedreigt hij burgemeester Robben. K. krijgt daarvoor een taakstraf van 60 uur.'
Onderzoek	Een onderzoek werd ingesteld naar aanleiding van de dreiging. Eventuele gevolgen daarvan zijn niet te herleiden uit het artikel.	'Als we de burgemeester te grazen kunnen nemen, zullen we het niet laten', luidde de ene bedreiging waar justitie nu onderzoek naar doet, zo blijkt uit de brief van de officier van justitie die de burgemeester eind vorige week heeft ontvangen'
Onderduiken	De burgemeester moest onderduiken naar aanleiding van de dreiging.	'Locoburgemeester Bouke Arends (51) van de gemeente Emmen heeft in maart drie weken ondergedoken gezeten in Engeland. Hij deed dat op dringend advies van het Openbaar Ministerie, nadat er serieuze bedreigingen jegens hem waren geuit.'
Vrijspraak	De zaak rondom de dreiging is voorgekomen en de verdachte is vrijgesproken.	'Volgens de man was het allemaal niet zo bedoeld. (...) De rechter geloofde de man. Zijn woordkeuze was 'enorm onhandig', maar niet voldoende voor een veroordeling. Ze sprak hem daarom vrij.'
Bewaking en onderduiken	De burgemeester in kwestie moest naar aanleiding van de dreiging zowel bewaakt worden als onderduiken.	'Je bent op twee manieren beknot. Het eerste is dat ik hier in de stad niet gewoon kan rondlopen. Dat is toch een van de leuke dingen van bestuurder zijn. Niet in die ivoren toren zitten, maar gewoon op straat een praatje maken. Mijn woning is hier dichtbij. Ik wandelde of fietste altijd naar het werk. Het tweede is dat je dus niet meer thuis woont.'
Waarschuwing	De verdachte van de dreiging kreeg een waarschuwing.	'Een kogel door z'n kop', reageert hij op een online artikel in een community op Facebook. Loohuis voelt zich niet direct bedreigd, maar laat wel weten: het is niet iets waar je zo maar even overheen stapt. Ook omdat het effect heeft op je gezin.'' De 45-jarige man komt uiteindelijk voor de rechter, maar komt er vanaf met een waarschuwing.'
Boete	De verdachte van de dreiging kreeg een boete.	

Label	Definitie	Voorbeeld
Aangifte gedaan	Bij de labels gevangenisstraf, taakstraf en boete zijn er natuurlijk aangiftes gedaan. Om het verschil in berichtgeving duidelijk te maken is ervoor gekozen die fragmenten niet te labelen onder aangifte, maar onder de straf die ze kregen als die werd benoemd in het artikel	'Burgemeester Joyce Langenacker van Ouder-Amstel deed dit jaar een aantal keer aangifte wegens zware beledigingen aan haar adres. Ook zij herkent het beeld dat burgemeesters regelmatig te maken krijgen met bedreigingen.'
Gedwongen behandeling	De verdachte van de dreiging kreeg een gedwongen behandeling	'De 43-jarige man uit Sint-Maartensdijk die ervan verdacht werd de Rotterdamse burgemeester Ahmed Aboutaleb te hebben bedreigd, wordt opgenomen in een psychiatrisch ziekenhuis. Dat heeft de rechtbank in Middelburg bepaald.'