Masterthesis

Een verkenning naar de governance ten aanzien van cybercrime in Oost-Nederland

"Want goede netwerken kunnen veel meer in de samenwerking"

Naam:	Jelle Kuiper
Studentnr:	s1014258
Datum:	oktober 2020
Eerste lezer:	prof. dr. M. Herweijer
Tweede lezer:	prof. dr. I. Helsloot
Aantal woorden:	35.707

Radboud Universiteit

Masterthesis geschreven in het kader van de Master Besturen van Veiligheid aan de Faculteit der Managementwetenschappen, Opleiding Bestuurskunde, Radboud Universiteit Nijmegen

Inhoudsopgave

BEGRIPPENLIJST **2**

VOORWOORD **3**

SAMENVATTING **4**

1. INLEIDING **6**

1.1. AANLEIDING 7
1.2 DOELSTELLING 8
1.3 HOOFDVRAAG 8
1.4 DEELVRAGEN 8
1.5 MAATSCHAPPELIJKE EN WETENSCHAPPELIJKE RELEVANTIE 9
1.6 VOORBESCHOUWING THEORETISCH KADER 9
1.7 VOORBESCHOUWING METHODOLOGISCH KADER 10
1.8 LEESWIJZER 10

2. BELEIDSKADER **11**

2.1 VEILIGHEIDSNETWERK OOST-NEDERLAND 12
2.2 CONTEXT 12
2.3 ACTOREN 13
2.4 DOELSTELLINGEN 14
2.5 CYBERCRIME IN OOST-NEDERLAND 14
2.6 SLACHTOFFERSCHAP CYBERCRIME 15
2.7 MELDINGSBEREIDHEID CYBERCRIME 16

3. THEORETISCH KADER **19**

3.1 DEFINIËRING CYBERCRIME 19
3.2 CYBERWEERBAARHEID 22
3.3 DE VEILIGHEIDSKETEN 23
3.4 DEFINIËRING GOVERNANCE NETWORK 24
3.5 GOVERNANCE RONDOM CYBERCRIME 26
3.6 CONCEPTUEEL MODEL 27

4. METHODOLOGISCH KADER **30**

4.1 ONDERZOEKSSTRATEGIE 31
4.2 RESPONDENTEN 31
4.3 METHODEN VAN DATAVERZAMELING 32
4.4 OPERATIONALISATIE 33
4.5 METHODEN VAN DATA-ANALYSE 35
4.6 BETROUWBAARHEID EN VALIDITEIT 35

5. RESULTATEN EN ANALYSE **37**

5.1 WAT IS CYBERCRIME VOLGENS DE GEMEENTEN EN EXPERTS UIT HET WERKVELD? 38
5.2 *HOE ZIET HET ONDERDEEL 'BEDROG EN DIEFSTAL' IN DE PRAKTIJK ERUIT?* 40
5.3 HOE ZIET DE HUIDIGE SAMENWERKING OP HET GEBIED VAN BEDROG EN DIEFSTAL ERUIT? 61
5.4 WELKE ROLLEN EN VERANTWOORDELIJKHEDEN HEBBEN DE BETROKKEN ACTOREN BINNEN DE VEILIGHEIDSKETEN? 70
5.5 WELKE KANSEN/VERBETERINGEN ZIEN GEMEENTEN EN EXPERTS OM DE WEERBAARHEID VAN INWONERS TE VERGROTEN? 79

6. CONCLUSIE, AANBEVELINGEN EN REFLECTIE **83**

6.1 CONCLUSIE 84
6.2 AANBEVELINGEN 86
6.3 REFLECTIE 87

LITERATUURLIJST **88**

BIJLAGEN **94**

Begrippenlijst

Begrip	**Definitie/verklaring**
Geldezel (money mule)	Een geldezel is een rekeninghouder die bewust of onbewust wordt misbruikt voor criminele doeleinden.
Cloud	Het online opslaan van bestanden via het internet.
Sexting	Sexting is het verzenden en/of ontvangen van seksueel getinte beeldmateriaal of tekstberichten door middel van een applicatie of mobiel device.
RIEC	Regionaal Informatie en Expertise Centrum
Quick Response (QR) code	Een Quick Response (QR) code geeft toegang tot een website zonder dat de eindgebruiker het adres hoeft te typen.

Voorwoord

Beste lezer,

Voor u ligt mijn masterthesis “Een verkenning naar een governance ten aanzien van cybercrime in Oost-Nederland” die ik heb geschreven ter afronding van de master Bestuurskunde (specialisatie Besturen van Veiligheid) aan de Radboud Universiteit te Nijmegen. Dit onderzoek heb ik geschreven in opdracht van het Veiligheidsnetwerk Oost-Nederland. In dit onderzoek heb ik de governance in kaart gebracht van het onderdeel bedrog en diefstal binnen de cybercrime. Het onderzoek beoogt tevens een frisse start te maken met het expertteam Cyber van het Veiligheidsnetwerk Oost-Nederland. In de afgelopen maanden is de urgentie van cybercrime alleen maar gestegen. Daarom is het van belang dat er niet alleen kennis en expertise wordt uitgewisseld maar ook daadwerkelijk stappen worden gezet om effectief samen te werken.

Het afronden van deze thesis maakt eveneens een einde aan mijn studententijd. Na mijn opleiding Integrale Veiligheid in Rotterdam heb ik gekozen voor een nieuwe uitdaging in Nijmegen. De pre-master en de masterspecialisatie Besturen van Veiligheid hebben mij veel nieuwe inzichten gebracht. Naast mijn studie heb ik ook met veel plezier de politieke kant van de bestuurskunde mogen ervaren als fractielid in de Nijmeegse politiek. De combinatie tussen theorie en praktijk heb ik als zeer waardevol ervaren.

Tot slot wil ik mijn stagebegeleider Mariska Rijneveld bedanken voor de mogelijkheid om bij het Veiligheidsnetwerk Oost-Nederland af te studeren. Ik heb met veel plezier deelgenomen aan activiteiten, respondenten gesproken en aan mijn onderzoek gewerkt. Verder wil ik mijn scriptiebegeleider prof. dr. Michiel Herweijer bedanken voor de begeleiding en de constructieve feedbackmomenten. Aansluitend daarop wil ik mijn dank uitspreken aan alle respondenten die deel hebben genomen aan dit onderzoek. Zonder jullie inbreng was dit onderzoek niet gelukt.

Jelle Kuiper
Deventer, oktober 2020

Samenvatting

In Oost-Nederland hebben de 76 gemeenten, het Openbaar Ministerie en de politie aangegeven de mogelijkheden te verkennen om cybercrime gezamenlijk aan te pakken. Het Veiligheidsnetwerk Oost-Nederland heeft daarom cybercrime tot speerpunt gemaakt in de Veiligheidsstrategie 2019-2022. Er is echter nog geen pasklaar antwoord op wat cybercrime precies is, hoe en door wie deze criminaliteit wordt uitgevoerd en hoe deze criminaliteit het beste aangepakt kan worden. Daarnaast ontstaat een spanningsveld over de vraag in hoeverre de traditionele bestuurlijke actoren (politie, Openbaar Ministerie, gemeenten, etc.) verantwoordelijk zijn voor het garanderen van 'digitale veiligheid' en waar de verantwoordelijkheden van andere partijen zoals inwoners, ondernemers en IT-providers beginnen.

Dit onderzoek richt zich op de verschillende vormen van 'bedrog en diefstal' binnen de cybercrime. De doelstelling van het onderzoek is inzicht verschaffen in de actoren en de samenhang van governance netwerken ten aanzien van het thema bedrog en diefstal. De hoofdvraag luidt als volgt: '*Welke actoren zijn betrokken bij de aanpak van bedrog en diefstal binnen de cybercrime, welke taken en verantwoordelijkheden hebben deze actoren en in hoeverre verhoudt de samenwerking zich ten aanzien van cybercrime van het Veiligheidsnetwerk Oost-Nederland tot de randvoorwaarden voor succesvolle samenwerking in een governance network?*'

Om de governance netwerken inzichtelijk te maken zijn semi-gestructureerde interviews afgenomen met beleidsadviseurs van gemeenten in Oost-Nederland en experts uit het werkveld. Dit onderzoek vertrekt vanuit de governance network theorie van Provan en Kenis (2008) waarbij de randvoorwaarden van succesvolle samenwerking worden vastgesteld.

Het begrip cybercrime laat zich niet eenvoudig definiëren. Gemeenten hebben een voorkeur voor het begrip gedigitaliseerde criminaliteit ofwel cybercrime in brede zin. Dit zijn de klassieke vormen van criminaliteit waar een digitaal component aan gekoppeld is. Het Openbaar Ministerie en de politie hanteren een strikte scheiding tussen beide vormen vanwege de juridische basis. Dit in tegenstelling tot organisaties die nauw betrokken zijn bij ondernemers in het midden- en kleinbedrijf, waarbij de focus niet ligt op de cybercrime in brede of enge zin, maar bij de maatschappelijke effecten van deze vormen van criminaliteit voor de onderneming.

Inwoners en ondernemers beschikken veelal over onvoldoende risicobewustzijn. De risico's worden onvoldoende herkent vanwege onbewuste onwetendheid. De basismaatregelen worden vaak niet genomen omdat de noodzaak ontbreekt om aandacht te besteden aan veiligheidsmaatregelen.

De gemeente speelt op lokaal niveau een belangrijke rol in het creëren van bewustwording en het cyberweerbaar maken van inwoners en ondernemers. Gemeenten dienen bestuurlijke maatregelen te nemen bij online verstoringen en hun eigen informatiebeveiliging op orde te brengen. Tot slot dienen gemeenten zicht te krijgen op de aard en omvang van slachtofferschap en daderschap op lokaal niveau. Om een gerichte aanpak of beleid te maken is het voor gemeenten van belang om te weten hoe groot het probleem daadwerkelijk is en welke vorm van bedrog en diefstal prioriteit heeft. De daadwerkelijke opsporing en vervolging wordt gezien als kerntaak van de traditionele strafrechtelijke instituties. Niet alleen gemeenten dienen eindgebruikers weerbaar te maken. Dit geldt eveneens voor de politie en Openbaar Ministerie, maar ook voor regionale veiligheidsnetwerken en belangenverenigingen. Regionale veiligheidsnetwerken in het inzichtelijk maken van lokale

initiatieven, het uitwisselen van kennis en het activeren van gemeenten om met het thema cyber aan de slag te gaan.

De capaciteit van zowel gemeenten als experts uit het werkveld laat een zorgwekkend beeld zien. In de volle breedte is er te weinig tijd, middelen of prioriteit bij gemeenten op het gebied van cybercrime. De meeste respondenten ervaren dat de politie over onvoldoende capaciteit beschikt op het thema cybercrime. Niet alleen aan de kant van de opsporing ligt te weinig capaciteit, ook de vervolging van verdachten wordt als een zwakke schakel ervaren.

In Oost-Nederland zijn verschillende overleggremia's waarin cybercrime en/of gedigitaliseerde criminaliteit besproken wordt. Het expertteam Cyber van het Veiligheidsnetwerk Oost-Nederland staat nog in de kinderschoenen. Het expertteam kan het best gedefinieerd worden als een leiderorganisatienetwerk (Provan & Kenis, 2008). Het team beschikt over een lage mate van doelconsensus en relatief veel deelnemers. Op dit moment is in de praktijk geen sprake van structurele samenwerking tussen de deelnemers. Na het vertrek van de ambtelijk trekker bij het expertteam Cyber bleek onvoldoende bereidheid om een vervolg te geven aan de periodieke bijeenkomsten.

Zowel gemeenten als experts uit het werkveld geven aan dat samenwerken op het gebied van cybercrime niet alleen maar positieve resultaten oplevert. Ondanks dat beide groepen aangeven behoefte te hebben aan netwerkcompetenties (Provan & Kenis, 2008). Geconcludeerd kan worden dat de samenwerking noodzakelijk is om het vraagstuk aan te pakken. De samenwerking tussen verschillende organisaties blijkt in de praktijk soms weerbarstig te zijn.

Inwoners en ondernemers zijn zelf verantwoordelijk voor hun offline en online handelingen. Dit betekend echter niet dat betrokken organisaties geen taak hebben of een rol kunnen vervullen. Zo hebben supercontrollers, appontwikkelaars en hosting- en serviceproviders de taak om software updates beschikbaar te stellen en criminele webwinkels te sluiten. In de preventieve schakel heeft de gemeente een sleutelpositie om eindgebruikers weerbaar te maken. Ook op landelijk niveau dienen brancheorganisaties, belangenverenigingen, webwinkels, maar ook verzekeraars en banken hun klanten en leden te wijzen op de risico's van bedrog en diefstal. De Veiligheidsregio is in samenwerking met de betrokken (veiligheids)partners verantwoordelijk voor de voorbereiding op een ramp of crisis in het cyberdomein, waarbij de vitale infrastructuur wordt geraakt en de maatschappelijke effecten groot zijn. Ook in het cyberdomein blijft de politie samen met het Openbaar Ministerie verantwoordelijk voor de opsporing en vervolging van daders. Tot slot dienen banken, verzekeraars, maar ook Slachtofferhulp Nederland en de Fraudeinfodesk slachtoffers te helpen om herhaling te voorkomen.

Het thema cybercrime dient op lokaal, regionaal en nationaal niveau geagendeerd te worden op de politieke en bestuurlijke agenda's om capaciteit vrij te maken en meer draagvlak te creëren. Ook door het delen van slachtofferschap kan de urgentie benadrukt worden. De focus voor gemeenten gaat uit naar de informatiebeveiliging, maar ook naar het verkrijgen van inzicht in de aard en omvang van cybercrime op lokaal niveau. Op het gebied van communicatie ligt er eveneens een grote uitdaging voor de overheid. Het onderwijs kan een rol vervullen in het cyberweerbaar maken van eindgebruikers. De preventieve aanpak van cybercrime is voor gemeenten een complexe uitdaging. Kleinere gemeenten voelen de behoefte om doelgericht aan de slag te gaan met praktische handvaten. Grotere gemeente zoals Deventer en Zwolle hebben meer capaciteit en willen het vraagstuk ook op langer termijn borgen. Ongeacht de grootte van de gemeente zijn lokale overheden in het algemeen op zoek naar best-practices.

1. Inleiding

1. Inleiding

1.1. Aanleiding

In 2004 vroeg het Sociaal en Cultureel Planbureau (SCP) hoe burgers keken naar Nederland in 2020. Volgens deze voorspelling bleken 82% van de Nederlanders bang te zijn voor cybercriminaliteit in de toekomst (SCP, 2019). Het SCP concludeert in 2019 dat cybercriminaliteit nog steeds iets is om bang voor te zijn. Nederlanders worden steeds vaker slachtoffer van digitale criminaliteit, terwijl de traditionele vormen van criminaliteit afnemen (CBS, 2020). Het gaat bij cybercrime om digitale vormen van criminaliteit waarbij personen via internet of via andere digitale informatiedragers slachtoffer kunnen worden. Dit komt tot uiting via digitale vormen van identiteitsfraude, aan- en verkoopfraude, hacken en pesten via het internet. Uit onderzoek van Europol (2019) blijkt dat cybercriminelen zich steeds meer richten op grotere en meer winstgevende doelen. Naast particulieren zijn bedrijven en overheden ook kwetsbaar voor digitale criminaliteit. Ruim 20% van de bedrijven is in 2016 getroffen door een cyberaanval (CBS, 2017). De gevolgen van digitale criminaliteit hebben ook grote impact op de economie. Uit onderzoek van accountantskantoor Deloitte (2017) blijkt dat cybercrime naar schatting 10 miljard euro per jaar kost. Een kwart hiervan (2,4 miljard euro) is gekoppeld aan cyberaanvallen op de publieke sector. Volgens Deloitte zijn aanvallen op de publieke sector met name gericht op verstoring van de operationele continuïteit en verminderde betrouwbaarheid van producten en diensten. Door ontbrekende weerbaarheid ligt ontwrichting van de maatschappij op de loer (NCTV, 2019). De WRR (2019) constateert dat verstoring of uitval van de digitale infrastructuur niet alleen directe gevolgen kan hebben voor de samenleving, maar ook voor de economie, alsmede voor het vertrouwen in de democratische rechtstaat.

Bij het optreden van een ramp of crisis in de fysieke wereld bestaan er wet- en regelgeving en professionele crisisdiensten. Bij de bestrijding van een brand is het grotendeels duidelijk wie welke taken en verantwoordelijkheden heeft. Dit in tegenstelling tot cybercrime, waarbij de samenwerking en aanpak nog niet volledig zijn uitgekristalliseerd. Ondanks dat staat digitale veiligheid steeds hoger op de bestuurlijke prioriteitenlijst (VNG, 2020). Dit geldt niet alleen voor de samenwerking op landelijk niveau, maar ook op het regionale en lokale niveau. In het landsdeel Oost-Nederland hebben de 76 gemeenten, het OM en de politie aangegeven de mogelijkheden te verkennen om cybercrime gezamenlijk aan te pakken. Het Veiligheidsnetwerk Oost-Nederland heeft daarom cybercrime tot speerpunt gemaakt in de Veiligheidsstrategie 2019-2022. Er is echter nog geen pasklaar antwoord op wat cybercrime precies is, hoe en door wie deze criminaliteit wordt uitgevoerd en hoe deze criminaliteit het beste aangepakt kan worden (Veiligheidsnetwerk Oost-Nederland, z.d.). Daarnaast ontstaat een spanningsveld over de vraag in hoeverre de traditionele bestuurlijke actoren (politie, OM, gemeenten, etc.) verantwoordelijk zijn voor het garanderen van ‘digitale veiligheid’ en waar de verantwoordelijkheden van andere partijen zoals, inwoners, IT-providers en ondernemers beginnen. De aanpak van lokale veiligheidsproblemen is geen exclusieve verantwoordelijkheid van traditionele strafrechtelijke instituties, zoals het OM en de politie (Terpstra & Krommendijk, 2010). Steeds vaker wordt de wederzijdse afhankelijkheid tussen overheden, maatschappelijke organisaties, bedrijven en andere partijen bij de vorming en uitvoering van overheidsbeleid onderkend (Klijn & Koppenjan, 2016). Uit onderzoek van Banton (1964) blijkt dat de traditionele strafrechtelijke instituties alleen hun werkzaamheden goed kunnen verrichten in nauwe samenwerking met burgers en bedrijven. Zo dienen burgers ook maatregelen te nemen om hun huis en voertuig te beveiligen.

De kerngroep Cybercrime van het Veiligheidsnetwerk Oost-Nederland initieert op basis van het uitvoeringsplan 2019-2020 een brede regionale samenwerking bij de aanpak van cybercrime, waarbij zowel traditionele strafrechtelijke instituties als onderwijsinstanties en het bedrijfsleven deel uitmaken van het expertteam en/of de werkgroepen. Dit betekent dat de samenwerking tussen de betreffende actoren in het kader van cybercrime – bestuurskundig gezien - aangemerkt kan worden als een 'governance network'. Het thema cybercrime wordt inmiddels op meerdere bestuurlijke niveaus op de agenda gezet. Niet alleen op landelijk niveau ligt hier een verantwoordelijkheid maar ook op lokaal niveau speelt de gemeente een centrale rol. Vanaf de jaren '90 ligt de focus van gemeenten steeds meer op zowel een zelfstandige als een gezamenlijke bijdrage aan veiligheid (Prins & Cachet, 2011). Naast de coördinerende rol van gemeenten op het gebied van openbare orde en veiligheid hebben lokale overheden ook meer een rol gekregen bij de preventieve aanpak van veelvoorkomende criminaliteit (Terpstra & Mein, 2010; Bantema et al., 2018). Dit pakt de gemeente in de praktijk veelal op met lokale (veiligheids)partners. Ook cybercrime kan op basis van de veiligheidsmonitor (CBS, 2020) inmiddels beschouwd worden als een vorm van veelvoorkomende criminaliteit. Daarnaast geven steeds meer gemeenten aan dat zij een rol (willen) spelen bij de aanpak van cybercrime (van Gemeren, 2019, p. 61). In dit onderzoek worden de taken en verantwoordelijkheden van organisaties binnen de governance in kaart gebracht, waarbij de focus ligt op het onderdeel 'bedrog en diefstal'. In essentie gaat het om het stelen van informatie of het illegaal verkrijgen van voorwerpen van waarde van individuen of organisaties met behulp van digitale middelen (Holt & Bossler 2014, p. 25).

1.2 Doelstelling

De doelstelling van het onderzoek is inzicht verschaffen in de actoren en samenhang van governance netwerken ten aanzien van het thema bedrog en diefstal binnen cybercrime, ten einde aanbevelingen te doen aan het Veiligheidsnetwerk Oost-Nederland hoe het governance network omtrent cybercrime vorm te geven.

1.3 Hoofdvraag

Om de informatie te vergaren waarmee aan deze doelstelling kan worden voldaan is de volgende onderzoeksvraag geformuleerd: *'Welke actoren zijn betrokken bij de aanpak van bedrog en diefstal binnen de cybercrime, welke taken en verantwoordelijkheden hebben deze actoren en in hoeverre verhoudt de samenwerking ten aanzien van cybercrime van het Veiligheidsnetwerk Oost-Nederland zich tot de randvoorwaarden voor succesvolle samenwerking in een governance network?'*

1.4 Deelvragen

Om tot beantwoording van de geformuleerde probleemstelling te komen, is een aantal deelvragen opgesteld die hieronder worden weergegeven.

1. *Wat is cybercrime volgens gemeenten en de experts uit het werkveld?*
2. *Hoe ziet bedrog en diefstal in de praktijk eruit volgens gemeenten en de experts?*
3. *Hoe ziet de huidige samenwerking op het gebied van bedrog en diefstal eruit?*
4. *Welke rollen en verantwoordelijkheden hebben de betrokken actoren binnen de veiligheidsketen?*

5. *Welke kansen/verbeteringen zien gemeenten en experts om de weerbaarheid van inwoners (tegen bedrog en diefstal) te vergroten?*

1.5 Maatschappelijke en wetenschappelijke relevantie

Cybercrime kan om meerdere redenen gezien worden als een '*wicked problem*', het gaat om een complex vraagstuk, bestaande uit talloze verschijningsvormen die in de loop der tijd onderhevig zijn aan verandering. De technologische ontwikkeling staat daarbij niet stil. De toenemende digitalisering van de samenleving biedt criminelen nieuwe kansen om slachtoffers te maken. Daarnaast wanen cybercriminelen zich veilig en anoniem vanwege de lage pakkans in vergelijking tot de klassieke vormen van criminaliteit. Kenmerkend daarbij is de gezamenlijke inspanning van de overheid, markt en samenleving (Van Steden, 2011 p. 49). Cybercrime overschrijdt niet alleen de bestuurlijke kaders, maar ook disciplinaire en territoriale grenzen. Daders kunnen vanuit Nederland opereren via verschillende servers in het buitenland waar de Nederlandse autoriteiten geen samenwerkingsafspraken mee heeft. Hierdoor loopt de opsporing en vervolging vertraging op en lijken daders vrij spel te hebben op het internet. De dader hoeft daarnaast geen fysiek contact te hebben met de (potentiele) slachtoffers, waardoor een duidelijk signalement van de dader onbekend blijft. Slachtoffers kunnen immers op basis van willekeur uitgekozen worden doordat deze personen de gelegenheid bieden om in te breken. Daarnaast zitten de betrokken actoren bij de aanpak van cybercrime grotendeels vast in de bestaande systemen en structuren die niet flexibel zijn. De kennis en informatiepositie van de politieorganisatie zijn zeer beperkt (Helsloot & Groenendaal, 2014). De traditionele strafrechtelijke keten heeft externe partijen nodig om tot opsporing en vervolging over te gaan. Dit maakt de aanpak van cybercrime diffuus en complex. Het onderzoek beoogt een bijdrage te leveren aan de doelstelling van het team Cyber van het Veiligheidsnetwerk Oost-Nederland door de governance in kaart te brengen. De samenwerking tussen meerdere partijen in een governance network is een kleine stap richting een weerbare samenleving. Cybercrime kan immers de digitale infrastructuur in Nederland verstoren of volledig tot stilstand brengen (WRR, 2019). Digitale ontwrichting heeft impact op het vertrouwen van burgers in de democratische rechtsstaat.

Dit onderzoekt beoogt ook een wetenschappelijke bijdrage te leveren aan de kennis over de veranderende relatie tussen overheid, traditionele strafrechtelijke instituties en andere partijen bij de aanpak van cybercrime. Digitalisering brengt grote veranderingen teweeg in de relatie tussen het bestuur en de bestuurden. Tussen het bestuur en de bestuurden vormt zich een digitale interface. Bestuurders hebben voortaan vooral te maken grote databestanden die worden benaderd met algoritmen en datamining. Burgers hebben voortaan de maken met digitale loketten en overheidsberichten via de DigiD-inbox. Met dit onderzoek wordt beoogd een bijdrage te leveren aan de bestaande kennis rondom het begrip governance network en het verschijnsel digitalisering. Daarnaast tracht dit onderzoek van toegevoegde waarde te zijn omtrent het functioneren van governance networks, in het bijzonder bij de bestrijding van cybercrime. Daarnaast schept het onderzoek een beeld van de verschillende wijzen waarop regionale veiligheidsnetwerken omgaan met de aanpak van cybercrime.

1.6 Voorbeschouwing theoretisch kader

Cybercrime kan gezien worden als '*wicked problem*'. Dit bemoeilijkt het beleid dat is gericht op de aanpak van cybercrime. Het gaat om een complex vraagstuk bestaande uit talloze verschijningsvormen die in de loop der tijd onderhevig zijn aan verandering. Bij de aanpak van cybercrime zijn meerdere

beleidsmakers en besluitvormers betrokken met uiteenlopende belangen en verantwoordelijkheden, zowel nationaal als internationaal. Daarnaast is de digitale omgeving aan snelle verandering onderhevig, waardoor de aanpak van cybercrime op dit moment nog veel alternatieve beleidsbenaderingen kent en uitkomsten en effecten van beleid onzeker zijn (Dunn, 2008). Daarnaast is er sprake van een verschuiving van offline naar online criminaliteit (Cuyper & Weijters, 2016). Dit wordt deels veroorzaakt door een steeds sterkere verplaatsing van fysieke transacties naar digitale transacties. In sommige delen van onze maatschappij is die digitalisering verder voortgeschreden (Facebook, Marktplaats, banken, TikTok, EBay) dan in andere sectoren (vrachtverkeer, supermarkten en onderwijs). Met de digitalisering van de maatschappelijke transacties verplaatst zich ook de criminaliteit. Van offline geleidelijk naar online. Ook de overheden die belast zijn met handhaving zullen deze trend moeten volgen. Er is al met al sprake van verweving tussen cybercrime, gedigitaliseerde criminaliteit en traditionele vormen van criminaliteit (Boerman et al., 2017). Minister Fred Grapperhaus bevestigt het beeld dat cybercrime zich continu blijft ontwikkelen en zet om die reden in op flexibiliteit en samenwerking bij de integrale aanpak van cybercrime (Ministerie van Justitie en Veiligheid, 2019). In het theoretisch kader wordt allereerst het begrip ‘governance network’ nader gedefinieerd en vanuit bestuurskundig perspectief uitgewerkt. Het oprichten van een governance network is noodzakelijk om gezamenlijk een gedeeld probleem op te lossen en output te genereren die individuele actoren niet zonder de hulp van andere partijen kunnen oplossen” (Gray, 1985, p. 911-936).

1.7 Voorbeschouwing methodologisch kader

Om de deelvragen te beantwoorden wordt er een interpretatieve onderzoeksbenadering gekozen, met als doel om te begrijpen hoe gemeenten en experts een rol spelen bij de aanpak van bedrog en diefstal binnen de cybercrime. We willen weten hoe zij met dit maatschappelijke verschijnsel worden geconfronteerd. Wat denken zij er aan te kunnen doen? De focus van het onderzoek ligt bij de interactie tussen de betrokken actoren. Door individuele vraaggesprekken te voeren kunnen de verschillende actoren begrepen worden vanuit hun eigen positie en context. Diepte-interviews met vertegenwoordigers van de deelnemende organisaties sluiten het best aan bij de doelstelling van dit onderzoek.

Om antwoord te geven op de onderzoeksvragen, wordt gebruik gemaakt van een tweetal dataverzamelingsmethoden: diepte-interviews en documentenanalyse. De interviews worden afgenomen bij verschillende gemeenten in Oost-Nederland en bij experts van relevante organisaties op het gebied van cybercrime. Daarnaast worden de beleidsdocumenten van gemeenten en experts uit het werkveld doorzocht op tijd, middelen en beleidsprioriteit van het thema cybercrime.

1.8 Leeswijzer

In dit eerste hoofdstuk wordt ingegaan op de aanleiding en doelstelling van dit onderzoek en worden de bijbehorende probleemstelling en onderzoeksvragen beschreven. Daarnaast worden de wetenschappelijke en maatschappelijke relevantie van het onderzoek nader toegelicht. In hoofdstuk 2 wordt het beleidskader gereconstrueerd. Hoofdstuk 3 gaat in op de theoretische aspecten van dit onderzoek. Vervolgens wordt de onderzoeksmethodiek beschreven in hoofdstuk 4, waarnaar de onderzoekresultaten in hoofdstuk 5 worden beschreven. In hoofdstuk 6 volgt de conclusie, gevolgd door de aanbevelingen en reflectie op het uitgevoerde onderzoek.

2. Beleidskader

2. Beleidskader

Het hoofdstuk begint met een uiteenzetting over het Veiligheidsnetwerk Oost-Nederland. Daarna volgt een beschrijving van de context waarbinnen het Veiligheidsnetwerk Oost-Nederland werkzaam is. Vervolgens komen de betrokken actoren en hun doelstellingen op het gebied van cybercrime/gedigitaliseerde veiligheid aan bod.

2.1 Veiligheidsnetwerk Oost-Nederland

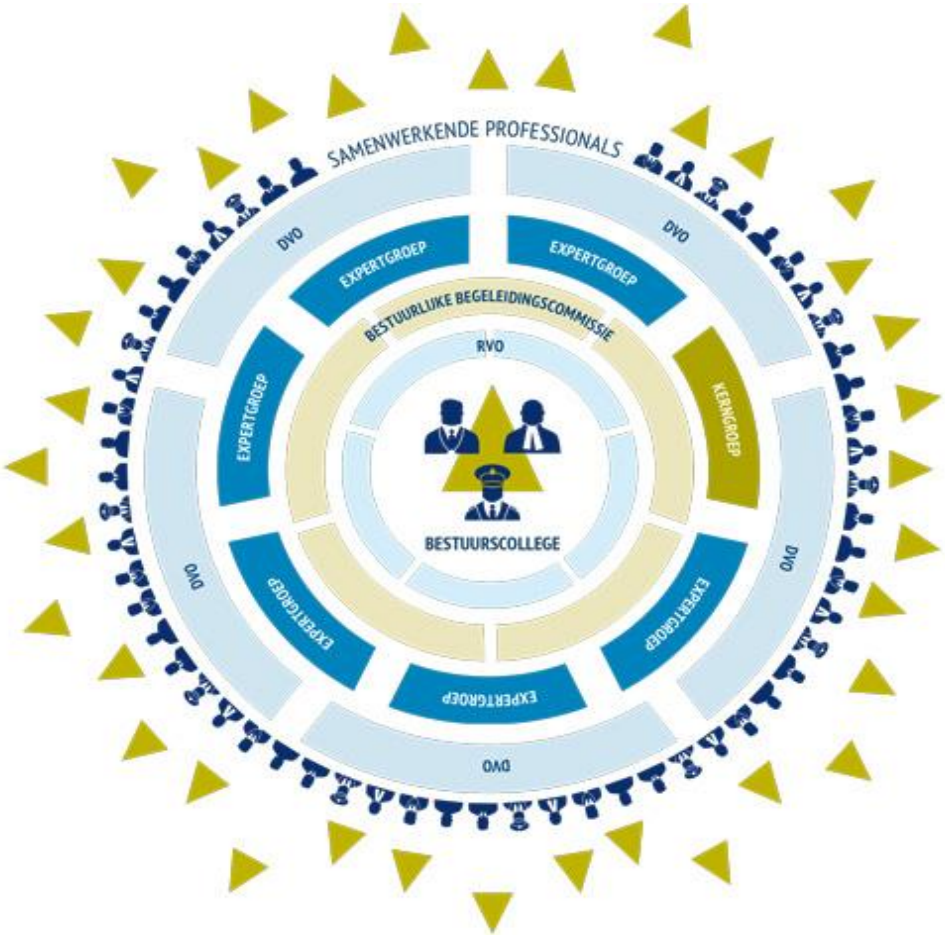
Het Veiligheidsnetwerk Oost-Nederland is een regionaal samenwerkingsverband van veiligheidspartners in de provincie Gelderland en Overijssel. De focus van het veiligheidsnetwerk richt zich op sociale veiligheid. Het gaat hierbij om de mate waarin mensen beschermd zijn en zich beschermd voelen tegen persoonlijk leed door criminaliteit, overtredingen en overlast door andere mensen (Stol, W., & Tielenburg, C. 2011). Het Veiligheidsnetwerk Oost-Nederland heeft als doel om gezamenlijk criminaliteit en onveiligheid aan te pakken. De betrokken veiligheidspartners binnen het netwerk ontwikkelen producten, bundelen kennis, expertise en best practices en wisselen informatie onderling uit. Het Veiligheidsnetwerk Oost-Nederland maakt gebruik van bestaande structuren in de regio en verbindt relevante partners en stimuleert nieuwe aanpakken op het gebied van sociale veiligheid. Daarnaast dient het veiligheidsnetwerk ook het vertrouwen van burgers in de overheid te versterken.

Het Veiligheidsnetwerk Oost-Nederland richt zich op een aantal speerpunten die zijn vastgelegd in de Veiligheidsstrategie (2019), te weten: kwetsbare personen (zorg en veiligheid), ondermijning, cybercrime/gedigitaliseerde criminaliteit en informatiegestuurd werken. Deze speerpunten zijn vastgesteld door de 76 gemeenten, politie, Openbaar Ministerie. De bestuurlijke inbedding van de Veiligheidsstrategie is geborgd in de Bestuurlijke Begeleidingsgroep (BBG). In de Bestuurlijke Begeleidingsgroep zit vanuit elk district één burgemeester (tevens portefeuillehouder van een vastgesteld speerpunt), een vertegenwoordiger van de politie en een afgezant van de parketleiding van het OM. De projectleider en coördinator sluiten eveneens aan bij dit overleg. In het verleden werden speerpunten geprioriteerd op basis van de vastgestelde integrale veiligheidsplannen van alle gemeenten van Oost-Nederland en de beleidsnota's van politie en Openbaar Ministerie. Nu worden de prioriteiten geagendeerd door de deelnemende burgemeesters in het Districtelijk Veiligheidsoverleg (DVO), op voorwaarde dat de samenwerking op het niveau van Oost-Nederland meerwaarde heeft. De Bestuurlijke Begeleidingsgroep (BBG) begeleid vervolgens en zorgt voor borging in de uitvoering.

2.2 Context

Het Veiligheidsnetwerk Oost-Nederland kent de volgende drie overlegstructuren: bestuurlijke besluitvorming, bestuurlijke afstemming en ambtelijke uitvoering. De bestuurlijke besluitvorming vindt tweejaarlijks plaats door het bestuurscollege. Het bestuurscollege, bestaat uit alle burgemeesters, de hoofdofficier van justitie en de politiechefs van Oost-Nederland (zie figuur 2.1). Zij komen bij elkaar naar aanleiding van het Regionaal Veiligheidsoverleg (RVO) onder leiding van regioburgemeester Hubert Bruls van Oost-Nederland. Daarnaast is Onno van Veldhuizen regioburgemeester van Twente en tevens voorzitter van zowel de Bestuurlijke Begeleidingsgroep (BBG) als het Districtelijk Veiligheidsoverleg (DVO) Twente. Hierdoor vormt regioburgemeester Onno van Veldhuizen de *'linking pin'* tussen de Bestuurlijke Begeleidingsgroep en het Regionaal Veiligheidsoverleg (RVO). Naast het bestuurscollege vormen de lokale driehoeken ook een bestuurlijk

besluitvormingsoverleg op lokaal niveau. De lokale driehoek bestaat uit de burgemeester, een officier van justitie en de politiechef. De burgemeester heeft op lokaal niveau het gezag over de openbare orde en veiligheid en de officier van justitie de regierol over de opsporing van strafbare feiten. In samenspraak worden de lokale prioriteiten en de inzet van politie vastgesteld, op basis van het lokale veiligheidsbeleid. Zij zijn gezamenlijk verantwoordelijk voor de uitvoering van de Veiligheidsstrategie.



Figuur 2.1 Netwerkstructuur Veiligheidsnetwerk Oost-Nederland

Vervolgens worden de strategische doelen door expertteams uitgewerkt in projectplannen met tactische en operationele doelstellingen. Het expertteam is verantwoordelijk voor de ambtelijke uitvoering en dient allereerst inzichtelijk te maken wat de aard en omvang van het probleem is. Vervolgens worden de taken en verantwoordelijkheden van de betrokken actoren vastgesteld en mogelijke handelingsperspectieven onderzocht. Op basis daarvan zoekt het expertteam aansluiting en afstemming bij bestaande initiatieven en samenwerkingsverbanden. Tot slot dienen de multidisciplinaire expertteams budget en projectsubsidies aan te vragen en in de wacht te slepen voor de vastgestelde projecten.

2.3 Actoren

Het Veiligheidsnetwerk Oost-Nederland werkt samen met verschillende veiligheidspartners. De inzet van deze partners is nodig om de strategische, tactische en operationele doelstellingen van de Veiligheidsstrategie te halen. Betrokken actoren dragen bij aan de samenwerking door het uitwisselen van informatie, het maken van werkafspraken en te participeren in expertteams en deel te nemen aan

projecten. Elk expertteam bestaat uit leden van verschillende organisaties en wordt voorgezeten door een burgemeester. De burgemeester is daarmee tegelijkertijd ook bestuurlijk portefeuillehouder. Daarnaast wordt op elk thema binnen de veiligheidsstrategie een ambtelijk trekker aangesteld. Aan het expertteam Cybercrime nemen vertegenwoordigers van de volgende organisaties deel:

- Gemeenten: Winterswijk, Ede, Neder-Betuwe, Rijssen-Holten, Nijmegen, Renkum, Zwarte Waterland, Deventer en Bronckhorst.
- Regionaal Informatiepunt Integrale Veiligheid (RCIV)
- Politie Oost-Nederland
- Hogeschool Saxion
- Openbaar Ministerie
- Space53
- Veiligheidsregio IJsselland
- Veiligheidsregio Gelderland-Zuid
- Provincie Overijssel

2.4 Doelstellingen

Het Veiligheidsnetwerk Oost-Nederland heeft naar aanleiding van vragen van de aangesloten 76 gemeenten, het OM en de politie het thema cybercrime/gedigitaliseerde criminaliteit als speerpunt gekozen. Het speerpunt bevindt zich momenteel in de verkennende fase. Het onderwerp wordt nader afgebakend. Er wordt een overzicht gemaakt van wie welke taken en verantwoordelijkheden heeft binnen de veiligheidsketen. Het Uitvoeringsplan Cybercrime 2019-2020 van het Veiligheidsnetwerk Oost-Nederland bestaat uit de volgende doelstellingen:

- de verkenning van een eventuele verschuiving in de criminaliteit op basis van de politiecijfers van Oost-Nederland. Deze verkenning dient inzichtelijk te maken in welke mate de criminaliteit van de fysieke wereld naar de digitale wereld verschuift.
- het uitwerken van een overzicht van de governance op het gebied van cybercrime. De betrokken organisaties dienen in kaart te worden gebracht waaraan ook handelingsperspectieven zijn verbonden. Dit overzicht dient de verantwoordelijkheden en taken van de actoren vast te stellen binnen de volgende schakels van de veiligheidsketen: proactie, preventie, en repressie. Daarnaast dient het ook antwoord te geven op de vraag of de overheid een rol speelt bij een bepaald handelingsperspectief.
- te onderzoeken of op dit terrein meer kan worden samengewerkt met het bedrijfsleven.
- tenslotte wordt gestreefd naar algehele deskundigheidsbevordering en samenwerking op het gebied van cybercrime/gedigitaliseerde criminaliteit.

2.5 Cybercrime in Oost-Nederland

De toenemende digitalisering leidt tot stijging van het aantal cybercrime zaken die worden gemeld bij de politie (2015). Uit het meerjarenbeleidsplan 2015-2018 van de politie Oost-Nederland blijkt dat het aantal zaken in de afgelopen jaren is toegenomen. Dit betreft het aantal registraties van computercriminaliteit bij de politie eenheid Oost-Nederland (zie figuur 2.2) Het aantal aangiften is echter afgenomen van 385 in 2015 naar 10 in 2018.

Op basis van de cijfers kan geconcludeerd worden dat de aangiftebereidheid de laatste jaren tot 2018 is gedaald. Uitgaande van 76 gemeenten in Oost-Nederland betekent dit 5 aangiften per gemeente in

2015 naar 2 aangiften per gemeente in 2018. Uitgaande van het aantal aangiften per gemeente baart dat geen reden tot zorg. Maar misschien zijn de aangiften geen goede indicator. Het aantal opgehelderde zaken ligt in het tijdvak van 2015 tot 2018 op 8,4%. Hieruit kan worden geconcludeerd dat het aantal zaken dat werkelijk leidt tot een vervolging door het Openbaar Ministerie zeer gering is. Hoewel het aantal aangiften van cybercrime door de jaren heen omlaag ging, zijn er niet meer zaken opgelost. Op basis van deze data kan gesteld worden dat het voor burgers en ondernemers niet loont om aangifte te doen.

	aangiften	opgehelderde zaken	aantal verdachten
2015	385	30	45
2016	215	20	25
2017	270	15	20
2018	140	20	50

Figuur 2.2 Aantal aangiften en vervolging (politie, 2018)

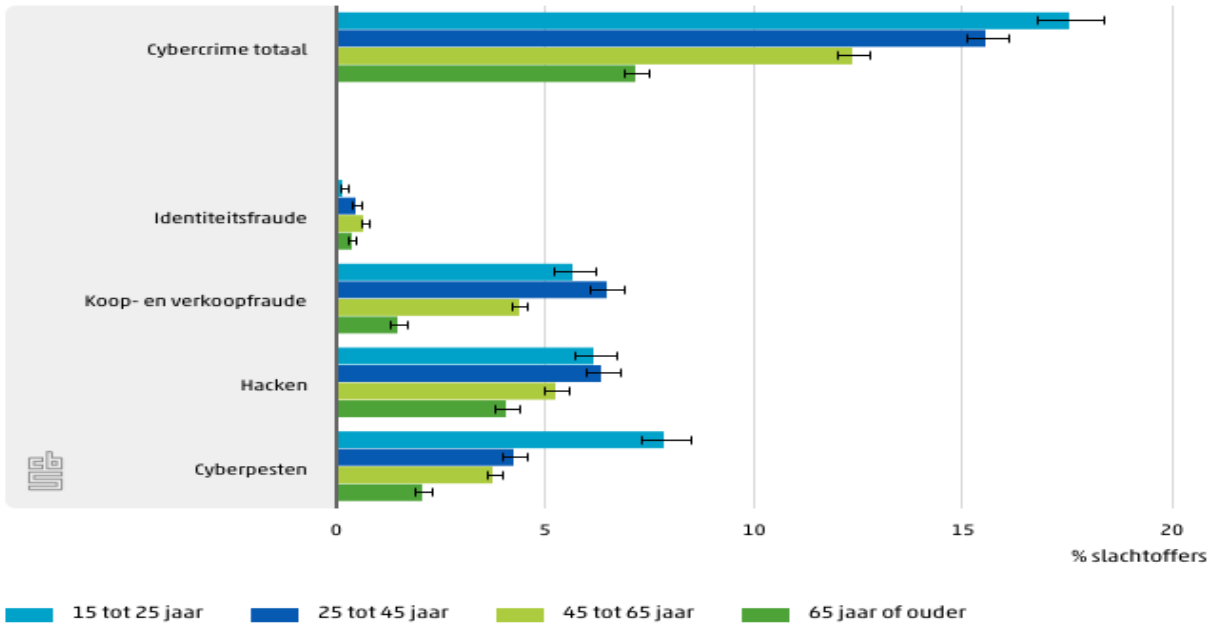
De politie Oost-Nederland heeft de afgelopen jaren ingezet op meer capaciteit en expertise bij de districten en lokale teams, waarbij de aandacht is gericht op de aanpak van cybercrime (politie, 2020). Uit het meerjarenbeleidsplan blijkt dat de focus ligt op de volgende thema's: aantasting van de vitale infrastructuur, verstoring van online dienstverlening, gegevensdiefstal en identiteitsfraude. In het meerjarenbeleidsplan van 2019-2022 is de focus verschoven naar de landelijke top 5 van cybercriminaliteitsvormen: hacken, digitale fraude, phishing, sexting, afpersing en cyberpesten. De politie eenheid heeft in 2019 besloten een cybercrimeteam op te richten, bestaande uit 18 medewerkers. Door deze kennis en expertise te bundelen verwacht de politie een breed scala aan digitale criminaliteit aan te pakken (politie, 2020).

2.6 Slachtofferschap cybercrime

Uit de Veiligheidsmonitor van het CBS (2019) blijkt dat 13% van de Nederlanders van 15 jaar of ouder slachtoffer wordt van cybercrime. Deze vorm van digitale criminaliteit maakte vorig jaar bijna 2 miljoen slachtoffers in heel Nederland. De meeste mensen worden volgens het CBS (2019) slachtoffer van hacken, gevolgd door koop- en verkoopfraude, cyberpesten en identiteitsfraude. Dit verschilt overigens per leeftijdsgroep. In figuur 2.3 zijn 4 leeftijdsgroepen en verschillende vormen van cybercrime te onderscheiden. Uit deze grafiek blijkt dat jongeren tussen de 15 tot 25 jaar vaker slachtoffer van cybercrime worden dan alle andere leeftijdsgroepen. Uit de cijfers blijkt dat jongeren met name kwetsbaar zijn voor cyberpesten. Daarnaast hebben jongeren tussen de 15 tot 25 jaar bijna 2,5 keer meer kans lopen om slachtoffer te worden van cybercrime dan ouderen van 65 jaar of ouder. De jongste leeftijdsgroep wordt gevolgd door de leeftijdsgroepen van middelbare leeftijd en tot slot de oudere leeftijdsgroep. En mogelijk verklaring is in het aantal uren dat jongeren tussen de 15 tot 25 jaar per dag besteden aan social media en andere online activiteiten (CBS, 2018).

Hacken is de meest voorkomende vorm van cybercrime en betreft met name het inbreken op een website of profielsite (CBS, 2019). De meeste slachtoffers behoren tot de leeftijdscategorie tussen de 25 tot 45 jaar. Bij koop- en verkoopfraude zijn met name de leeftijdsgroepen 25 tot 45 jaar kwetsbaar, gevolgd door de leeftijdsgroep 15 tot 25 jaar. Koopfraude komt vaker voor dan verkoopfraude en betreft het niet leveren van de gekochte goederen of diensten. Verkoopfraude is het niet betalen van goederen of diensten (CBS, 2019). De laatste categorie die het CBS onderscheidt

in de verschillende vormen van cybercrime is identiteitsfraude. Bij deze vorm van criminaliteit worden relatief veel mensen van middelbare leeftijd en ouderen getroffen in vergelijking tot de jongeren.

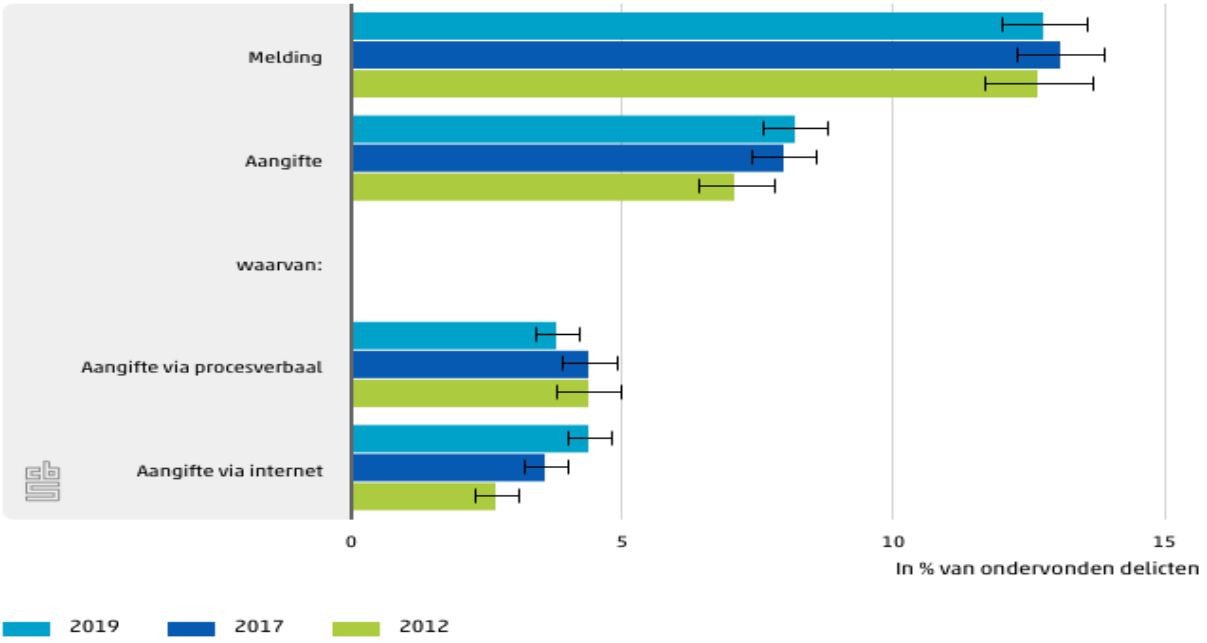


Figuur 2.3 slachtofferschap cybercrime naar leeftijd (CBS, 2019)

Op basis van de slachtoffer gegevens van het CBS kan geconcludeerd worden dat het aantal aangiften bij de politie (zie paragraaf 2.5) niet in verhouding staat tot het aantal slachtoffers van cybercrime in Nederland. Daarnaast bevestigt dit het beeld dat lang niet alle slachtoffers aangiften doen van cybercrime.

2.7 Meldingsbereidheid cybercrime

De aangiftebereidheid van slachtoffers van cybercrime ligt beduidend lager dan bij traditionele vormen van offline criminaliteit. Uit cijfers van de Veiligheidsmonitor van het CBS (2019) blijkt dat slechts 8,2



Figuur 2.4 Melding en aangiften cybercrime (CBS, 2019)

procent van de slachtoffers aangifte doet van cybercrime in tegenstelling tot 22,9 procent bij traditionele vormen van criminaliteit. Hoewel de meldingsbereidheid al jaren daalt deed in 2012 nog circa 28,7 procent van de slachtoffers aangifte. Figuur 2.4 laat een verontrustend beeld zien van een zeer lage meldingsbereidheid op het gebied van cybercrime in vergelijking tot traditionele vormen van criminaliteit. Uit de cijfers blijkt eveneens dat maar één op de twaalf cyber incidenten werkelijk wordt omgezet in een aangifte. Tot slot kan op basis van de statistieken geconcludeerd worden dat ongeveer de helft van de aangiften online wordt gedaan en het aantal aangiften via internet jaarlijks stijgt, terwijl het aantal aangiften via een proces verbaal juist een daling laat zien. Op basis van het aantal slachtoffers en het aantal daadwerkelijke aangiften van cybercrime kan geconcludeerd worden dat veel incidenten niet geregistreerd worden bij de politie, ofwel een groot deel van deze vormen van criminaliteit blijft verborgen: er is sprake van een omvangrijk *'dark number'*.

De lage meldingsbereidheid wordt eveneens bevestigd in een onderzoek 'Slachtoffer van online criminaliteit, wat nu?' van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving en de Erasmus Universiteit (2020), waarbij slechts één op zeven inwoners en ondernemers van cybercrime aangifte doet van cybercrime bij de politie. Daarnaast blijkt uit hetzelfde onderzoek dat de achterliggende reden om geen aangifte te doen met name zijn: "ik los het zelf op" en "het heeft geen zin, de politie zal er niets aan doen".

3. Theoretisch kader

3. Theoretisch kader

In dit hoofdstuk worden de theoretische begrippen die centraal staan in dit onderzoek uiteengezet en gedefinieerd. Allereerst wordt het begrip cybercrime gedefinieerd, waarnaar ook cyberweerbaarheid en het begrip de veiligheidsketen uiteengezet worden. Vervolgens worden de theoretische uitgangspunten van de governance network beschreven.

3.1 Definiëring cybercrime

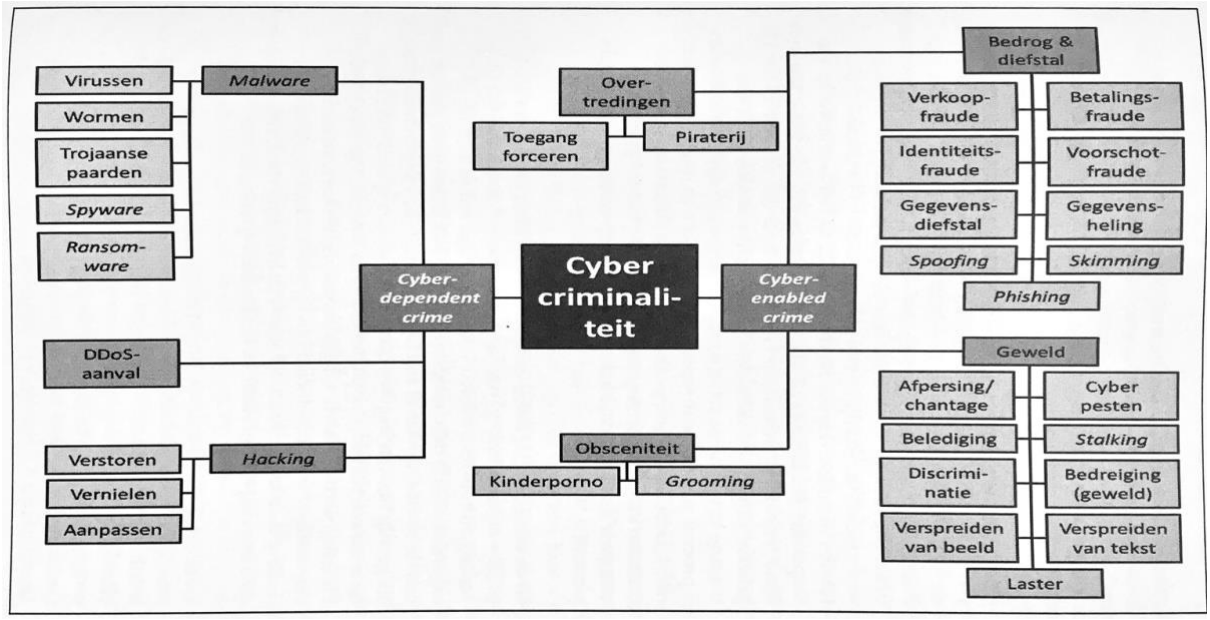
In de literatuur is geen eenduidige definitie van cybercrime te vinden. Voordat dit onderzoek verder inzoomt op het onderwerp is het van belang om inzicht te krijgen in de verschillende definities van cybercrime. Cybercrime wordt in de literatuur regelmatig vervangen door 'digitale criminaliteit', 'hightech crime' of 'computer-related crime' (WODC, 2016). De definitie van cybercrime wordt zowel nationaal als internationaal anders ingevuld. De Europese Commissie geeft aan dat het gaat om criminele handelingen waarbij cybercriminelen gebruik maken van elektronische communicatienetwerken en informatiesystemen (European Commission, 2016) De Europese Commissie legt tevens de nadruk op het feit dat cybercrime een wereldwijd probleem is. Dit in tegenstelling tot de Verenigde Naties, zij stellen dat een strikte definitie voor cybercrime niet nodig is, zolang het niet in een juridische context beschreven staat (UNODC, 2013).

De (cyber)criminoloog David Wall (2007) geeft de volgende definitie: 'misdrijven met behulp van de computer'. Door gebruik te maken van deze definitie wordt meer richting gegeven aan de inhoudelijke vormen van cybercrime. Hierbij kan gedacht worden aan '*malware*', waarbij kwaadaardige software wordt gebruikt om een bepaald computersysteem te verstoren waardoor gevoelige informatie ontvreemd kan worden en toegang verkregen kan worden tot private computersystemen. Deze vorm van criminaliteit bestond nog niet voorafgaand aan het computertijdperk. Wel staat vast dat het gebruik van ICT een wezenlijke rol moet spelen bij het plegen van een misdrijf. Het definiëren van cybercrime wordt duidelijker aan de hand van het schema van de Politieacademie (2009). In het rapport 'Verkenning cybercrime in Nederland 2009' wordt cybercrime als volgt gedefinieerd: "alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt". In de literatuur wordt onderscheid gemaakt tussen cybercrime in ruime en in enge zin (Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013).

	Cybercrime: alle vormen van criminaliteit waarbij ICT een wezenlijke rol speelt	
Categorie	Cybercrime in enge zin	Cybercrime in ruime zin
Uitwerking	Criminele activiteiten waarbij ICT zowel instrument als doelwit is	Criminele activiteiten waarbij de inzet van ICT als instrument van wezenlijk belang is voor het plegen van het delict en waarbij ICT niet het doelwit is

Figuur 3.1 Definitie van cybercrime (Politieacademie, 2009)

Deze verdeling wordt gemaakt aan de hand van welke rol ICT inneemt bij het misdrijf. Bij cybercrime in enge zin is Informatie- en Communicatietechnologie (ICT) zowel het instrument als het doel. Cybercrime in enge zin wordt in de literatuur ook wel aangeduid als *'computer-dependent crime'* (zie figuur 3.2).



Figuur 3.2 Overzicht verschillende vormen van cybercrime (Spithoven, 2020, p.49)

In deze categorie vallen verschillende soorten cybercrime die niet zonder computer uit te voeren zijn. Holt en Bossler (2014) rekenen de volgende subcategorieën tot cyber-dependent crime:

- De eerste subcategorie is *malware.* Deze vorm van cybercrime werkt door middel van opzettelijk kwaadaardige software waarmee systemen geïnfecteerd raken (Moser, Kruegel & Kirda, 2007: 421). Een andere benaming voor dit fenomeen is 'malicieuze software'. Malware kan zich in verschillende gedaanten voordoen, namelijk: virussen, wormen, trojaanse paarden, spyware en ransomware. Een device kan op verschillende wijzen besmet raken met malware, zoals het klikken op een link in een e-mail of website (politie, z.d.). Malware kan ook geïnstalleerd worden op systemen door illegale en gekraakte software.
- De tweede subcategorie die Holt en Bossler onderscheiden is *hacking.* Onder hacking wordt het volgende verstaan: 'het zonder overleg en toestemming toegang forceren tot andermans computer, accounts en/of systemen met als doel deze te verstoren, vernielen of aan te passen' (Leukfeldt, 2016). Hacken kan door middel van verschillende technieken. Cybercriminelen kunnen op basis van een aantal basale privégegevens wachtwoorden raden, maar ook misbruik maken van lek in netwerken of computersystemen (Van der Hulst & Neve, 2008). Een hackpoging kan in essentie eenvoudig van aard zijn maar wordt doorgaans uitgevoerd door iemand met digitale kennis en vaardigheden (Van der Hulst & Neve, 2008). De motieven van daders lopen uiteen van financieel gewin tot ideologisch hacken om personen of organisaties bewust te maken van de risico's (Van der Hulst & Neve, 2008).
- De laatste subcategorie die Holt en Bossler onderscheiden binnen de cyber-dependent crime zijn '*Distributed Denial of Service'* (DDos-)aanvallen. Een DDos-aanval is een gerichte aanval op een computersysteem of netwerk, waardoor een website overbelast raakt. Dit kan veroorzaakt worden door één computer, in dat geval heet het een DoS-aanval. Meerdere computers kunnen samen een DDoS-aanval uitvoeren. In de praktijk gaat het vaak om

aanvallen van meerdere computers die met elkaar verbonden zijn. Deze computers vormen een zogenaamd '*botnet*', dit zijn meerdere computers die centraal aangestuurd kunnen worden (politie, z.d.). Als alle computer gelijktijdig één website bezoeken dan raakt het systeem overbelast waardoor de website of server crasht.

Een tweede definitie heeft betrekking op cybercrime in ruime zin. Daarbij wordt ICT enkel gebruikt als middel. Het gaat bij cybercrime in brede zin om traditionele vormen van criminaliteit. In de literatuur wordt dit vaak aangeduid met 'cyber enabled crime'. Het gaat bij deze vorm van criminaliteit met name om het verkrijgen van geld (UNODC, 2013). Holt en Bossler (2014) onderscheiden de volgende subcategorieën van cyber-enabled crime:

- De eerste subcategorie zijn *overtredingen*. In deze categorie worden de geldende grenzen van eigenaarschap overschreden (Holt & Bossler, 2014). Hiertoe behoren enerzijds het forceren van de toegang en anderzijds digitale piraterij. Dit betekent dat een persoon zich onrechtmatig toegang verschaft tot systemen of apparaten. Onder digitale piraterij wordt het volgende verstaan: het verkrijgen van digitale producten, zoals muziek, films en foto's zonder instemming van de eigenaar of auteur (Gopal et al., 2004; Higgins, Fell en Wilson, 2007).
- De tweede subcategorie van Holt en Bossler is *bedrog en diefstal*. Bij deze subcategorie horen verschillende verschijningsvormen. De meest voorkomende is *verkoopfraude* (Bloem & Harteveld, 2012). Bij verkoopfraude wordt er gefraudeerd met online handel, veilingfraude, of via advertenties op marktplaats of eBay (Van Wilsem, 2013; Leukfeldt, Domenie & Stol, 2010). Ook *phishing* is een vorm van digitale oplichting en gebeurt met name via e-mail, WhatsApp en sms – ook wel smishing genoemd - (politie, z.d.) Criminelen sturen slachtoffers valse betaalverzoeken of dirigeren hen naar (bank)websites waar de inloggegevens worden buitgemaakt. Een andere vorm van de subcategorie bedrog en diefstal is *skimming,* waardoor (bank)pasgegevens worden gekopieerd. Vervolgens wordt de pincode van het slachtoffer elders afgekeken om daadwerkelijk geld op te nemen. Geld kan ook afhandig worden gemaakt middels *voorschotfraude*. Hierbij proberen oplichters slachtoffers te bewegen om een gedeelte van de aanschafsom van een bepaalde dienst of product vooruit te betalen. Vervolgens wordt de daadwerkelijke dienst of product nooit geleverd. Andere vormen van voorschotfraude zijn datingfraude of Nigeriaanse fraude (politie, z.d.). Bij *identiteitsfraude* wordt de identiteit van het slachtoffer buit gemaakt, met het doel om deze te misbruiken (Grijpink, 2003). Een andere vorm is *spoofing,* waarbij daders een valse identiteit aannemen om betrouwbaar over te komen. Dit kan bijvoorbeeld door het vervalsen van een ogenschijnlijk betrouwbaar ogende website of e-mailadres. Bij gegevensdiefstal worden persoonlijke gegevens die niet bestemd zijn voor anderen buitgemaakt. Deze gegevens kunnen onrechtmatig in handen van kwaadwillende personen vallen door bijvoorbeeld een datalek. Hierdoor hebben criminelen toegang tot ongeoorloofde en onbedoelde toegang tot persoonlijke gegevens Als de persoonlijke gegevens afkomstig uit een datalek vervolgens worden doorverkocht dan kan dit bestempeld worden als gegevensheling.
- De volgende subcategorie die Holt en Bossler onderscheiden is (digitaal) *geweld*. Geweld via digitale middelen kent meerdere verschijningsvormen. Vast staat dat een kwaadwillende persoon schade kan toebrengen aan het slachtoffer. Dit kan door middel van afpersing of chantage, waarbij het slachtoffer onder bedreiging iets moet doen of laten. Een andere en veelvoorkomende vorm is *cyberpesten*, ofwel digitaal pesten. Het gaat hierbij om een stelselmatige vorm van geweld waarbij een kwaadwillende probeert het slachtoffer verbaal of psychologische schade toe te brengen (Veenstra e.a., 2005). *Belediging* is het opzettelijk

aantasten van iemands eer, reputatie en goede naam. *Laster* betreft het kwaadspreken over een ander. Bij *stalking* maakt een kwaadwillende persoon opzettelijk inbreuk op de privacy van een ander, waardoor het slachtoffer in zijn of haar vrijheid en veiligheid wordt beperkt (politie, z.d.). Dit kan door iemand voortdurend lastig te vallen, te volgen of contact te zoeken (WODC, 1998). *Discriminatie* betreft het maken van een ongeoorloofd onderscheid op basis van sekse, geloof of levensovertuiging. Onder *bedreiging* valt het dreigen met fysiek geweld of de dood tegen personen en/of eigendommen. Het *verspreiden van beeld of tekst* zonder toestemming van het slachtoffer valt eveneens onder geweld.

- De laatste subcategorie die Holt en Bossler onderscheiden binnen de cyber-enabled crime is obsceniteit. Binnen dit thema vallen seksueel getinte uitdrukkingen en het verspreiden van seksueel beeld en/of beeldmateriaal via digitale communicatie. Hieronder valt enerzijds kinderporno en anderzijds '*grooming*'. Bij dit laatste fenomeen worden kinderen digitaal in de val gelokt. Hierbij legt een volwassen persoon contact met een minderjarige, met de intentie om elkaar te ontmoeten. Bij de ontmoeting wordt meestal een poging gedaan om pornografisch materiaal te vast te leggen. De persoon die deze grooming uitvoert bedient zich van een fictieve identiteit, vaak aanzienlijk jonger dan de echte leeftijd van de dader.

3.2 Cyberweerbaarheid

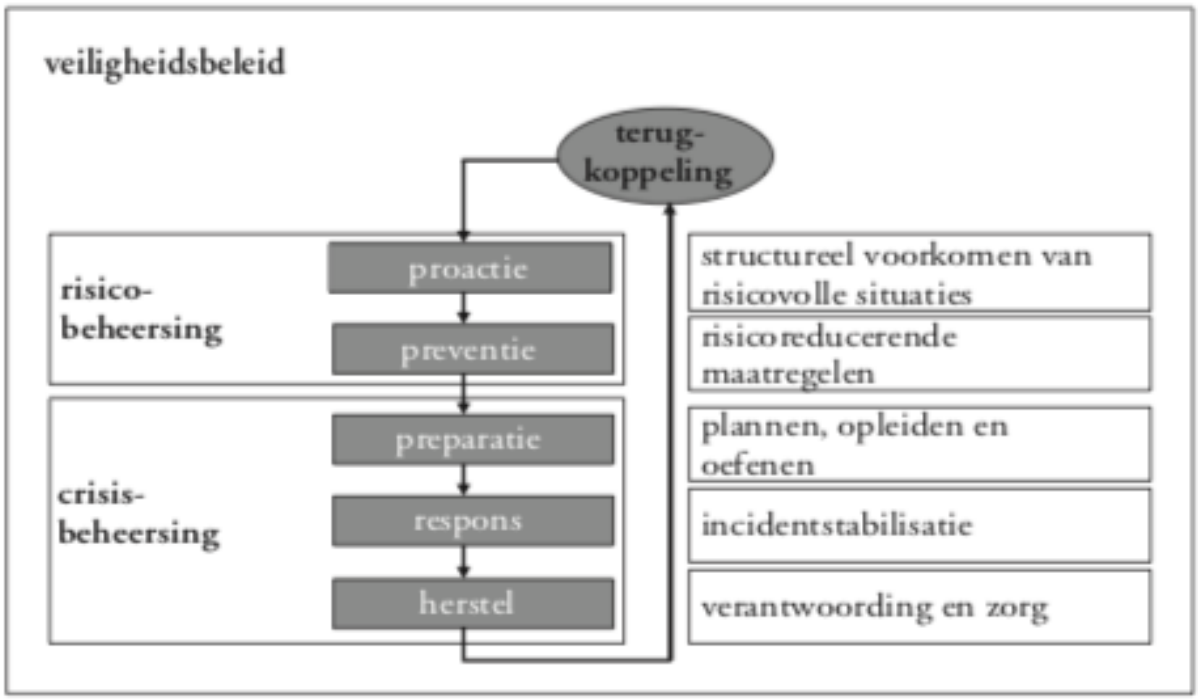
Uit cijfers van het CBS blijkt dat jaarlijks 1,2 miljoen mensen te maken hebben met digitale criminaliteit (2018). Dit staat in schril contrast met het feit dat twee derde van de Nederlanders denken dat hun eigen kennis over digitale en online veiligheid goed genoeg is (Motivaction, 2019). Om deze vorm van criminaliteit te voorkomen, is het van belang dat potentiële slachtoffers 'cyberweerbaar' worden. Het begrip *cyberweerbaarheid* is een containerbegrip en kan breed opgevat worden. Opvallend is dat de term cyberweerbaarheid nog weinig voorkomt in de Nederlandse literatuur. Het begrip wordt in verschillende documenten gebruikt zonder enige definitie. Het Nationaal Cyber Security Centrum (2016) definieert cyberweerbaarheid als de mogelijkheid om gebruik te maken van ICT zonder het risico of kans om daarbij geraakt te worden door schade. Het gaat hierbij om mogelijke risico's door misbruik, maar ook door verstoring of uitval vanwege beperkte beschikbaarheid van ICT. Daarnaast kunnen schendingen van vertrouwelijkheid van informatie of schade aan de integriteit van bepaalde informatie ontstaan. Spithoven (2020) stelt dat de onbekendheid met de risico's en een laag zelfvertrouwen van mensen in het werken met de computer en internet, een belangrijke bijdrage levert aan het onderbewustzijn en het vertonen van onveilig gedrag van mensen.

Tot op heden is het onduidelijk hoe Nederlanders zich beschermen tegen cybercrime (WODC, 2019). Dit wordt veroorzaakt doordat mensen ander gedrag vertonen dan dat zij zelf in interviews aangeven te doen. De interviewgegevens vormen dus geen goede afspiegeling van het feitelijke cybergedrag. Een mogelijke verklaring hiervoor kan gerelateerd worden aan het fenomeen: de '*cybersecurity paradox'* (Van Der Zee, 2018). Uit onderzoek blijkt dat de meeste mensen waarde hechten aan cybersecurity (Madden & Rainie, 2015), terwijl dit niet overeenkomt met de online gedragingen (Smith & Louis, 2008; Spiekermann, Grossklags, & Berendt, 2001). Je zou ook kunnen zeggen dat er sprake is van naïviteit. Ook in andere onderzoek blijkt dat veel respondenten sociaal wenselijke antwoorden geven die veraf staan van hun feitelijke gedrag. Naast burgers hebben ook ondernemers (bedrijven) te maken met een stijging van het aantal cyberincidenten. Uit onderzoek blijkt dat belangrijke delen van het Midden en Kleinbedrijf (MKB) te weinig middelen en kennis heeft om cyberdreigingen te voorkomen en de risico's voor hun onderneming te onderkennen (Verhagen, 2006). Spithoven (2020)

en Misana-ter Huurne et al. (2020) stellen dat cyberweerbaarheid bestaat uit een combinatie van enerzijds risicobewustzijn en anderzijds feitelijk zelfbeschermend gedrag.

3.3 De veiligheidsketen

Het reduceren van risico's en het waarborgen van veiligheid wordt in Nederland onderscheiden aan de hand van het begrip de veiligheidsketen (Tweede Kamer, 1992). Aan de hand van de veiligheidsketen worden de risico's systematisch inzichtelijk gemaakt (Stol e.a., 2016). Het Nederlandse model is afgeleid van het oorspronkelijke model dat in de Verenigde Staten ontwikkeld is. De Amerikaanse Federal Emergency Management Agency (FEMA) ontwikkelde de veiligheidsketen met vier schakels: mitigation (vermindering), preparedness (paraatheid), response (reactie) en recovery (herstel). De huidige veiligheidsketen bestaat uit de volgende vijf schakels: proactie, preparatie, preventie, repressie en nazorg (figuur 3.3).



Figuur 3.3 De Veiligheidsketen (Helsloot, 2007, p. 17).

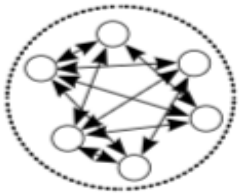
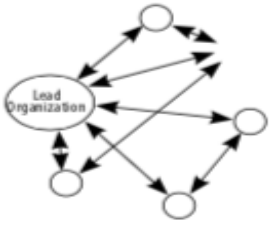
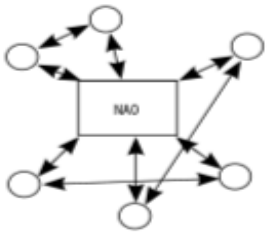
Een belangrijke uitkomst van het denken in veiligheidsketens is het integrale en multidisciplinaire karakter van de aanpak. Alle betrokken actoren worden in kaart gebracht en het gehele besluitvormingsproces wordt geborgd. Elke schakel binnen de veiligheidsketen vraagt om een gerichte aanpak. Het vertrekpunt van het model begint bij risicomanagement ofwel het beheersen van risico's. De eerste stap is het inventariseren van de risico's zodat een compleet beeld ontstaat. Bij proactie gaat het om het structureel voorkomen van onveiligheid. Dit geldt bijvoorbeeld voor de vergunningverlening voor de organiseren van een grootschalig evenement of de bouw van een kerncentrale. De volgende schakel bevindt zich eveneens in de categorie risicomanagement en heeft als doel de aanwezige risico's zoveel mogelijk te beperken. Het gaat bij preventie om het pakket aan maatregelen om de mogelijke effecten van risico's te reduceren. Dit geldt bijvoorbeeld voor het instellen van antivirus software of het bijwerken van computer updates waardoor veiligheidslekken voorkomen kunnen worden. Het structureel voorkomen van risico's en het invoeren van risico reducerende maatregelen kunnen veelal niet voorkomen dat restrisico's overblijven. Daarnaast

kunnen onvoorziene omstandigheden plaatsvinden waardoor een ramp of crisis kan optreden. De volgende drie aspecten van de veiligheidsketen zijn om die reden gericht op crisismanagement ofwel het beheersen van een crisis.

Het eerste onderdeel is preparatie. Hierbij gaat het om het plannen, opleiden van personeel en het oefenen met rampscenario's. De volgende schakel is repressie, waarbij het gaat om de respons van de betrokken veiligheidspartners op normschendingen. Het is van essentieel belang om een ramp of crisis te stabiliseren, ofwel het daadwerkelijke optreden van hulpdiensten. In de fase na het daadwerkelijk optreden is het van belang om nazorg te bieden aan degenen die dat nodig hebben en de situatie voor zo ver mogelijk te herstellen. In de laatste fase is het ook van belang om verantwoording af te leggen en leerpunten te trekken uit de onvermijdelijke evaluaties.

3.4 Definiëring governance network

In dit onderzoek staat ook het begrip governance network centraal. Alvorens het onderzoek wordt uitgevoerd is het van belang dit begrip te definiëren. Provan en Kenis (2008) definiëren het begrip governance network als volgt: "groups of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal" (p. 231). Het gaat hierbij niet uitsluitend om de individuele belangen van de deelnemende organisaties, maar om het nastreven van

Netwerk governance	**Zelfregulerend net-werk**	**Leiderorganisatie-netwerk**	**Netwerk administra-tieve organisatie (NAO)**
Visualisatie			
Principe	Geen administratieve entiteit, participatie in netwerkmanagement door alle partijen	Administratieve entiteit (en netwerk-manager) is een be-langrijke netwerkpartij die ook een rol heeft in het primaire proces	Een toegewezen en aparte entiteit is gecreëerd om het netwerk te managen

Figuur 3.4 Drie vormen van network governance (Provan & Kenis, 2008, p.301)

een gezamenlijk doel dat dan vaak een regionaal karakter heeft. Provan en Kenis stellen dat een gezamenlijke '*outcome*' gerealiseerd kan worden door het verbinden of delen van kennis, capaciteit, activiteiten en vaardigheden. Deze onderdelen dienen met minimaal drie organisaties gedeeld te worden. Een governance netwerk onderscheidt zich van de klassieke vormen van governance, zoals de markt (directe ruil), hiërarchische lijnen binnen een organisatie of samenwerkingsrelaties (aanwijzingen, instructies). Provan en Kenis (2008) stellen dat er drie verschillende governance networks in de praktijk voorkomen. Het ontwerp en de aansturing kan per situatie verschillend zijn. In figuur 3.4 zijn de verschillende vormen van network governance die Provan en Kenis (2008) onderscheiden weergegeven.

De eerste organisatievorm die Provan en Kenis onderscheiden is het zelfregulerend netwerk. Het zelfregulerend netwerk is de minst complexe organisatievorm en kent geen administratieve entiteit en bestaat doorgaans uit weinig netwerkleden. Provan en Kenis (2008) stellen dat een netwerk met maximaal acht deelnemers zichzelf kan aansturen in een zelfregulerend netwerk (figuur 3.5). Als de samenwerking meer deelnemers betreft dan zal er een gecentraliseerde vorm optreden. De betrokken organisaties werken onderling of collectief samen in het netwerk. De deelnemende partijen regelen onderling de aansturing, dit wordt niet collectief aangestuurd door een specifieke organisatie. Deelnemers zijn bij deze vorm nauw betrokken en nemen deel aan activiteiten van het netwerk. De deelnemers zijn zelf verantwoordelijk voor de onderlinge samenwerking binnen het netwerk. Dit voordeel is tegelijkertijd ook een valkuil, onderlinge afstemming en het bereiken van consensus kan bij het zelfregulerend netwerk een nadeel zijn (Provan & Kenis, 2008). Deelnemende partners richten zich meer op de eigen bijdrage aan het netwerk dan aan de coördinatie behoefte die het netwerk zelf heeft.

Governancevorm	Vertrouwen	Aantal netwerk-leden	Doelconsensus	Behoefte aan net-werkcompetenties
Zelfregulerend netwerk	Hoog	Weinig	Hoog	Laag
Leiderorganisatienetwerk	Laag	Moderaat	Relatief laag	Moderaat
Netwerk administratieve organisatie (NAO)	Moderaat	Moderaat tot veel	Relatief hoog	Hoog

Figuur 3.5 Contigentiefactoren voor netwerkeffectiviteit (Provan & Kenis, 2008, p. 303)

Een tweede vorm van governance network is het leiderorganisatienetwerk. Deze organisatievorm komt het meest voor in de praktijk en kan zowel bottom-up ontstaan als ook top-down opgelegd worden. Vaak wordt een bestuurder van de centrumgemeente – bijvoorbeeld de burgemeester – aangewezen om voor de nodige coördinatie te zorgen: agenda, besluitenlijst, afvinken afsprakenlijstje. Het leiderschapsnetwerk kenmerkt zich door een centrale administratieve entiteit. Deze administratieve entiteit kan ingevuld worden door een netwerkmanager. In een leiderschapsnetwerk worden inhoudelijke zaken gecoördineerd door één deelnemer van het netwerk. Essentieel voor het leiderschapsnetwerk is de legitimatie van de coördinerende deelnemer. Binnen het netwerk moet immers consensus bereikt worden over gemeenschappelijke besluiten en doelstellingen. Bij besluitvorming op basis van eenstemmigheid heeft in feite elke deelnemer veto-macht. Na afsluiting van de interne besluitvorming kan het netwerk met een leiderschapsvorm met één gezicht naar buiten treden. Een nadeel van een leiderorganisatienetwerk is de kans op belangenverstrengeling van de coördinerende deelnemer met de deelbelangen van de organisatie die hij/zij vertegenwoordigt, waardoor andere deelnemers kunnen afhaken. Is de voorzitter van de centrumgemeente in staat de belangen van de eigen gemeente te scheiden van die van het netwerk als geheel? Dat vergt een zekere stuurmanskunst.

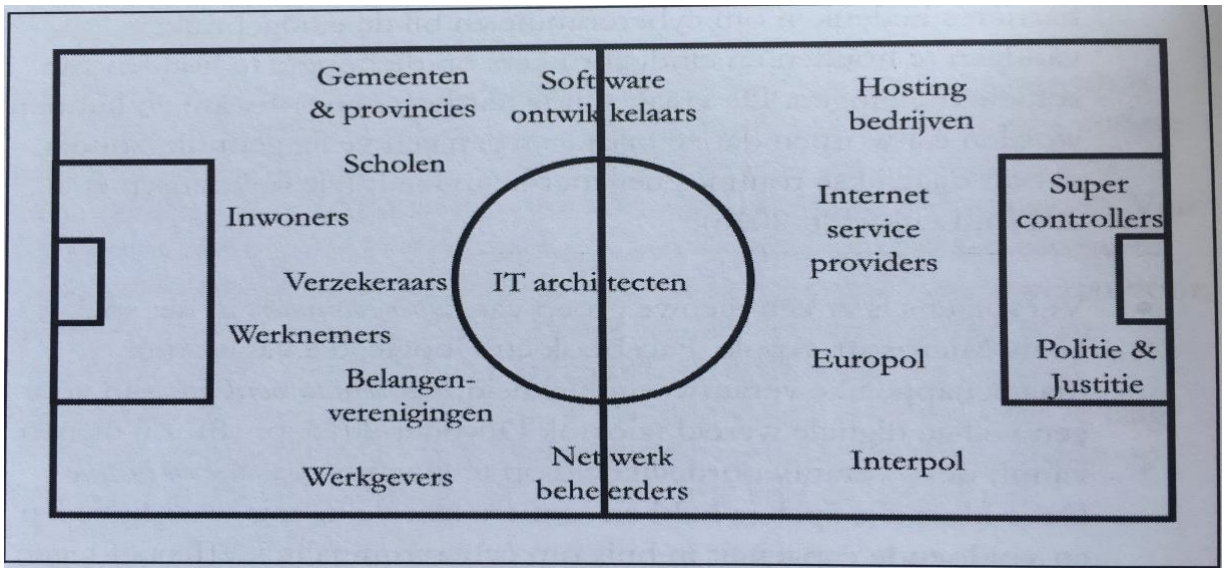
De laatste organisatievorm die Provan en Kenis (2008) onderscheiden is de netwerk administratieve organisatie (NAO). Bij deze vorm wordt een eigen, nieuwe entiteit gecreëerd om het netwerk te managen, dit geldt voor zowel de administratieve als inhoudelijke afhandeling. Het voordeel van deze organisatievorm is dat een aparte organisatie aangewezen wordt, waardoor niet één van de deelnemers een coördinerende rol op zich hoeft te nemen. De schijn van belangenverstrengeling kan hierdoor voorkomen worden. Het nadeel is dat er een extra organisatie

aan het netwerk wordt toegevoegd. Ook deze nieuwe organisatie heeft op haar beurt eigen belangen en zal actief op zoek gaan naar eigen financieringsbronnen.

Naast de contigentiefactoren van Provan en Kenis (2008) kunnen ook andere factoren van invloed zijn op succesvolle van samenwerking tussen meerdere organisaties. Zo leidt een duidelijke verdeling van taken en voldoende tijd, middelen en beleidsprioriteit tot betere onderlinge afstemming en capaciteit (Jacob, Veenstra & Dijkstra, 2016).

3.5 Governance rondom cybercrime

Met het oog op de afhandeling van een ramp of crisis in de fysieke wereld bestaan er wet- en regelgeving, rampenplannen en professionele crisisdiensten. Bij de bestrijding van een brand is het grotendeels duidelijk wie welke taken en verantwoordelijkheden heeft. Dit in tegenstelling tot cybercrime, waarbij nu nog onduidelijk is welke wet- en regelgeving van toepassing is en welke organisatie er moet optreden. Mede hierdoor is de samenwerking tussen hulpverleners en hun gemeenschappelijke aanpak nog niet uitgekristalliseerd. Om inzicht te krijgen in de taken en verantwoordelijkheden van betrokken partijen hebben Jansen et al., (2017) het volgende overzicht gemaakt op basis van het 'voetbalmodel van achter naar voren' van Boutellier (2005). Jansen et al., (2017) stellen dat burgers een belangrijke rol spelen in de frontlinie, zij moeten zich immers veilig gedragen en de feitelijke voorzorgsmaatregelen nemen om cybercrime te voorkomen. Ook zouden burgers inbreuken op hun digitale veiligheid aan de opsporingsinstanties moeten melden. Deze taak en verantwoordelijkheid geldt eveneens voor werknemers van organisaties. De eindgebruikers moeten geïnformeerd worden over de risico's en op welke wijze burgers en werknemers zich digitaal veilig kunnen gedragen. De eindgebruikers dienen de door hen gebruikte software up-to-date te houden, voorzichtig om te gaan met privé-informatie en sterke wachtwoorden te gebruiken, waardoor het risico op slachtofferschap van cybercrime wordt verminderd. Eindgebruikers die in de frontlinie staan kunnen verschillende rollen aannemen om zichzelf en andere personen te beschermen. Deze rollen kunnen gekoppeld worden aan menselijke verhoudingen in het dagelijks leven. Zo kunnen collega's elkaar op het werk attent maken op de risico's van gevaarlijke online activiteiten, maar ook vrienden onderling kunnen elkaar wijzen op de risico's van het delen van privé-informatie op social media.



Figuur 3.5 Betrokken spelers bij cybercrime (Spithoven, 2020 p.68)

Alleen als eindgebruikers bereid zijn om incidenten te melden dan kunnen andere linies in het voetbalmodel, zoals het middenveld en de verdedigingslinie, beter aansluiten op de praktijk. Jansen et al., stellen tot slot dat eindgebruikers ook een rol kunnen vervullen middels burgerinitiatieven of activistische bewegingen (zoals Bits of Freedom), waarmee zij proberen om de samenleving veiliger om te laten gaan met de digitale wereld.

In het middenveld spelen gemeenten, provincies, werkgevers en maatschappelijke organisaties een belangrijke rol. De organisaties in het middenveld hebben niet de primaire taak om de beveiliging van burgers en werknemers op zich te nemen. Zij dienen echter wel te zorgen voor het creëren van een veilige omgeving. Stol (2018) concludeert dat gemeenten op dit moment nauwelijks een rol spelen in de bestrijding van digitale criminaliteit. De gemeente is echter wel verantwoordelijk voor de openbare orde en veiligheid. De gemeenten zijn vaak een formele gesprekspartner binnen het lokale veiligheidsnetwerk (de lokale driehoek). De gemeente heeft een coördinerende rol en kan partijen met elkaar verbinden en bijvoorbeeld initiatieven om burgers (scholieren, ouderen) cyberweerbaar te maken stimuleren.

Het middenveld kent volgens Jansen et al., nog meer partijen die hun klanten of achterban kunnen informeren over de mogelijke veiligheidsrisico's, waaronder branche- en belangenverenigingen, hostingbedrijven. Tot slot dienen softwareontwikkelaars, IT architecten en beheerders van digitale infrastructuren te voorkomen dat eindgebruikers slachtoffer worden van cybercriminaliteit. Dit kunnen zij doen door hun klanten op de hoogte te houden van de mogelijke veiligheidsrisico's. Daarnaast hebben zij een rol om barrières op te werpen om cybercriminelen tegen te gaan.

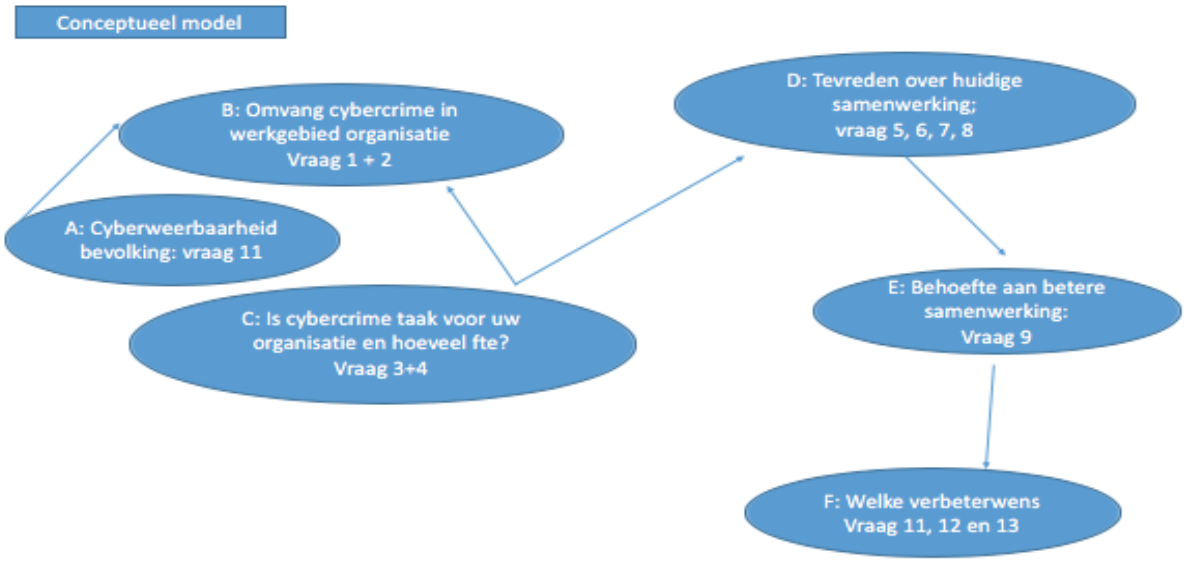
Achter het middenveld bevinden zich de 'super controllers'. Dit zijn de grote spelers in de digitale wereld, waaronder: Google, Facebook, Apple en Amazone. Deze super controllers kunnen het gedrag van eindgebruikers beïnvloeden door beveiligingsmaatregelen in te voeren. Deze partijen worden steeds vaker op hun maatschappelijke rol aangesproken, mede vanwege hun monopoloïde machtspositie in de markt. Ook zij zijn medeverantwoordelijk voor veilige digitale wereld (Dcypher, 2018 p.18). Daarnaast worden de super controllers steeds vaker in strafzaken gevraagd om informatie te delen met politie en justitie. Social media platformen worden ook op hun verantwoordelijkheid aangesproken als 'moderator' op het voorkomen van ongewenste uitlatingen op sociale media. In de achterhoede bevinden zich ook partijen die primair de taak hebben om de samenleving veiliger te maken vanaf de verdedigingslinie.

Volgens Leukfeldt et al., (2013) dienen niet alleen de klassieke partners in de strafrechtketen cybercrime tegen te gaan, maar gaat het om een gezamenlijk optreden van alle actoren in het voetbalmodel: dit kan worden omschreven als 'totaalvoetbal': ook de verdedigers hebben aanvallende taken; en ook de spitsen verdedigen mee. Dit vergt echter afstemming tussen de verschillende actoren en een brede samenwerking op het gebied van cybercrime. De partners binnen de strafrechtketen zijn vanuit hun eigen rol en bevoegdheid binnen de rechtstaat verantwoordelijk voor de opsporing, vervolging en berechting van daders.

3.6 Conceptueel model

Naar aanleiding van de besproken literatuur is het onderstaande conceptuele model opgesteld om behulpzaam te zijn bij het beantwoorden van de centrale vraag van het onderzoek. De centrale vraag in deze thesis betreft welke problemen en kansen de traditionele handhavende organisaties tegenkomen bij het aanpakken van bedrog en diefstal als vormen van cybercrime. Daarnaast moet in

dit onderzoek ook duidelijk worden welke taken en verantwoordelijkheden de genoemde organisaties hebben, met wie ze samenwerken, in hoeverre ze daar tevreden mee zijn en welke mogelijkheden ze zien om op het terrein van bedrog en diefstal effectief handhavend op te treden. De vragenlijst die is gebruikt stelt een aantal concrete vragen die kunnen worden veralgemeniseerd tot in totaal zes factoren.



Figuur 3.6 Conceptueel model

In de eerste plaats is er de vraag of de doelgroep/jurisdictie waarvoor de handhavende instantie werkt, erg digitaal weerbaar is of juist niet. Over het algemeen zijn ouderen en VMBO-scholieren niet erg digitaal vaardig en zijn zij ook kwetsbaar; studenten aan de technische universiteiten en medewerkers van IT-bedrijven hoef je niet veel wijs te maken; zij zijn digitaal vaardig en wellicht ook behoorlijke cyber veilig: hoewel hier natuurlijk het psychologische risico aanwezig is dat mensen die zich heel veilig voelen zich toch risicovol gaan gedragen en mensen die zich bewust zijn hoe beperkt hun kennis is zich juist heel terughoudend kunnen opstellen.

Als er in een gebied een lage digitale vaardigheid bestaat en dus een hoge cyberrisico, dan mag aangenomen worden dat er in het gebied ook regelmatig met succes digitaal wordt ingebroken; dat er valse identiteiten worden verworven; dat er conto's worden geplunderd en dat er succesvol wordt misleid. Dus we mogen aannemen dat de door de instantie waargenomen omvang van de cybercrime dan redelijk hoog is: de factor B heeft dan een hoge waarde. Tussen cyberveiligheid en omvang cybercrime wordt een negatief verband verondersteld: hoe cyber veiliger de bedrijven in het werkgebied, hoe minder cybercrime wordt waargenomen.

Als een organisatie veel problemen waarneemt zijn er twee strategieën denkbaar; "*het is heel erg maar het is niet onze schuld, u moet met uw klacht ergens anders zijn*"; de andere reactie is natuurlijk de wake up call; "*he, er is een groot probleem; hier is voor ons een taak; we gaan er aandacht aan besteden"*; een tussen mogelijkheid is: we gaan er lippendienst aan bewijzen; dat betekent: veel over praten, vaak iets over zeggen: maar er feitelijk niets aan doen: symboolbeleid is een andere term. Tussen de factor C (het is een taak voor ons en we zetten erop in) en de waarneming van de omvang van het probleem is er waarschijnlijk een positieve relatie: hoe meer feitelijke aandacht je aan een probleem kan besteden, hoe beter je kan zien hoe groot het probleem is: minder dark numbers.

Als je het een probleem vindt en je wilt er wat aan doen en je kunt er ook wat aan doen, dan kan het zijn dat je uitkomt op samenwerking: Je wil het dossier rond krijgen om daadwerkelijk een strafrechtelijke sanctie op te kunnen leggen; je hebt een andere partij nodig om voorlichting te kunnen geven over preventieve maatregelen. In de factor D wordt gevraagd naar de tevredenheid over de huidige vorm van samenwerking. Niet helemaal duidelijk is over welke vorm van samenwerking we het hebben. Dat moet blijken tijdens de gesprekken.

Er is samenwerking van onderop, aan de hand van een concreet incident dat om een passend antwoord vraagt; er is ook samenwerking van bovenaf; je kan ergens subsidie voor krijgen; je wordt gevraagd om mee te doen met een landelijk experiment; het vermoeden is dat in de vragenlijst vaker wordt gevraagd naar de tevredenheid over de top-down-samenwerking (subsidie gedreven) dan over de bottom-up samenwerking (vanuit problemen in het dagelijkse werkveld). In dat dagelijkse werkveld lijkt de zogeheten ketensamenwerking van groot belang. Die moet beter om tot vervolging, berechting en bestraffing te komen. Het beeld is dat er achterin de keten nog weinig in gereedheid is gebracht. Is er bijvoorbeeld al wel een landelijk coördinerend officier van justitie voor cybercrime? Hoeveel zaken zijn er tot nog toe finaal afgedaan. De laatste twee factoren gaan over omissies in de huidige samenwerking; behoefte aan verbeterde samenwerking en waar meer specifiek behoefte aan is: het kan goed zijn dat de wensen per type organisatie verschillen.

4. Methodologisch kader

4. Methodologisch kader

In dit hoofdstuk worden de keuzes die bij de opzet van het onderzoek zijn gemaakt uitgewerkt. Dit hoofdstuk gaat in op de vraag hoe de deelvragen worden beantwoord, welke informatie nodig is en hoe die verzameld wordt. Om dit te beantwoorden worden achtereenvolgens de onderzoeksstrategie, onderzoekseenheden, methoden van dataverzameling, operationalisatie, methode van data-analyse en de betrouwbaarheid en validiteit beschreven.

4.1 Onderzoeksstrategie

Om de deelvragen te beantwoorden wordt er een kwalitatieve en interpretatieve onderzoeksbenadering gekozen, met als doel in kaart te brengen welke actoren betrokken kunnen worden in de aanpak van cybercrime en welke verantwoordelijkheden zij daarbij hebben. Het onderzoek richt zich immers op het verzamelen en interpreteren van talig materiaal om vervolgens uitspraken te doen over een sociaal verschijnsel (Bleijenberg (2013, p. 10). Hierdoor kunnen de verschillende actoren begrepen worden vanuit hun eigen perspectief, in de veronderstelling dat er niet één werkelijkheid bestaat (Van Thiel, 2010). Maar dat elke organisatie met een aparte uitsnede van de werkelijkheid wordt geconfronteerd. Om dit te bewerkstelligen sluiten diepte-interviews met verschillende gemeenten binnen Oost-Nederland en experts van relevante organisaties goed aan bij de doelstelling van het onderzoek.

De uitvoering van kwalitatief onderzoek wordt in dit onderzoek uitgevoerd aan de hand van een casestudy, waarbij de onderzoeker onderdeel is van de sociale actie. (Bleijenbergh, 2013 p. 32). Een casestudy is geschikt voor het onderzoeken van een sociaal verschijnsel in een natuurlijke omgeving (Bleijenbergh, 2013, p. 36). Het doel van het onderzoek is om de governance in kaart te brengen op het gebied van bedrog en diefstal binnen cybercrime. In dit onderzoek wordt de aanpak van een aantal gemeenten besproken met experts die betrokken zijn bij de aanpak van cybercrime in Oost-Nederland (Spithoven, 2020).

4.2 Respondenten

In dit onderzoek zijn respondenten benaderd uit twee groepen. De eerste groep bestaat uit verschillende gemeenten in Oost-Nederland. Allereerst worden de betrokken gemeenten benaderd die onderdeel uitmaken van het expertteam Cyber van het Veiligheidsnetwerk Oost-Nederland. Het Veiligheidsnetwerk Oost-Nederland heeft in de Veiligheidsstrategie 2019-2022 cybercrime/gedigitaliseerde criminaliteit als thema geprioriteerd. Het multidisciplinaire team cybercrime heeft de volgende doelstellingen geformuleerd: 1) het in kaart brengen van de mogelijk verschuivende criminaliteit in Oost-Nederland, van offline naar online criminaliteit, 2) het samenstellen van een overzicht van de ketenpartners en welke rol de overheid daarin heeft, 3) het laten participeren van het bedrijfsleven in de aanpak van cybercrime en tot slot 4) het stimuleren van de kennisuitwisseling en onderlinge samenwerking. Tot slot wordt het Veiligheidsnetwerk Oost-Nederland getoetst aan de hand van de voorwaarden voor succesvolle samenwerking. Ook gemeenten in Oost-Nederland die niet deel uitmaken van het Expertteam Cyber kunnen in tweede instantie betrokken worden in dit onderzoek, afhankelijk van de respons van de desbetreffende gemeenten. De contactinformatie van deze groep werd verkregen via de coördinator van het Veiligheidsnetwerk Oost-Nederland. Uiteindelijk zijn er in dit onderzoek zeven respondenten geïnterviewd die werkzaam zijn bij zeven verschillende gemeenten in Oost-Nederland.

De tweede groep deelnemers bestaat uit experts van relevante organisaties die betrokken zijn of kunnen worden bij de aanpak van cybercrime in Oost-Nederland (Spithoven, 2020). Deze personen zijn gekozen op basis van hun kennis of expertise op dit thema of omdat zij een bepaalde doelgroep vertegenwoordigen die van belang is of kan zijn in de aanpak van cybercrime. Deze tweede onderzoeksgroep is deels lid van het expertteam Cyber van het Veiligheidsnetwerk. Daarnaast zijn er op basis van eigen intuïtie en in overleg met de coördinator van het Veiligheidsnetwerk Oost-Nederland nog andere experts bij dit onderzoek betrokken. De contactgegevens van de experts zijn deels via de coördinator van het Veiligheidsnetwerk verkregen. Mochten zij (nog) niet betrokken zijn bij het expertteam Cyber dan zijn zij via contactgegevens op het internet benaderd (open source). Dit geldt bijvoorbeeld voor de het Cybercentrum voor de Maakindustrie (CCM) omdat deze instantie betrokken is bij het cyberweerbaar maken van MKB'ers in Oost-Nederland. Dat geldt ook voor de Ouderenbond KBO-PCOB omdat zij een belangrijke doelgroep vertegenwoordigen die vaak naar voren komt als kwetsbaar. Ook het Regionaal Informatiepunt Integrale Veiligheid (RCIV) en de VeiligheidsAlliantie Regio Rotterdam (VAR) behoren tot deze tweede groep. De VAR is een regionaal samenwerkingsverband tussen het Openbaar Ministerie, 25 gemeenten en de politie.

Groep 1: Gemeenten	**Groep 2: Experts**
Gemeente Neder-Betuwe	Cybercentrum voor de Maakindustrie
Gemeente Deventer	Hogeschool Saxion / Space 53
Gemeente Nijmegen	Seniorenorganisatie KBO-PCOB
Gemeente West-Betuwe	Ondernemersorganisatie VNO-NCW
Gemeente Renkum	MKB Cybercampus
Gemeente Winterswijk	Openbaar Ministerie
Gemeente Enschede	VeiligheidsAlliantie Rotterdam
	Politie Expertisecentrum Cybercrime en Digitaal Opsporen
	Veiligheidsregio IJsselland
	Regionaal Informatiepunt Integrale Veiligheid

Tabel 4.2 verdeling van deelnemers

4.3 Methoden van dataverzameling

Om antwoord te geven op de onderzoeksvraag, wordt gebruik gemaakt van een tweetal dataverzamelingsmethoden: semi-gestructureerde interviews en documentanalyse. In dit onderzoek is er voor gekozen om meerdere dataverzamelingsmethoden te hanteren om zo de kwaliteit van het onderzoek te vergroten (Bleijenbergh, 2013, p. 32). Respondenten kunnen tijdens het interview een ander beeld schetsen dan wat er staat beschreven in documenten. Het is daarom van belang om de interviews met de respondenten zoveel mogelijk te vergelijken met de beschikbare documenten (de double check).

Semi-gestructureerde interviews

In dit onderzoek wordt gebruik gemaakt van semi-gestructureerde interviews. Interviews bij kwalitatief onderzoek worden ook wel open interviews genoemd (Bleijenbergh, 2013). Een open interview biedt voor de onderzoeker meer ruimte om gegevens te verzamelen in vergelijking tot een gestandaardiseerde vragenlijst met gesloten antwoord categorieën. Daarnaast levert deze wijze van interviewen een rijkere en gevarieerde hoeveelheid informatie op (Bleijenbergh, 2013). Deelnemers

aan dit onderzoek worden immers gezien als experts. Het afnemen van interviews is gebruikelijk om een sociaal verschijnsel te doorgronden vanuit het perspectief van de organisatie die de desbetreffende respondent vertegenwoordigt. In dit onderzoek is gekozen voor een semi-gestructureerde wijze van interviewen. Dit betekent dat de formulering van de vraagstelling van te voren vast wordt gesteld door de onderzoeker. Een voordeel van semi-gestructureerde interviews is dat de onderzoeker aan de hand van het gesprek kan sturen op de volgorde van de vragen. Hierdoor heeft de onderzoeker de vrijheid om te bepalen welke vragen tijdens het interview in elk geval besproken worden.

De interviews zijn afgenomen in de maanden juni, juli en augustus. Het interview duurde gemiddelde circa 50 minuten. Het interview werd indien mogelijk op locatie van de desbetreffende respondent afgenomen. Wanneer fysiek afspreken niet mogelijk was vanwege de coronamaatregelen, werd het interview afgelegd via Skype, Microsoft Teams of Zoom. Voorafgaand aan het interview is het 'informed consent' formulier (zie bijlagen) aan de respondenten overhandigd of vooraf via de email verzonden. Respondenten dienen van te voren akkoord te gaan met de gestelde voorwaarden, waaronder het maken van een geluidsopname van het interview. Een geluidsopname draagt immers bij aan de kwaliteit van de data en draagt bij aan de controleerbaarheid van het onderzoek (Boeije, 2008, p. 61). De respondentenlijst is opgenomen in bijlage 1. Daarnaast wordt de anonimiteit van de respondenten gewaarborgd. De namen van de desbetreffende deelnemers zijn dan ook niet te vinden in deze lijst.

Documentanalyse

In dit onderzoek wordt naast van semi-gestructureerde interviews ook gebruik gemaakt van documentanalyse, wat een bijdrage heeft gegeven aan het verdiepende karakter van deze casestudie. Documentanalyse vergroot de betrouwbaarheid en validiteit van het onderzoek, omdat de documenten een directe afspiegeling vormen van wat er op een bepaald moment vastgesteld is (Bleijenberg, 2013). Het risico bestaat immers dat respondenten een sociaalwenselijk antwoord geven. In het onderzoek worden relevante openbare documenten van gemeenten en experts uit het werkveld doorzocht op het thema cybercrime. De beleidsdocumenten maken duidelijk of cybercrime een speerpunt is van een organisatie. Daarnaast kan soms uit de documenten worden afgeleid hoeveel capaciteit er beschikbaar is gesteld voor deze taak. Wel moet worden bedacht dat deze documenten met een ander doel werden opgesteld dan om bij te dragen aan de beantwoording van de deelvragen van dit onderzoek.

4.4 Operationalisatie

De semi-gestructureerde vragenlijst bouwt voort op het conceptuele model dat aan het eind van hoofdstuk 3 werd gepresenteerd. In tabel 4.5 worden de dimensies en indicatoren gekoppeld aan de interviewvragen.

Dimensie	**Indicator**	**Operationalisatie**
Definitie cybercrime	Cybercrime in brede en enge zin	Wat verstaat u onder cybercriminaliteit?
Deel 1: Eigen praktijk	Vormen van cybercrime	Welke vormen van 'bedrog en diefstal' ziet u vooral in uw praktijk voorbij komen?

	Slachtofferschap	Welke doelgroepen worden vooral door deze vormen van bedrog en diefstal getroffen?
	Toenemende digitalisering, cyberweerbaarheid, risicobewustzijn	Hoe ontstaat volgens u de gelegenheid voor deze vormen van bedrog en diefstal?
	Governance rondom cybercrime	Wat is uw taak en wat is de taak van uw organisatie in het tegengaan van deze vormen van bedrog en diefstal?
	Voldoende middelen, tijd en beleidsprioriteit	Hoeveel capaciteit is er voor deze taken vrijgemaakt? Is dit voldoende volgens u?
Deel 2: Huidige samenwerking	Aantal deelnemers	Met welke andere organisaties werkt uw organisatie momenteel samen in het tegengaan van deze vormen van bedrog en diefstal?
	Duidelijke verdeling van taken, doelconsensus	Wat zijn ieders taken in deze samenwerking?
	Voldoende tijd, middelen en beleidsprioriteit	Ervaart u dat de andere organisaties voldoende capaciteit hebben voor de uitvoering van deze taken?
	Duidelijke meerwaarde van samenwerken	Hoe ervaart u deze samenwerking? Zijn er zaken die het samenwerken bemoeilijken?
Deel 3: Actorenanalyse	Veiligheidsketen	Welke organisaties zouden volgens u nog meer moeten worden betrokken om inwoners en ondernemers weerbaarder te maken tegen bedrog en diefstal?
	Veiligheidsketen	Wat zou er volgens u idealiter per fase van de veiligheidsketen moeten gebeuren om de weerbaarheid van inwoners en ondernemers te vergroten?
	Veiligheidsketen	Welke partijen kennen idealiter welke verantwoordelijkheden per fase?
Deel 4: Afsluiting	n.v.t.	Welke kansen/verbeteringen ziet u om de weerbaarheid van inwoners en ondernemers (tegen bedrog en diefstal) te vergroten voor de toekomst?
	n.v.t.	Hebben wij in dit interview nog iets gemist dat u wilt meegeven?

Tabel 4.5 operationalisatie

4.5 Methoden van data-analyse

Om de deelvragen te beantwoorden wordt er een interpretatieve onderzoeksbenadering gekozen, met als doel om te begrijpen welke taken en verantwoordelijkheden organisaties onderkennen in de governance rondom het onderdeel bedrog en diefstal binnen de cybercrime. Om dit te bewerkstelligen sluiten diepte-interviews met vertegenwoordigers van de betrokken organisaties het best aan bij de doelstelling van dit onderzoek. De meerwaarde van de vergelijking tussen het expertteam cyber en de groep vertegenwoordigers van relevante organisaties is dat op deze manier verschillende denkwijzen van beide groepen tegen elkaar afgezet kunnen worden. Door deze groepen (vertegenwoordigers gemeenten en experts) met elkaar te vergelijken kan er gekeken worden naar overeenkomsten en verschillen. Dit kan bijvoorbeeld gaan over verschillende inzichten in de aard en omvang van bedrog en diefstal maar ook over de ervaren urgentie van het thema cybercrime. Inzicht in deze overeenkomsten en verschillen kunnen waardevolle inzichten geven.

Het interview wordt op basis van de geluidsopname getranscribeerd via het programma Atlas.ti. De transcripten worden in de volgende fase van het onderzoek voorzien van open codering, ofwel axiaal coderen. De transcripten worden met elkaar vergeleken en op basis daarvan voorzien van codes. Als bepaalde codes vaker voorkomen dan kunnen ze gesorteerd en gegroepeerd worden. Het aanbrengen van codering leidt immers tot patronen en samenhang in de data (Van Thiel, 2010).

Uit onderzoek van Klijn & Koppejan (2016) blijkt dat een netwerk op een kwalitatieve en kwantitatieve manier onderzocht kan worden. De kwalitatieve methode biedt echter meer diepgang om de werkelijkheid van de governance op het gebied van cybercrime te bestuderen. Binnen deze casestudy bevinden zich twee deelcases. Enerzijds de expertgroep cybercrime van het Veiligheidsnetwerk Oost-Nederland en anderzijds een groep met vertegenwoordigers en experts van relevante organisaties buiten het Veiligheidsnetwerk Oost-Nederland. Hierdoor ontstaat een gevarieerd beeld van het functioneren van een cybernetwerk en de randvoorwaarden om succesvol cybercrime het hoofd te bieden. De interviews worden afgenomen bij de betrokken actoren binnen de VeiligheidsAlliantie regio Rotterdam en het Veiligheidsnetwerk Oost-Nederland op het gebied van cybercrime.

4.6 Betrouwbaarheid en validiteit

Deze paragraaf gaat in op de validiteit en betrouwbaarheid van het onderzoek. Allereerst behandelt deze paragraaf de interne validiteit. Daarna wordt ingegaan op de externe validiteit van dit onderzoek. Tot slot gaat deze paragraaf in op de betrouwbaarheid van de onderzoeksresultaten. Interne validiteit gaat over de vraag of het onderzoek meet wat het beoogt te meten (Bleijenbergh, 2013). Interne validiteit is het belangrijkste criterium in het beoordelen van kwalitatief onderzoek (Bleijenbergh, 2013, p 110). De belangrijkste dataverzamelingsmethode die in dit onderzoek centraal staat is het semi-gestructureerde interview. In een semi-gestructureerd interview is de formulering van de vragen van tevoren vastgelegd. Een voordeel van halfgestructureerde interviews is dat de vergelijkbaarheid van de antwoorden op de vragen enigszins wordt vergroot. Een nadeel van halfgestructureerde interviews ten opzichte van ongestructureerde interviews – waarbij er van tevoren weinig tot geen vragen zijn vastgelegd – is echter dat het gesprek een bepaalde richting wordt opgestuurd door de onderzoeker. In dit onderzoek zijn achttien interviews afgenomen met respondenten bij verschillende gemeenten en experts uit het werkveld. Er is gekozen om eerst zoveel mogelijk leden van het expertteam Cyber/gedigitaliseerde criminaliteit te interviewen. Aan de hand daarvan verwacht de onderzoeker een beter beeld te krijgen van de betrokken actoren van het netwerk.

Om de validiteit te bevorderen is getracht om expliciet door te vragen op de antwoorden die respondenten geven. Om de interne validiteit van het onderzoek te vergroten zijn twee vormen van triangulatie toegepast. De eerste vorm van triangulatie die is toegepast is methodologische triangulatie. De data in dit onderzoek is namelijk verzameld met behulp van verschillende dataverzamelingsmethoden, namelijk halfgestructureerde interviews en een documentenanalyse. De tweede vorm van triangulatie die is toegepast is triangulatie ten aanzien van databronnen. Doordat meerdere personen uit meerdere veiligheidsnetwerken zijn geïnterviewd, vergroot dit de interne validiteit van het onderzoek (Baarda, De Goede & Teunissen, 2009).

Externe validiteit heeft betrekking op de generaliseerbaarheid van resultaten. Dit houdt in dat de onderzoeksbevindingen te generaliseren zijn naar een grotere populatie (Bleijenbergh, 2013, p. 111). In dit onderzoek worden twee veiligheidsclusters onderzocht. De onderzoeksresultaten zullen hierdoor beperkt generaliseerbaar zijn voor andere clusters waarin kennis wordt uitgewisseld.

Betrouwbaarheid houdt in dat de onderzoeksbevindingen niet worden vertekend door toevallige afwijkingen (Bleijenbergh, 2013). Om de betrouwbaarheid van dit onderzoek te waarborgen is gekozen voor een semi-gestructureerd interview. De vragenlijst is van tevoren vastgelegd, waardoor alle respondenten dezelfde vragen krijgen voorgelegd. Dit vergroot de betrouwbaarheid van het onderzoek (Bleijenbergh, 2013). Daarnaast is de betrouwbaarheid van dit onderzoek vergroot doordat de interviews zijn opgenomen middels een voicerecorder. Daarnaast is een lijst met geraadpleegde documenten en de interviewhandleiding opgenomen in de bijlage. Hierdoor is het controleerbaar in hoeverre de onderzoeksresultaten voortkomen uit deze documenten. In het voorgaande is omschreven hoe de verzamelde gegevens zijn verwerkt, vergeleken en geanalyseerd. In principe is het mogelijk voor een andere onderzoeker om met de zelfde gegevens tot overeenkomstige conclusies te komen.

5. Resultaten en analyse

5. Resultaten en analyse

In dit hoofdstuk worden de resultaten gepresenteerd. Allereerst wordt ingegaan op wat cybercrime is volgens de gemeenten en de experts uit het werkveld. Aansluitend wordt duidelijk hoe bedrog en diefstal eruit ziet in de praktijk. Vervolgens wordt ingegaan op de vraag welke samenwerkingsverbanden, rollen en verantwoordelijkheden betrokken organisaties hebben. Aansluitend daarop geven experts hun visie op hoe de cyberweerbaarheid van inwoners en ondernemers kan worden vergroot.

5.1 Wat is cybercrime volgens de gemeenten en experts uit het werkveld?

Een aantal respondenten geeft aan dat cybercrime een complex fenomeen is. Uit de antwoorden blijkt dat er niet één overkoepelende definitie voor is. De respondenten geven aan dat er veel verschillende vormen van cybercrime onder verstaan kunnen worden. Cybercrime vormt een containerbegrip waarvan vele visies en definities mogelijk zijn.

R9: Dan zie je dat het een heel breed thema is. En dat begint volgens mij met marktplaatsfraude, naar bijvoorbeeld wat er in Lochem is gebeurd. Dat ze inbreken en bijna alle informatie en de gegevens gijzelen tot aan hacken van vitale functies. Dus het is best een breed domein.
R2: Dat vind ik ook gelijk een hele lastige, omdat er heel veel onder valt. Eigenlijk alles wat op het digitale manier geprobeerd wordt om misbruik te maken van mensen.

Een aantal experts en gemeenten maken een scheiding tussen cybercrime in enge of in brede zin. Bij cybercriminaliteit in enge zin is ICT zowel het middel als het doel. De beleidsadviseurs van de gemeente Enschede, Renkum, Deventer en Nijmegen geven aan dat ze onderscheid maken tussen enerzijds ‘gedigitaliseerde criminaliteit’ in brede zin en anderzijds cybercrime in enge zin.

R4: Ik gebruikte zelf de termen digitale criminaliteit en cybercrime. Cybercrime is dan criminaliteit als middel en doelwit. En gedigitaliseerde criminaliteit is meer de ouderwetse criminaliteit die een impuls heeft gekregen. Conclusie was dat ik zelf altijd sprak over gedigitaliseerde criminaliteit en meestal in de breedste zin van het woord. Cybercrime is dus net wat nauwer.
R18: Ik vind nog steeds de beste definitie: cybercrime is eigenlijk criminaliteit waarbij ICT zowel doel als middel is. Daarmee baken je het af van bijvoorbeeld gedigitaliseerde criminaliteit. Dus dat vind ik nog de meest praktische definitie van cybercrime.

Het begrip ‘gedigitaliseerde criminaliteit’ staat dichterbij gemeenten dan cybercrime in enge zin. Dit is in feite een vorm van de klassieke criminaliteit met een digitale component. De meeste gemeenten geven aan dat cybercrime in de brede zin het meest tot de verbeelding spreekt. Gedigitaliseerde criminaliteit is tot op zekere hoogte tastbaar en heeft met name fysieke gevolgen. Dit in tegenstelling tot de cybercrime in enge zin, waarbij het stereotype van *‘ICT-whizzkids’* naar voren komt en het digitale werkproces van een andere organisatie wordt verstoord. Deze vormen van criminaliteit spelen zich volledig af binnen het digitale domein en zijn veelal niet direct zichtbaar of tastbaar voor de buitenwereld. Gemeenten geven niet alleen aan dat ze geen raad weten met deze vormen van criminaliteit, maar ook dat ze met enige scepsis kijken naar de rol van de gemeente op dit vlak.

R12: Maar ja, ik heb meer met de brede zin van cybercrime. Dus meer de gedigitaliseerde criminaliteit en niet alleen de data naar data crime.
R6: De digitale dingen van het hacken van schijven of het stelen van bedrijfsinformatie, wat eigenlijk verder van je af staat. Waar je concreet niet direct iets mee kan en waar je wel iets mee wil. Het staat verder bij je vandaan omdat het geen fysieke zaken zijn natuurlijk.
R9: Dus het zou niet meer een soort ding moeten zijn van een aantal, ik zeg het onbeschoft, van die 'nerdachtige types' moeten zijn die heel de dag achter de computer zitten met allemaal pizzadozen om zich heen.

De traditionele strafrechtelijke instituties, zoals de politie en het Openbaar Ministerie, maken wel bewust onderscheid tussen cybercrime in brede en in enge zin. Dit onderscheid wordt bewust gemaakt omdat de definitie berust op een juridische basis, namelijk de twaalf wetsartikelen die daar specifiek op gericht zijn. Ondanks de juridische basis blijft het begrip cybercrime een discussiepunt volgens het Openbaar Ministerie.

R5: Dat is een blijvende discussie, in de zin van; is het nu cybercrime of is het nu gedigitaliseerde criminaliteit? Dan heb ik het over; één, cybercrime in enge zin, dat is dus hacken en vernielen. (…) Ja, en als je het theoretisch wil benaderen; computercriminaliteit met ICT als middel en als doel.

Op basis van de interviews geven de experts aan dat cybercrime een bepaalde criminele handeling met zich meebrengt, waar vaak een bepaald verdienmodel achter zit. De handeling is in het voordeel van de crimineel en in het nadeel van de organisatie of persoon die het treft. Het verdienmodel hoeft echter niet altijd aanwezig te zijn wanneer statelijke actoren deelnemen, tenzij het economische spionage betreft. Een criminele handeling kan op verschillende wijzen plaatvinden, waaronder het stelen, ontfutselen of het misbruik maken van gegevens.

R13: Dat kan dus het phishing zijn maar ook ander misbruik zijn of namelijk aan de haal gaan met die gegevens of verkopen van die gegevens verstaan wij onder cybercrime.

VNO-NCW en de MKB Cybercampus maken bewust geen onderscheid in enge of brede zin. Het gaat hen uiteindelijk om de effecten die cybercrime veroorzaken op individuen of op de maatschappij. Voor deze organisaties maakt het geen wezenlijk verschil hoe de criminaliteit wordt gepleegd. De focus op het middel of het doel is voor deze experts ondergeschikt aan de maatschappelijke effecten die cybercrime teweeg brengt of kan brengen.

R14: Door de ogen door de ondernemer is alles wat via de computer van hen crimineel geld kost cybercriminaliteit. Ik zie het daarom maar zo breed mogelijk
R15: Ik ben niet zo van dat onderscheid, zeg maar. Dus het zijn alle vormen van criminaliteit met een digitale component, zeg maar.

Tussenconclusie
Het begrip cybercrime laat zich niet eenvoudig definiëren. Zowel gemeenten als experts uit het werkveld geven verschillende definities van dit relatief nieuwe fenomeen. Het merendeel van de respondenten hanteert een scheiding tussen cybercrime in brede en enge zin. Ondanks deze basale scheiding hebben met name gemeenten meer met het begrip gedigitaliseerde criminaliteit ofwel

cybercrime in brede zin. Dit zijn de klassieke vormen van criminaliteit waar een digitaal component aan gekoppeld is. Cybercrime in de brede zin spreekt gemeenten meer aan vanwege het feit dat deze vormen van criminaliteit vaker in de actualiteit verschijnen en meer tot de verbeelding spreken. Dit in tegenstelling tot cybercrime in enge zin, waarbij ICT zowel gebruikt wordt als middel en als doel. Deze vormen van criminaliteit staat verder bij gemeenten vandaan en wordt in verband gebracht met '*ICT-whizzkids'.* Het Openbaar Ministerie en de politie hanteren een strikte scheiding tussen beide vormen vanwege de juridische basis. Dit in tegenstelling tot organisaties die nauw betrokken zijn bij ondernemers in het midden- en kleinbedrijf, waarbij de focus niet ligt op de cybercrime in brede of enge zin, maar bij de maatschappelijke effecten van deze vormen van criminaliteit voor de onderneming.

5.2 *Hoe ziet het onderdeel 'bedrog en diefstal' in de praktijk eruit?*

Gemeenten en experts beantwoorden deze deelvraag op basis van vier subvragen. Bij ieder interview werd de respondenten gevraagd welke vormen van 'bedrog en diefstal' de gemeenten en de experts in de praktijk voorbij zien komen.

5.2.1 Veel voorkomende vormen van bedrog en diefstal

In deze paragraaf geven gemeenten en experts uit het werkveld aan welke vormen van bedrog en diefstal (Holt & Bossler 2014, p. 25) vaak voorkomen onder inwoners en ondernemers.

De beleidsadviseurs en experts uit het werkveld geven aan dat alle vormen van bedrog en diefstal in de praktijk voorkomen met daarbij elk zijn specifieke doelgroep. Enkele respondenten wisten niet welke vormen van bedrog en diefstal in de praktijk vaak voorkomen, omdat ze niet beschikken over betrouwbare cijfers. Daarnaast geven de respondenten aan dat de cijfers die op dit moment bekend zijn het spreekwoordelijke 'topje van de ijsberg' betreffen, aangezien de meldingsbereidheid van cyber gerelateerde criminaliteit zeer laag ligt. De meeste experts geven aan dat het onduidelijk is hoeveel cybercriminaliteit er daadwerkelijk plaatsvindt. De oorzaak hiervan ligt volgens enkele respondenten niet alleen in de lage meldingsbereidheid. Maar ook in het feit dat inwoners en ondernemers zich schamen wanneer zij slachtoffer worden van cybercriminaliteit. Het aantal meldingen dat gedaan wordt bij de politie ligt volgens de experts beduidend lager dan het daadwerkelijke aantal incidenten in de praktijk. Dit blijkt eveneens uit tabel 2.1 in het theoretisch kader (hoofdstuk 2). Uit de ontwikkeling van het aantal aangiften blijkt dat steeds minder eindgebruikers aangiften doen van cybercrime. De veiligheidsmonitor (2019) van het CBS laat echter een ander beeld zien als het gaat om slachtofferschap. In 2019 werd bijna 14% van de Nederlandse bevolking slachtoffer van cybercrime, dit komt neer op 2 miljoen personen van 15 jaar of ouder.

R3: Ik moet eerlijk zeggen: het is best moeilijk om dat direct te onderbouwen met cijfers en die zijn er vaak niet echt op gemeentelijk niveau.
R6: Ik denk dat veel mensen er ook geen aangifte van doen, dat is natuurlijk het verhaal waar je het in terug ziet. Maar die cijfers zijn in de praktijk veel lager dan dat ze in de praktijk voor komen.
R8: Maar alles waar geen aangifte van wordt gedaan, dat zien zij niet. Van veel delicten in dit domein wordt geen aangifte van gedaan. Omdat de schaamte heel groot is. De aangiftebereidheid van mensen was rond de 8%.

Indien de respondent zegt geen beeld te kunnen schetsen van de veel voorkomende vormen van bedrog en diefstal in de praktijk, is de vraag gesteld wat de respondent het meest voorbij ziet komen op basis van hun beleving of aan de hand van nieuwsberichten. Op basis van de interviews wordt het volgende beeld geschetst door gemeenten en experts (zie tabel 5.2). Een kleine kanttekening kan daarbij gemaakt worden dat sommige respondenten aangeven dat alle vormen van bedrog en diefstal in de praktijk voorkomen. Hieronder staan echter de vormen waarvan de respondenten denken dat ze het meest in de praktijk voorkomen. Uit tabel 5.1 blijkt dat gemeenten en experts met name phishing en spoofing in de praktijk voorbij zien komen bij inwoners en ondernemers. Bij phishing wordt andermans persoonlijke informatie op een schijnbaar vertrouwde wijze buitgemaakt.

Vormen van bedrog en diefstal	**Gemeenten**	**Experts**	**Aantal**
Phishing	Neder-Betuwe, Deventer, Nijmegen, West-Betuwe, Winterswijk	Cybercentrum voor de Maakindustrie, Openbaar Ministerie, KBO-PCOB, MKB Cybercampus, politie	10
Spoofing	Deventer, Enschede, Renkum	Openbaar Ministerie, RCIV, KBO-PCOB, VNO-NCW, VAR, Politie, Veiligheidsregio IJsselland	10
Verkoopfraude	Neder-Betuwe, West-Betuwe, Winterswijk, Enschede	RCIV, MKB Cybercampus, VAR, Veiligheidsregio IJsselland	8
Betalingsfraude	West-Betuwe, Nijmegen, Winterswijk	Openbaar Ministerie, KBO-PCOB, Cybercentum voor de Maakindustrie	6
Gegevensdiefstal	Nijmegen, Winterswijk, Enschede	AIVD, RCIV, Cybercentrum voor de Maakindustrie	6
Identiteitsfraude	Deventer, Renkum	RCIV, MKB Cybercampus	4
Skimming	Winterswijk, Neder-Betuwe		2
Voorschotfraude	West-Betuwe		1
Gegevensheling			0

Tabel 5.1 overzicht van vormen van bedrog en diefstal

Eindgebruikers ontvangen bijvoorbeeld een e-mail waarbij ze criminelen met een één klik toegang kunnen verschaffen tot het computersysteem. Een expert van de landelijke politie geeft aan dat phishing al vele jaren bovenaan staat als het gaat om de verschillende vormen van bedrog en diefstal. Ook het Cybercentrum voor de Maakindustrie geeft aan dat met name phishing veelvuldig voorkomt bij MKB bedrijven.

R18: Phishing is natuurlijk al jarenlang onze 'pain in the ass', zeg maar. Ik heb de cijfers net gezien van april-mei. Daar schrik je je dood van, echt. Over die twee maanden loopt het al meer dan twee miljoen aan schade. Dat is bizar veel.

Ondernemers hebben volgens het MKB Cybercampus te maken met een variant van phishing, namelijk *'spearphishing'*. Deze vorm is in tegenstelling tot de gewone modus operandi, specifiek gericht op een individu, organisatie of bedrijf. De phishing activiteiten zijn bijvoorbeeld specifiek gericht op een persoon met een sleutelpositie in een organisatie, waarbij bepaalde informatie of toegang tot het netwerk verkregen kan worden. Een andere veel voorkomende variant bij ondernemers is volgens VNO-CNW de zogeheten CEO-fraude. Bij CEO-fraude veronderstelt een medewerker een e-mail van de Chief Executive Officier - de baas - te ontvangen. In de e-mail vraagt de CEO om geld over te maken naar een rekeningnummer. In werkelijkheid wordt deze e-mail door criminelen verzonden en wordt het geld na de transactie doorgesluisd naar de rekening van de criminelen.

R14: CEO-fraude is behoorlijk gestegen geloof ik de afgelopen jaren. Het ging volgens mij over 1,7 miljard euro. Je hebt natuurlijk ook een paar hele grote gevallen gehad.

Het Openbaar Ministerie geeft aan dat ongeveer de helft van het aantal zaken dat binnenkomt betrekking heeft op '*whaling*'. Deze vorm van cybercrime wordt door criminelen gebruikt om fraudeleuze email te versturen naar sleutelposities binnen organisaties met als doel om gevoelige of financiële data te verkrijgen. Whaling komt grotendeels overeen met de subvorm spearphishing.

Een andere veel voorkomende vorm van bedrog en diefstal is '*spoofing*', waarbij criminelen zich voordoen als een vertrouwd persoon van het slachtoffer. Dit komt met name tot uiting in de 'vriend-in-noodfraude' of de 'WhatsApp fraude'. De definitie 'vriend-in-noodfraude' is onlangs door de politie en het Openbaar Ministerie vastgesteld, maar wordt door anderen gezien als WhatsAppfraude. Deze vorm van fraude wordt gepleegd door middel van het communicatiemiddel WhatsApp.

R3: Vriend-in-noodfraude staat hier niet tussen, de WhatsApp-fraude. Daar doe je je voor als iemand anders: door het OM wordt dat vriend-in-nood-fraude genoemd, dat is de nieuwste term.
R9: Spoofing heb ik dus gehoord en ik zie daar ook wel regelmatig dat mensen dat delen zeg maar. Dat ze best verwonderd zijn tegenover de daders. Dat ze meepraten en uiteindelijk berichtjes sturen dat soort dingen.

Ondernemers hebben met name te maken met CEO-fraude. Deze vorm van bedrog en diefstal kan eveneens geschaard worden onder een subvorm van spoofing. Hierbij sturen criminelen een bericht naar sleutelpersonen binnen een organisatie uit naam van een baas of leidinggevende, met het doel om geld afhandig te maken. De brancheorganisatie weet bij klassieke vormen van criminaliteit vaak wel wat er speelt volgens een beleidsadviseur van VNO-NCW. Dit in tegenstelling tot meldingen van cybercriminaliteit.

R14: Dus dat hele MKB leeft in een soort roze wolk, van ons gebeurt dat niet. Want de grote bedrijven die staan in de krant en cijfers, als die er zijn dan zijn die goed, want er wordt nauwelijks aangifte van gedaan.

Bij het midden- en kleinbedrijf speelt imagoschade en reputatieverlies een belangrijke factor om geen aangifte te doen van cybercriminaliteit. Opmerkelijk is dat met name grote bedrijven in de media komen als slachtoffer van cybercriminaliteit. In tegenstelling tot het MKB waar het aantal meldingen

zeer laag is. Volgens VNO-NCW komt dit met name door de beperkte kennis over het fenomeen binnen de politie. Ondernemers weten van elkaar wel of er is ingebroken, daarover ontstaat volgens de brancheorganisatie collectieve woede en medeleven onder ondernemers. In tegenstelling tot cybercriminaliteit waarbij het gevoel van schaamte overheerst.

R15: Op dit moment is het niet zo uitnodigend om voor een MKB'er om het aanmeldproces in te gaan bij de plaatselijke politie. Dat betekent dat de schade vaak groter is dan nodig is, omdat te lang wordt gewacht soms of dat er (wordt gedacht dat er) onvoldoende kennis binnen de politieorganisatie is om dingen te doen.

Naast phishing en spoofing geven gemeenten en de experts aan dat verkoopfraude veelvuldig voorkomt in de praktijk, waarbij producten gekocht worden maar uiteindelijk niet geleverd worden. De politie geeft aan dat het in de begin van de coronacrisis tijdelijk afnam maar dat het aantal aangiften daarna steeg. Veel mensen zaten immers min of meer noodgedwongen thuis waardoor het aantal online aankopen omhoog ging. Ook andere experts zien het aantal meldingen van verkoopfraude stijgen.

R8: En ik weet dat er regionaal verkoopfraude is, marktplaatsfraude denk ik.
R18: We hebben het even zien dalen aan het begin van de coronacrisis. Iedereen dacht ik doe even niks, want elk pakketje dat we binnen krijgen kan een virus bevatten. Na een paar weken was dat die angst wel weer over en gingen mensen juist heel veel dingen doen via internet. Dus het aantal aan- en verkoopfraude gevallen neemt nu weer toe.

Tussenconclusie
Zowel gemeenten als experts geven aan dat ze geen of in zeer beperkte mate zicht hebben op deze vormen van bedrog en diefstal. De meest voorkomende vormen op dit moment zijn: phishing en spoofing. De respondenten geven aan dat spoofing vaak voorkomt in de variant van WhatsAppfraude of vriend-in-nood-fraude. Op de tweede plek staat verkoopfraude, waarbij eindgebruikers worden opgelicht via online webwinkels.

5.2.2 Kwetsbare doelgroepen

In deze paragraaf wordt antwoord gegeven op de vraag welke doelgroepen kwetsbaar zijn voor vormen van bedrog en diefstal. De gemeenten en experts schetsen het volgende beeld van de kwetsbare doelgroepen van bedrog en diefstal. Zij verdelen de kwetsbare doelgroepen in één algemene groep en twee subgroepen.

Kwetsbare doelgroep	**Gemeenten**	**Experts**	**Aantal**
Alle eindgebruikers	Deventer, Nijmegen, West-Betuwe, Winterswijk, Renkum, Enschede	Cybercentrum voor de Maakindustrie, KBO-PCOB, VNO-NCW, politie	12
Ouderen	West-Betuwe, Winterswijk, Renkum, Enschede	Saxion, RCIV, Veiligheidsregio IJsselland, MKB Cybercampus, Politie	9

Jongeren	Deventer, Nijmegen, Winterswijk, Renkum, Enschede	RCIV, VAR, politie	8
Organisaties		Cybercentrum voor de Maakindustrie, VNO-NCW, MKB Cybercampus, Saxion	4

Tabel 5.3 kwetsbare doelgroepen volgens de gemeenten

Alle eindgebruikers

Alle respondenten die werkzaam zijn voor de gemeente geven aan dat iedereen. Volgens de beleidsadviseur van de gemeente Deventer komt het voor in alle lagen van de bevolking. Uit onderstaande quotes blijkt dat criminelen zich niet richten op specifieke groepen, maar dat slachtofferschap van deze vormen van bedrog en diefstal iedereen kan overkomen. Dit komt volgens het Cybercentrum voor de Maakindustrie doordat criminelen steeds geavanceerder te werk gaan, waardoor iedereen slachtoffer kan worden van vormen van bedrog en diefstal.

R3: Dus het is niet direct te herleiden naar één groep: het komt in alle lagen voor, zeg maar.
R6: Ik denk dat ze zich richten op iedereen. Ze proberen het gewoon.
R9: Als ik dingen hoor is dat wel in een redelijke dwarsdoorsnede van de samenleving.

Iedereen kan in principe geraakt worden door cybercriminelen. Zo blijkt uit onderzoek dat phishing geen onderscheid maakt op basis van een risicoprofiel (Leukfeldt & Yar, 2016). Bij alle eindgebruikers valt immers wel wat te halen, zo is de redenering van VNO-NCW. De respondenten geven aan dat dit te maken heeft met de mate van risicobewustzijn. Daarnaast verkiezen eindgebruikers vaker gebruikersgemak boven veiligheid, waardoor de kans op slachtofferschap toeneemt. Zo refereert een expert van het MKB Cybercampus aan de nieuwe applicatie van de ING bank waarbij de toegang tot de privégegevens met een Quick Respons (QR) code van een oud device naar een nieuw device kan worden overgezet. Deze methode maakt het voor eindgebruikers gemakkelijk om het nieuwe device toegang te verlenen tot privé-gegevens, maar introduceert volgens de expert daarmee ook nieuwe kansen en mogelijkheden voor criminelen.

R14: Iedereen. Letterlijk iedereen, want voor de computer maakt het niet uit waar iemand zit of wat die doet. Ze hebben allemaal een bankrekening en allemaal gegevens.
R16: Ik denk dat eigenlijk iedereen kan zijn. Dat het jou en mij ook kan overkomen.

Een aantal respondenten geven aan dat er binnen de groep van eindgebruikers wel specifieke doelgroepen zijn die extra kwetsbaar om slachtoffer te worden van bedrog en diefstal, waaronder jongeren, ouderen en organisaties.

Ouderen

De eerste specifieke kwetsbare doelgroep die bij de gemeenten wordt genoemd, zijn de ouderen. Deze doelgroep beschikt volgens de gemeenten Neder-Betuwe, Nijmegen en Renkum enerzijds over beperkte kennis en vaardigheden. Daarnaast zijn ouderen niet opgegroeid met deze digitale mogelijkheden waardoor het risicobesef laag ligt.

R4. Ouderen die toch maar iets gaan proberen en naïef zijn schat ik in. Mensen die niet digitaal opgegroeid zijn.
R12: Ouderen zijn kwetsbaar omdat ze vaak wat digibeet 'er zijn en hoe ouder, hoe naïever ook in het leven.

De groep is volgens een vijftal experts met name kwetsbaar voor spoofing, zoals vriend-in-noodfraude/WhatsApp-fraude. Een expert merkt op dat ouderen sowieso gevoeliger zijn voor een vlotte babbel, ongeacht of dit fysiek of digitaal plaatsvindt. Volgens de seniorenorganisatie KBO-PCOB zijn ouderen extra kwetsbaar op het moment dat ze alleenstaand zijn en beschikken over weinig sociale contacten in hun omgeving. Hierdoor is het niet of beperkt mogelijk om bepaalde digitale zaken te overleggen of nog eens na te vragen. Volgens de politie is het logisch dat ouderen extra kwetsbaar zijn voor spoofing, zoals vriend-in-nood fraude of WhatsAppfraude. Zij beschikken in verhouding tot andere doelgroepen het vaakst over zowel geld als kinderen. Hierdoor zijn ouderen extra kwetsbaar voor deze specifieke vormen van bedrog en diefstal.

Jongeren
De tweede specifieke doelgroep die door de respondenten als extra kwetsbaar wordt bestempeld zijn jongeren. Deze doelgroep is volgens de respondenten om meerdere redenen extra kwetsbaar. Enerzijds gaat het volgens de gemeente Deventer om de kwetsbare jongeren met een laag opleidingsniveau.

R3: Wat uit beeld uit de politie en van de Rabobank naar voren komt bij dit soort criminaliteit is vooral toch kwetsbare jongeren: dan heb je het over leertrajecten en praktijkonderwijs of praktijkgeschoold.

Anderzijds maken deze vormen van bedrog en diefstal volgens de gemeente Deventer en Nijmegen voornamelijk slachtoffers onder studenten ofwel jongeren met een hoger opleidingsniveau. Jongeren bestellen in verhouding met andere doelgroepen meer op het internet, waardoor de kans op slachtofferschap groter is (Ngo & Paternoster, 2011). Deze doelgroep denkt tevergeefs dat deze vormen van bedrog en diefstal hen niet treffen.

R4: Ik las dat juist hoger opleiden een doelgroep zijn omdat ze denken 'dat gebeurt mij niet'. Wat ik om mij heen zie is dat hogeropgeleiden veel bestellingen doen. Dat zou ook mee kunnen wegen. Hogeropgeleiden is wat mij betreft een aparte doelgroep waar je je op moet richten.

Volgens de gemeente Winterswijk is deze groep extra kwetsbaar omdat zij een bepaalde mate van achteloosheid ten toon spreiden. Daarnaast merkt een respondent van de gemeente Renkum op dat deze groep redelijk naïef in het leven staat en de risico's daarmee onvoldoende serieus neemt. Hierdoor worden zij sneller slachtoffer. Een andere reden waarom jongeren kwetsbaar zijn is omdat ze simpelweg het meest gebruik maken van ICT en daardoor meer kans maken om slachtoffer te worden.

R9: Ik ben ook niet heel oud, ik denk dat onze generatie wel makkelijker is daarin en niet eens meldingen lezen of whatever. Gewoon klik, klik, klink en wegdoen. Daar zit een bepaalde achteloosheid in.

R18: Bij aan- en verkoopfraude zie je juist ook veel jongeren slachtoffer worden. Denk aan concertkaartjes, bijvoorbeeld, die zogenaamd aangeboden worden en natuurlijk nooit geleverd worden et cetera.

Jongeren worden niet alleen in verband gebracht met aan- en verkoopfraude maar ook met identiteitsfraude doordat zij zich inzetten of laten gebruiken als geldezel. Dit kan volgens het Regionaal Informatiepunt Integrale Veiligheid en de gemeente Deventer veroorzaakt worden door naïviteit van jongeren maar ook door de verleiding om snel geld te verdienen.

Organisaties
De derde doelgroep die kwetsbaar is voor bedrog en diefstal zijn organisaties. Een expert merkt op bijvoorbeeld overheidsinstellingen, onderwijsinstellingen en organisaties in vitale sectoren kwetsbaar zijn. Dit geldt ook voor onderwijsinstellingen, waarbij hackers bijvoorbeeld uit kunnen zijn op onderzoeksgegevens van wetenschappers. Sommige buitenlandse overheden zijn uit op deze gegevens met het doel deze buit te maken of te manipuleren. Een expert van de Veiligheidsregio IJsselland refereert aan de ransomware aanval bij de Universiteit van Maastricht, waarbij 269 servers van de onderwijsinstelling door criminelen werden versleuteld. De Limburgse onderwijsinstelling heeft uiteindelijk 197.000 euro betaald om de servers weer in oude staat te herstellen (Teeffelen, 2020).

R11: Dan kijk ik naar de universiteit van Maastricht, waar natuurlijk best wat gebeurd is.

Naast externe dreiging van bedrog en diefstal kunnen organisaties ook risico lopen door dreigingen van binnenuit. Een respondent van de Hogeschool Saxion refereert aan werknemers in een financieel onzekere situatie, die onder druk van andere personen kwetsbaar kunnen zijn voor vormen van bedrog en diefstal.

Tussenconclusie
Gemeenten en experts uit het werkveld concluderen dat vroeg of laat elke eindgebruiker te maken kan krijgen met cybercrime. Zowel inwoners als ondernemers die onvoldoende weerbaar zijn kunnen daardoor slachtoffer worden. Drie doelgroepen zijn volgens de respondenten extra kwetsbaar voor bedrog en diefstal. Allereerst worden jongeren aangemerkt als risicogroep, zij zijn extra kwetsbaar aangezien ze simpelweg vaker online zijn en in verhouding met andere doelgroepen meer online bestellingen doen. Ook ouderen vormen een kwetsbare doelgroep. Zij beschikken veelal over beperkte digitale kennis en vaardigheden en zijn vaker goedgelovig van aard. De laatste doelgroep zijn organisaties in de vitale sector, maar ook onderwijs- en overheidsinstellingen. Zij zijn extra kwetsbaar omdat deze organisaties de beschikking hebben over een grote hoeveelheid persoonlijke gegevens en gevoelige data. Vaak is in deze organisaties niemand verantwoordelijk gemaakt voor cybersafety.

5.2.3 Gelegenheid van bedrog en diefstal
De respondenten hebben ook antwoord gegeven op de vraag waarom bepaalde doelgroepen of organisaties kwetsbaar zijn.

Onvoldoende risicobewustzijn
De meeste experts geven aan dat eindgebruikers beschikken over te weinig besef van de risico's. De

experts geven aan dat veel mensen zich vaak niet bewust zijn van de risico's in het digitale domein en ook niet weten hoe ze zich daartegen kunnen beschermen. Dit komt niet alleen door onvoldoende risicobewustzijn maar ook door het gebrek aan het herkennen van deze gevaren. Zo geeft de gemeente Neder-Betuwe aan dat slachtoffers onvoldoende bekend zijn van het gebruik van bepaalde apps. Ook de gemeente Enschede geeft aan dat het risicobewustzijn onvoldoende aanwezig is bij inwoners en ondernemers.

R16: cybercrime bestaat wel, maar het is een 'ver-van-mijn-bed-show' voor heel veel mensen, maar het overkomt mij niet. Dus onvoldoende risicobewustzijn denk ik.

De gemeente Renkum en Winterswijk stellen dat eindgebruikers veelal onvoldoende bekend zijn met een veiliger alternatief of gebruikersgemak verkiezen boven veiligheid. Ook het veilige alternatief sluit niet altijd uit dat er nog restrisico's overblijven, maar het maakt de kans op slachtofferschap in elk geval kleiner.

R12: Onbekendheid met het risico en het veiligere alternatief. Welke kleine handelingen maken nou het risico in elk geval een stuk kleiner. Dan is het niet eens nul maar een stuk kleiner.
R9: Ik denk omdat mensen gewoon makkelijk zijn en makkelijker worden en ook niet niet… Wat ben ik nou eigenlijk aan het doen? Gewoon oja, weer een andere manier. Dus al die sites hebben verschillende manieren van betalen en dat soort dingen. Dus elke keer. Als het een beetje vreemd is denk je het zal wel erbij horen of wat heeft die nou weer bedacht.

De urgentie en de relevantie ontbreken bijvoorbeeld bij de ondernemer of het management om actie te ondernemen, omdat de mogelijke risico onvoldoende bekend zijn. Een aantal respondenten wijst ook op het feit de meeste dieven gelegenheidsdieven zijn. Eindgebruikers met een laag cyberbewustzijn die niet beschikken over de juiste vaardigheden lopen hierdoor extra kans om slachtoffer te worden. Deze slachtoffers zijn in feite onbewust onbekwaam. Zij zetten de digitale ramen en deuren soms wagenwijd open voor criminelen.

R10: Wij zien bijvoorbeeld heel veel slachtoffers bij MKB bedrijven waar eigenlijk niet eens heel veel te halen is, waar het wel heel makkelijk is om iets te halen. Gelegenheid maakt ook de dief.
R13: Dus de vaardigheid om dingen te herkennen. Wat ik al aangaf, het wordt zoveel mooier gemaakt dat het ook voor jou en mij lastiger is. Maar het is een kwestie van vaardigheid. Als je iets dagelijks doet is het ook makkelijker.

Onvoldoende cyberweerbaarheid
Een tweede reden waarom inwoners en ondernemers kwetsbaar zijn is vanwege onvoldoende weerbaarheid bij eindgebruikers. Een aantal experts geven aan dat inwoners en ondernemers zich onvoldoende kunnen wapenen tegen vormen van bedrog en diefstal. Dit komt volgens het MKB Cybercampus door een gebrek aan digitale vaardigheden. Criminelen spelen in op de kwetsbaarheden. Denk bijvoorbeeld aan spoofing waarbij ouderen worden opgelicht via WhatsApp. Door op het eerste oog vertrouwde personen in te zetten kunnen deze mensen geld afhandig worden gemaakt. Volgens de gemeente Nijmegen heeft dit grotendeels te maken met de naïviteit van eindgebruikers.
R4: Naïviteit, mensen die denken 'mij zal dit niet gebeuren', dan zal het juist wel een keer gebeuren. Daar kan je zeker van zijn.

R11: Onwetendheid met het middel met de device, onwetendheid met firewalls en wachtwoordbescherming en doorklinklinks, dat soort dingen.

Bedrijven en overheidsorganisaties beschikken eveneens over onvoldoende kennis en expertise op het gebied van cybersecurity. Volgens een expert van het Cybercentrum voor de Maakindustrie worden vaak de basismaatregelen niet of onvoldoende genomen binnen een organisatie, waardoor zijn extra kwetsbaar zijn en de continuïteit bij een incident direct in gevaar komt.

R10: Wat maakt deze bedrijven extra kwetsbaar? Omdat ze de basismaatregelen niet genomen hebben. Dus dan hebben het gewoon over patching, toegangsbeheer, antivirus, onvoldoende netwerk matering. Echt de standaard dingen omdat daar geen of onvoldoende maatregelen toe genomen zijn... En gecombineerd met die back-up die niet gedaan is.

Op basis van de geldende Algemene Verordening Gegevensbeheer (AVG) zijn gemeenten verplicht om een Chief Information Officer (CISO) aan te stellen. Een CISO behoort een onafhankelijke positie te hebben tegenover het management of bestuur van een gemeente. Deze functie is van belang voor de implementatie en uitvoering van informatiebeveiliging binnen een organisatie. Volgens een expert van de VeiligheidsAlliantie Rotterdam beschikken grotere gemeenten over voldoende capaciteit om bekwame CISO's aan te nemen die weten waarover ze het hebben. Dit geldt echter niet voor de kleinere gemeenten.

R17: De één heeft een CISO met heel veel ervaring en de ander zegt van joh, ik moet een CISO hebben dus volgens mij ben jij nog chef lege dozen dus dan ben jij de CISO omdat je weet hoe een computer werkt.

Een gebrek aan weerbaarheid geldt niet alleen voor overheidsinstellingen maar ook voor het midden- en kleinbedrijf. Volgens de expert van het Cybercentrum voor de Maakindustrie hebben veel ondernemers in het MKB helemaal geen beschikking over een CISO binnen de organisatie. Deze groep verwacht dat de ICT provider kan helpen bij incidenten. In de praktijk blijkt dit echter niet het geval te zijn. Daarnaast zien ondernemers in het MKB onvoldoende noodzaak om zich te wapenen tegen de risico's van cybercrime, vanwege de kosten die dat met zich meebrengt. De expert van VNO-NCW vat het samen met de woorden: 'ondernemers zijn immers bezig met de positieve kant van ondernemen, waarbij de waan van de dag voorrang heeft. Zolang de ondernemer niet getroffen wordt wanen zij zich veilig en ontbreekt de noodzaak om maatregelen te nemen.

R14: Als je niet het idee hebt dat het je kan treffen of dat het zoveel van collega's al getroffen heeft. Dat je echt loslopend wild bent, als je je dat niet realiseert dan… waarom zou je dan zoveel geld investeren in de beveiliging, als tijd investeren in organisatorische maatregelen?

Financiële nood

Een derde reden waardoor bepaalde doelgroepen kwetsbaar zijn voor vormen van bedrog en diefstal is de financiële prikkel. Criminelen spelen hierbij in op de kwetsbaarheden van eindgebruikers, zoals financiële nood. Kwetsbare jongeren kunnen bijvoorbeeld ingezet worden als geldezel, waardoor zij gemakkelijk slachtoffer kunnen worden van identiteitsfraude, maar ook van aan- of verkoopfraude.

R3: Het heeft ook zijn weerslag in de fysieke wereld doordat jongeren geronseld worden op schoolpleinen en daarmee ook gebruik maken van de kwetsbaarheid van die jongeren, door heel erg snel en gemakkelijk geld willen verdienen zonder daar iets voor te doen, terwijl ze wel onderaan de keten zitten van het criminele netwerk.
R17: Omdat zij financieel wat zwakker zijn en gevoelig zijn voor gadgets en leuke dingen om aan te schaffen. (…) Ze zien dus de urgentie qua tijd en het financiële voordeel, daarin zijn zij gewoon een stuk sneller. Ik denk dat dat de reden is waarom zij daarin trappen.

Ook andere doelgroepen kunnen kwetsbaar zijn voor financiële prikkels. Zo haalt de expert van ouderenbond KBO-PCOB aan dat ouderen die in financiële nood verkeren ook potentieel slachtoffer kunnen worden van bedrog en diefstal.

Lage pakkans
Eindgebruikers zijn kwetsbaar omdat de daders zich volgens de gemeente Enschede anoniem wanen. Daders hoeven niet fysiek op het plaats delict aanwezig te zijn waardoor de pakkans volgens de gemeente West-Betuwe een stuk kleiner is dan met de traditionele criminaliteit. Daarnaast kunnen daders zich ook in het buitenland begeven waardoor het lastig is de daders fysiek op te sporen.

R6: Dus de pakkans in gewoon erg klein en dat ze het vanuit hun luie stoel binnen of buiten Nederland kunnen regelen.
R16: En wat ook de gelegenheid bied is de anonimiteit van internet aan de daderkant.

Toenemende digitalisering
Door de toenemende digitalisering zijn eindgebruikers steeds vaker verbonden met het internet. Hoe meer tijd we online doorbrengen, hoe groter de kans op slachtofferschap volgens de politie. Daarnaast bestellen eindgebruikers steeds meer op het internet, waardoor het aantal aankopen in de fysieke omgeving afneemt.

R18: En de gelegenheid - we zijn zoveel online. Tijdens de coronacrisis zijn we nog meer online gegaan dan we voordien al deden. Dat is natuurlijk wel de digitale gelegenheid. (…) Als je tussen de twee en zes uur per dag achter een schermpje zit, dan ben je kwetsbaarder omdat je dan natuurlijk veel meer voorbij ziet komen (webshops, mailtjes, sms'jes, WhatsApp berichtjes).
R5: Ja dus toenemende mate van digitalisering. De diverse technieken die er niet makkelijker op zijn geworden en de vluchtige tijdsgeest. Dus alles moet snel, snel, snel.

De maatschappij wordt steeds digitaler ingericht waardoor het thema cybercrime zich niet alleen richt op de security van de bedrijfsvoering en de vitale infrastructuur. Eindgebruikers zijn ook thuis verbonden met het internet en werken ook thuis vanuit de '*cloud*'. Het is daarom niet alleen van belang om de security van de interne organisatie op orde te hebben, maar ook de safety. Eindgebruikers dienen ook thuis online weerbaar te zijn en veilig te handelen. Bedrijfsgegevens kunnen per slot van rekening ook bij werknemers thuis vanuit de cloud gestolen worden.

Tussenconclusie
Zowel gemeenten als de experts geven grotendeels identieke redenen aan waarom inwoners en ondernemers kwetsbaar zijn voor bedrog en diefstal. Eindgebruikers beschikken veelal over

onvoldoende risicobewustzijn. De risico's worden onvoldoende herkent, veelal vanwege onbewuste onwetendheid. Ook als eindgebruikers wel bekend zijn met de risico's wordt de kans op slachtofferschap als laag ervaren, doordat het een 'ver-van-mijn-bed-show' is. Dit wordt mede veroorzaakt door toenemende digitalisering en de afweging tussen gebruikersgemak versus veiligheid. De beleidsadviseurs geven aan dat daders zich anoniem wanen op het internet en de pakkans in verhouding tot de fysieke vormen van criminaliteit laag is. Zowel jongeren en ouderen zijn ook kwetsbaar vanwege financiële nood. De basismaatregelen worden vaak niet genomen door inwoners en ondernemers, waardoor zij zich onvoldoende kunnen wapenen. De experts geven aan dat de noodzaak om aandacht te besteden aan deze maatregelen veelal ontbreekt. Kleinere gemeenten zijn kwetsbaar door een gebrek aan kennis en expertise bij de door hen aangewezen Chief Information Officers (CISO).

5.2.4 Taken van organisaties

Tijdens het interview is gevraagd wat de taak van zijn of haar organisaties is bij het tegengaan van deze vormen van bedrog en diefstal. Indien dit niet besproken is, is de vraag gesteld: voert u of uw organisatie op dit moment ook taken uit om inwoners en ondernemers weerbaar te maken tegen bedrog en diefstal? Deze paragraaf maakt inzichtelijk welke taken de respondent aan zijn of haar eigen organisatie toekent.

Gemeenten

De respondenten geven aan dat de taken van gemeenten uiteen vallen in meerdere onderdelen en zowel intern als extern zijn georiënteerd, namelijk: 1) bewustwording creëren bij inwoners en ondernemers 2) bestuurlijke maatregelen, 3) eigen informatiebeveiliging op orde en tot slot 4) inzicht krijgen in aard en omvang van cybercrime.

Taken	**Gemeente**	**Aantal**
1. Bewustwording creëren bij inwoners en ondernemers	Neder-Betuwe, Deventer, Nijmegen, West-Betuwe, Winterswijk, Renkum, Enschede	7
2. Bestuurlijke maatregelen	Deventer, Nijmegen, Winterswijk, Enschede	4
3. Eigen informatiebeveiliging op orde	Nijmegen, Enschede	2
4. Inzicht krijgen in aard en omvang van cybercrime	Deventer	1

Tabel 5.3 Taken van gemeenten

Bewustwording creëren bij inwoners en ondernemers

De eerste taak van gemeenten is volgens alle respondenten om inwoners en ondernemers bewust te maken van de risico's en gevaren van cybercrime.

R9: En een tweede is dat wij wel dingen kunnen uitdragen en mensen daarvan bewust maken. Wij hebben natuurlijk een rol, wij staan in de spotlights.

De gemeente speelt volgens Winterswijk een sleutelpositie als het gaat om het weerbaar maken van inwoners en ondernemers. Ook Nijmegen sluit zich daar volledig bij aan. De lokale overheid kan door middel van voorlichting, het faciliteren van educatie en preventieve adviezen het risicobewustzijn van

inwoners en ondernemers vergroten. Daarnaast hebben de gemeenten volgens de beleidsadviseur van Nijmegen een aanjagende rol om cyber op te agenderen binnen de gemeente.

R3: Ik denk dat de voornaamste taak van de gemeente ligt op het bewust maken van inwoners en ondernemers en ook de weerbaarheid bevorderen: hoe zorgen we ervoor dat inwoners weten dat zij te maken hebben met frauduleuze transacties, dat ze te maken hebben met bedrog via WhatsApp? Hoe kunnen we inwoners daar handvaten bieden om daar niet in mee te gaan?
R6: In communicatie kunnen we het aanhalen maar hoe je het verder voorkomt zeg het maar… dan moet je gerichte bijeenkomsten gaan houden in bejaardentehuizen, die relatief gezien vaker slachtoffer zijn. Maar de bedoeling is wel dat we daar iets mee gaan doen.

Ook bij gemeenten waarbij deze kerntaak nog niet definitief is vastgesteld, wordt het belang van bewustwording onder inwoners en ondernemers onderstreept.

R12: Ik vind dat er een grotere rol rondom bewustwording en cybercriminaliteit bij de gemeente ligt. Maar tegelijkertijd is het nog geen kerntaak.

Bestuurlijke maatregelen
De tweede taak van de gemeente wordt door vier respondenten (Deventer, Nijmegen, Winterswijk, Enschede) omschreven als het treffen van bestuurlijke maatregelen binnen '*cyberspace*'. Door toenemende digitalisering voorzien steeds meer respondenten ook een online taak weggelegd voor gemeenten.

R3: Het nemen van bestuurlijke maatregelen, dat is een hele interessante: wat zou een burgemeester kunnen doen om ervoor te zorgen dat dit soort fraude niet of nauwelijks meer kan voorkomen? Hoe zorg je dat de situatie hersteld wordt? Op het moment dat we zicht hebben op iemand in de gemeente Deventer die dit stelselmatig doet, wat kunnen wij daar dan tegen doen?
R16: Maar dat is heel ontgonnen terrein, de bevoegdheden van de burgemeester. (…) De burgemeester heeft geen bevoegdheden in cyberspace. En dat is heel logisch maar ook een heel interessant vraagstuk. Wat kunnen we daar dan mee…

Voor het handhaven van de openbare orde en veiligheid in de fysieke wereld kan zowel strafrechtelijk als bestuursrechtelijk opgetreden worden. Maar voor de respondenten is het onduidelijk welke taken en verantwoordelijkheden de lokale overheid precies heeft in de digitale wereld. Dit dilemma wordt eveneens beschreven in het onderzoek 'burgemeesters in cyberspace' door Bantema et al., (2018).

Eigen informatiebeveiliging op orde
De derde taak die is weggelegd voor gemeenten is het op orde hebben van hun eigen ICT-systemen. Gemeenten zijn immers zelf verantwoordelijk voor het goed functioneren en beveiligen van de eigen digitale systemen en de continuïteit van de organisatie (VNG, 2017). Deze specifieke taak wordt door twee beleidsadviseurs van de gemeente Nijmegen en Enschede genoemd.

R4: De gemeente heeft zoveel informatie en dat gaat allemaal om burgers, bedrijven of verzin het maar. Om heel veel gevoelige informatie. Als die gegevens worden gestolen kan je er van alles en nog wat mee. Dus dat zou de gemeente goed op orde moeten hebben.

R16: Beschermen van je eigen IT systemen, daar zit bedrog en diefstal.

Opmerkelijk is dat de verantwoordelijkheid voor de beveiliging van de digitale systemen door één van de experts wordt doorgeschoven naar de ICT-afdeling van de desbetreffende organisatie. Deze derde specifieke taak wordt door alle andere gemeentelijke beleidsadviseurs niet als taak van de gemeente beschouwd of gezien als een gedeelde verantwoordelijkheid binnen de organisatie. Terwijl deze werknemers van de desbetreffende organisatie ook doelwit kunnen zijn van digitale vormen van bedrog en diefstal.

R16: Daar hebben we te voorkomen dat onze gegevens worden gestolen. Dus dat is een rol. Die ligt niet bij mij maar meer bij onze IT collega's, gelukkig.

Inzicht in de aard en omvang van cybercrime

De vierde taak van gemeenten is het inzicht verkrijgen in de aard en omvang van cybercrime. Het fenomeen cybercrime is nog onvoldoende in kaart gebracht. Om een gerichte aanpak of beleid te maken is het voor gemeenten van belang te weten hoe groot het probleem werkelijk is en welke vorm van bedrog en diefstal het meeste voorkomt. Een beleidsadviseur van de gemeente Deventer geeft in het interview aan dat deze taak op dit moment nog onvoldoende mogelijk is, vanwege het ontbreken van relevante informatie op lokale schaal.

R3: Daarnaast ook de beeldvorming: zoals je merkt, kan ik het niet altijd direct onderbouwen met cijfers specifiek voor de gemeente Deventer: dat is een traject dat we zijn ingeslagen met de politie en het OM, om dat meer te kunnen onderbouwen. Dus: in hoeverre komt verkoopfraude, spoofing, vriend-in-noodfraude hier nu voor?

Experts uit het werkveld

In tabel 5.4 geven alle experts uit het werkveld aan wat zijn of haar taak is van de desbetreffende organisatie waar de respondent werkzaam voor is.

Taken	Experts	Aantal
1. Bewustwording creëren bij inwoners en/of ondernemers	Cybersecuritycentrum voor de Maakindustrie, politie, Openbaar Ministerie, KBO-PCOB, Regionaal Informatiepunt Integrale Veiligheid, VeiligheidsAlliantie Rotterdam, VNO-NCW, MKB Cybercampus	8
2. Eigen informatiebeveiliging op orde	Veiligheidsregio IJsselland, Saxion, Regionaal Informatiepunt Integrale Veiligheid, VeiligheidsAlliantie Rotterdam	4
3. Belangen behartigen	KBO-PCOB, VNO-NCW	2
4. Opsporing en vervolging	Politie, Openbaar Ministerie	2
5. Gemeenten activeren, kennisuitwisseling stimuleren en lokale initiatieven inzichtelijk maken	Regionaal Informatiepunt Integrale Veiligheid, VeiligheidsAlliantie Rotterdam	2

Tabel 5.4 Taken van experts uit het werkveld

Bewustwording creëren bij inwoners en/of ondernemers

Het Cybersecurity Centrum voor de Maakindustrie (CCM) is gericht op de maakindustrie in de provincies Overijssel en Gelderland. De experts van het CCM geven bedrijven advies op het gebied van digitale veiligheid. Daarnaast vertalen zij dreigingsinformatie vanuit het Cyber Security Centrum (NCSC) naar relevante informatie voor bedrijven in de branche. In de praktijk voeren zij met experts een cybersecurityscan uit om bedrijven bewust te maken van mogelijke cyberrisico's. Dit is in feite een risicoanalyse waarbij bewustwording en het digitaal weerbaar maken van ondernemers centraal staat. Het CCM stimuleert daarnaast grote cybersecurity bedrijven om maatwerk te leveren aan kleine ondernemers in het MKB.

Het landelijke Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO) gaat uit van een taak die verder gaat dan het opsporen van criminelen. De politie heeft een strategie geformuleerd waarbij de organisatie uitgaat van weerbaarheid. Daarnaast verzorgt het landelijke Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO) ook voorlichting samen met diverse partners zoals Marktplaats.nl. De politie werkt ook samen met het handelsplatform om maatregelen te treffen, zoals het verstoren van criminelen bij vormen van aan- en verkoopfraude.

R18: Dus wij dragen bij aan de verhoging van de weerbaarheid van Nederland op het gebied van cybercrime. Dat is een hele belangrijke kanttekening, want je zou ook kunnen denken dat politie er is om boeven te vangen. Toch? Dat doen we ook.

Het OM onderschrijft het belang van het weerbaar maken van inwoners en ondernemers. De organisatie is samen met de politie bezig inwoners en ondernemers cyberweerbaar te maken. De respondent geeft daarbij wel aan dat preventie strikt formeel niet de taak is van het Openbaar Ministerie. Maar geeft wel aan dat bewustwording en preventie een positieve bijdrage leveren aan het verminderen van het aantal slachtoffers.

R5: Wij worden overspoeld met aangiftes, het wordt heel moeilijk om al die zaken in onderzoek te nemen. Zo kunnen we meer aan preventie doen, om zeg maar aan de voorkant al tot minder aangiftes te komen. (…) Dus het is niet dat wij de aangifte drempel moeten verlagen, dat wij meer aangiftes willen. Nee juist niet, wij willen juist zien te voorkomen dat men aangifte doet. Door bewustwording en door preventie.

Het MKB Cybercampus heeft als doel om de ondernemers in het MKB weerbaar te maken tegen cybercrime. De experts van het MKB Campus bieden een cybersecurityscan aan voor het bedrijfsleven. Deze scan wordt uitgevoerd door studenten met een relevante ICT opleiding onder leiding van een cybersecurity expert. Daarnaast zet de organisatie zich in op het gebied van bewustwording door middel van voorlichting en een MKB crisisgame.

KBO-PCOB faciliteert tabletcoaches, dit zijn vrijwilligers uit de organisatie die hun mede leeftijdsgenoten ondersteunen bij het gebruik van een tablet en tegelijkertijd wijzen ze op de mogelijke risico's. Daarnaast geven ze voorlichting op het gebied van digitalisering.

R13: Maar ook informatievoorziening, we hebben bijvoorbeeld tabletcoaches opgeleid die bijvoorbeeld die mensen verder kunnen 'scholen', laat ik het zo maar noemen en verder leren over dit soort fenomenen.

Eigen informatiebeveiliging op orde

Hogeschool Saxion heeft de taak van om intern de eigen informatiebeveiliging op orde te hebben. Volgens een respondent is dit met name de taak van de ICT-afdeling om andere medewerkers te wijzen op de mogelijke risico's van bedrog en diefstal. Dit kan de ICT afdeling doen door te wijzen op het regelmatig wijzigen van wachtwoorden.

R1: Dus zo'n ICT meneer moet mij wijzen op het maken van een goed password. En vooral niet een voorlopig password zo laten blijven he. Maar er echt op dat moment zeggen: je moet een eigen password maken. Er is wel een risico voor onze eigen bedrijfsinformatie, want dan zouden anderen informatie over studenten of toegang tot hun onderzoeken openbaar kunnen worden.

De Veiligheidsregio IJsselland onderstreept ook het belang van interne informatiebeveiliging. De informatieveiligheid wordt binnen de Veiligheidsregio gezien als een gedeelde verantwoordelijkheid en niet enkel de verantwoordelijkheid van de ICT-afdeling. Werknemers worden bijvoorbeeld bewust gemaakt van het feit dat ze hun 'tag' (toegangspas) niet moeten laten rondslingeren in het gebouw.

R11: De taak van de Veiligheidsregio is zeer beperkt binnen diefstal en bedrog.. (…) natuurlijk voor onze eigen informatiebeveiliging. Dus het heeft wel effect maar dan met een andere tak van sport. Wij onderscheiden de crisisbeheersing, waar we op moeten treden voor het effect buiten en onze eigen informatievoorziening: beschikbaarheid, integriteit en vertrouwelijkheid.

Opsporing en vervolging

De politieorganisatie krijgt volgens de desbetreffende expert zoveel aangiften binnen van cybercrime dat ze deze meldingen niet één voor één kunnen behandelen. Dit geldt bijvoorbeeld voor aan- en verkoopfraude, waarbij jaarlijks circa 40.000 aangiften binnenkomen. De politie bundelt aangiften waardoor de grote zaken worden opgepakt en verdachten worden opgespoord.

R18: Het is een golf wat over je heen komt, maar wat wij natuurlijk wel doen, is bundelen, want er zitten over het algemeen groeperingen achter. Dan krijg je dat weer overzichtelijker, en dan pakken we natuurlijk de grote zaken op. Prima, maar we kunnen dus nooit alles oppakken.

Het Openbaar Ministerie (OM) staat in voor vervolging van verdachten. Het OM is belast met het opsporen van strafbare feiten en het verzamelen van bewijsmateriaal. Daarnaast analyseren zij aangiftes die binnenkomen om vervolgens een verdachte te identificeren.

Belangenbehartiging

De seniorenorganisatie KBO-PCOB behartigt de belangen van ouderen. De organisatie zet ook in op het gebied van digitalisering. Zo is KBO-PCOB van mening dat er een alternatief vangnet moet zijn voor ouderen. Door de toenemende digitalisering kunnen ouderen soms niet mee komen met deze digitale ontwikkelingen, zoals internetbankieren.

De brancheorganisatie VNO-NCW behartigt de belangen van ondernemers in het MKB. Dit gebeurt met name op het gebied van wet- en regelgeving.

Gemeenten activeren, kennisuitwisseling stimuleren en lokale initiatieven inzichtelijk maken

Het Regionaal Coördinatiepunt Integrale Veiligheid (RCIV) en de VeiligheidsAlliantie Rotterdam (VAR)

zijn regionale veiligheidsnetwerken. In deze samenwerkingsverbanden zijn politie, Openbaar Ministerie, gemeenten en andere betrokken partijen aangesloten. De taak van het RCIV en de VAR op het gebied van digitale criminaliteit is om lokale initiatieven inzichtelijk te maken en uit te wisselen. De VeiligheidsAlliantie Rotterdam en het Regionaal Informatiepunt Integrale Veiligheid ondersteunen gemeenten met concrete instrumenten en campagnes om inwoners en ondernemers in het MKB cyberweerbaar te maken.

R8: Maar, we denken dat het voor onze regio een breed programma hebben waar we variëren van: poort dichthouden (weerbaar worden) tot bewustwording richting inwoners.
R17: Want de meesten hebben in hun integraal veiligheidsplan iets staan over cybercrime. Vaak alleen maar omdat het geadviseerd werd maar uitvoeren is vaak wat ingewikkelder. Dus wat wij doen is hen stimuleren. En wij proberen dan kant en klaar pakket aan te bieden waar zij gebruik van kunnen maken.

Tussenconclusie
De gemeente speelt op lokaal niveau een belangrijke rol in het creëren van bewustwording en het cyberweerbaar maken van inwoners en ondernemers. Dit geldt eveneens voor de politie en Openbaar Ministerie, maar ook voor belangenverenigingen en regionale veiligheidsnetwerken. Daarnaast zien gemeenten een taak voor zich weggelegd als het gaat om het nemen van bestuurlijke maatregelen tegen online verstoringen van de openbare orde en veiligheid. De derde taak is gericht op de interne organisatie en betreft het op orde brengen van de eigen informatiebeveiliging. Dit wordt door zowel gemeenten als experts gezien als een belangrijk onderdeel van de eigen interne organisatie. Tot slot dienen gemeenten zicht te krijgen op de aard en omvang van slachtofferschap en daderschap op lokaal niveau. Om een gerichte aanpak of beleid te maken is het voor gemeenten van belang om te weten hoe groot het probleem daadwerkelijk is en welke vorm van bedrog en diefstal prioriteit heeft. De daadwerkelijke opsporing en vervolging wordt gezien als kerntaak van de traditionele strafrechtelijke instituties. Daarnaast voorzien regionale veiligheidsnetwerken in het inzichtelijk maken van lokale initiatieven, het uitwisselen van kennis en het activeren van gemeenten om met het thema cyber aan de slag te gaan.

5.2.5 Capaciteit
De respondenten hebben tijdens het interview antwoord gegeven op de vraag hoeveel capaciteit er vrijgemaakt is voor taken op het gebied van cybercrime. De capaciteit wordt bepaald aan de hand van drie indicatoren: tijd, middelen, beleidsprioriteit. De vervolgvraag is of dit volgens de respondenten voldoende is voor de uitvoering.

Gemeenten
De beleidsadviseurs van de verschillende gemeenten schetsen het volgende beeld wat betreft tijd, middelen en beleidsprioriteit (zie tabel 5.4).

Gemeenten	**Tijd**	**Middelen**	**Beleidsprioriteit**
Neder-Betuwe	Voldoende	Onbekend	Geen beleidsprioriteit

Deventer	Voldoende	Onbekend	Geprioriteerd thema Meerjarenbeleidsplan 2020/2023
Nijmegen	Onvoldoende	Onbekend	Geen beleidsprioriteit
West-Betuwe	Voldoende	Onbekend	Geen beleidsprioriteit
Winterswijk	Voldoende	Onvoldoende	Geen beleidsprioriteit
Renkum	Onvoldoende	Onvoldoende	Geen beleidsprioriteit
Enschede	Onvoldoende	Onvoldoende	Geen beleidsprioriteit

Tabel 5.4 Capaciteit van gemeenten op basis van tijd, middelen en beleidsprioriteit

Tijd

Vier van de zeven beleidsadviseurs (Neder-Betuwe, Deventer en West-Betuwe en Winterswijk) geven aan dat ze voldoende tijd beschikbaar hebben voor cybercrime. Bij de gemeente Neder-Betuwe en West-Betuwe is er op dit moment geen specifiek aantal uren vrijgemaakt voor cyber. Het onderwerp behoort echter tot het standaard takenpakket van de beleidsadviseurs. De gemeente Neder-Betuwe geeft aan dat er op dit moment geen aanleiding is het aantal uren op dit terrein te vergroten.

R2: Maar ik denk wel dat als je een uitgebreid plan van aanpak wil, of op een projectmatige basis wilt werken. Dat je dan wel wat extra te besteden uren nodig hebt. Maar daar hebben we nu geen aanleiding voor.

De beleidsadviseur van de gemeente Deventer geeft aan dat er op dit moment voldoende capaciteit is vrijgemaakt om het thema digitale criminaliteit te ontwikkelen, namelijk 8 beschikbare uren in de week. De gemeente Renkum beschikt over onvoldoende tijd, vanwege de inspanningen rondom het COVID-19 virus. Een uitbreiding van het aantal FTE kan hierin uitkomst bieden, maar beleidsadviseurs van de gemeente Enschede en Nijmegen zien een uitbreiding op het gebied van cybercrime voorlopig niet gebeuren.

R4: Gemeenten moeten nu bezuinigen. Het is eigenlijk niet te verantwoorden om daar nu extra capaciteit bij te vragen op welk gebied dan ook. Dus blijven bij wat je doet en het liefst nog hetzelfde doen met minder mensen. Maar we weten dat het belangrijk is.
R16: Nee, dat is heel afhankelijk of er capaciteit bijkomt. Maar zeker met corona… Voor corona waren we al in 'financiële trouble' en na corona nog erger. Dus ik zie het somber in qua capaciteit en dan moet iemand dat erbij gaan doen.

De beleidsadviseurs van de gemeente Enschede en Deventer benadrukken het belang van samenwerking met andere gemeenten op het gebied van cybercrime. Zij komen bijeen in regionale veiligheidsnetwerken, zoals het Twentse expertteam Cybercrime van het Platform Integrale Veiligheidszorg (IVZ). Deze samenwerking staat volgens de gemeente Enschede echter in de kinderschoenen. Daarnaast geeft de respondent aan dat er op het gebied van cybercrime meer moet gebeuren.

R16: Dus is het een beetje doen wat we kunnen. En dat is eigenlijk wel jammer hoor want ik vind het wel een thema dat onvoldoende aandacht krijgt voor iets wat zo de toekomst is.

Middelen

Een ander component binnen het capaciteitsvraagstuk zijn de financiële middelen. De gemeenten Renkum, Winterswijk en Enschede geven aan dat er te weinig financiële middelen zijn om met het onderwerp Cyber aan de slag te gaan. Ook het vinden van het juiste personeel op dit gebied is een probleem. Zo geeft een respondent aan dat er in principe voldoende capaciteit is, maar dat het ontbreekt aan de juiste kennis en expertise op dit gebied. Dit komt doordat ICT-experts meer verdienen in de commerciële sector dan bij een overheidsinstelling.

R3: Het is niet op voorhand al gezegd dat je bij digitale criminaliteit of digitale veiligheid dit bedrag krijgt. Nee, er is echt gewoon nul euro begroot.
R9: Misschien is er op papier wel ruimte, maar ik hoor ook wel dat het lastig is om de goede mensen te vinden die daarmee bezig gaan. Dat heeft ook een beetje te maken met dat wij als overheid gewoon achterlopen met betalen in vergelijking met de markt, zeg maar.
R12: (..) maar eigenlijk omdat er gewoon geen budget is. Want als je alles van voor tot achter zelf moet doen dan kost het teveel geld.

Beleidsprioriteit

De gemeente Deventer heeft als enige het onderwerp cybercrime/digitale criminaliteit als speerpunt geprioriteerd in het meerjarenbeleidsplan 2020/2023. De overige zes gemeenten hebben cybercrime/gedigitaliseerde criminaliteit niet geprioriteerd in het Integraal Veiligheidsplan (IVP) of andere beleidsvisiedocumenten. Hierdoor blijft het thema buiten de beleidsplannen en is er geen vastgesteld politiek/bestuurlijk draagvlak om hiermee aan de slag te gaan. Daarnaast geeft de gemeente West-Betuwe aan dat sommige gemeenten ook kiezen voor andere prioriteiten dan het thema cybercrime.

R6: Sommige gemeenten hebben gewoon geen capaciteit en kiezen voor andere prioriteiten.

Experts uit het werkveld

De experts uit het werkveld schetsen het volgende beeld wat betreft tijd, middelen en prioriteit (zie tabel 5.5).

Gemeenten	**Tijd**	**Middelen**	**Beleidsprioriteit**
Politie (Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO)	Onvoldoende	Onvoldoende	Geprioriteerd beleidsthema
Openbaar Ministerie	Onvoldoende	Onvoldoende	Geprioriteerd beleidsthema
Regionaal Coördinatiepunt Integrale Veiligheid	Voldoende	Onvoldoende	Geprioriteerd beleidsthema
Hogeschool Saxion/Space53	Voldoende	Onbekend	Onbekend

Cybercentrum voor de Maakindustrie	Voldoende	Onvoldoende	Geprioriteerd beleidsthema
Veiligheidsregio IJsselland	Voldoende	Voldoende	Onbekend
KBO-PCOB	Onbekend	Onvoldoende	Geprioriteerd beleidsthema
VNO-NCW	Onvoldoende	Onvoldoende	Onbekend
VeiligheidsAlliantie Rotterdam	Onvoldoende	Onbekend	Geprioriteerd beleidsthema

Tabel 5.5 Capaciteit experts uit het werkveld op basis van tijd, middelen en beleidsprioriteit

Tijd

De expert van het Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO) geeft in het interview aan dat door de hoeveelheid aangiften het niet mogelijk is om elke aangifte apart in behandeling te nemen.

R18: Het is een golf wat over je heen komt, maar wat wij natuurlijk wel doen is bundelen, want er zitten over het algemeen groeperingen achter. Dan krijg je dat weer overzichtelijker, en dan pakken we natuurlijk de grote zaken op.

De expert van het ECDO benadrukt dat de politie, los van het capaciteitsvraagstuk, efficiënter kan werken op het thema cybercrime. Door intern slimmer te werken en extern samen te werken is het mogelijk efficiënter te werk te gaan. Daarnaast voorziet de expert van het ECDO een beperkte capaciteit als het gaat om digitaal rechercheren. De politie ziet niet alleen de klassieke taak die van de politie verwacht wordt, namelijk: 'boeven vangen'. Maar zij zien ook een rol voor zich weggelegd in de preventieve schakel van de aanpak van cybercrime.

Het Openbaar Ministerie beschikt over een geoormerkte capaciteit op het gebied van cybercrime. Volgens een respondent van het OM Oost-Nederland is er echter onvoldoende capaciteit voor het aantal zaken dat binnenkomt. Dat is binnen het Openbaar Ministerie geen uniek probleem voor het thema cybercrime, maar geldt ook voor alle andere vormen van criminaliteit. De respondent geeft dat het bij de beperkte capaciteit van het Openbaar Ministerie van belang is om bepaalde zaken voorrang te geven. Hierbij krijgen bepaalde zaken wel prioriteit en andere niet. De belangrijke zaken worden daardoor eerder opgepakt binnen de organisatie en andere zaken blijven liggen.

R5: Ja, is dat voldoende capaciteit? Nee, als je dat afzet tegen de omvang van het aantal aangiftes wat binnenkomt.

Het Regionaal Coördinatiepunt Integrale Veiligheid beschikt over voldoende vrijwillige inzet van betrokken organisaties om de werkzaamheden uit te voeren.

R8: We doen het op basis van vrijwilligheid vanuit de betrokkenheid van de betrokken gemeenten en de collega's van de veiligheidspartners. Dus ja, op dit moment mogen we zeker niet klagen. Er is voldoende inzet en betrokkenheid van alle partners. Dus daar ben ik heel blij mee.

Een expert van de ondernemersvereniging VNO-NCW stelt eveneens dat de organisatie beschikt over onvoldoende uren om de urgentie van cybercrime op de politieke agenda te zetten. Enerzijds omdat de urgentie van dit thema in politiek Den Haag niet alleen door VNO-NCW gedaan kan worden. Andere partijen dienen daar ook een rol in te spelen. En anderzijds omdat de desbetreffende respondent de enige beleidsmedewerker is binnen de organisatie die gaat over criminaliteit bij het midden- en kleinbedrijf. Daarnaast gaat de meeste aandacht van de beleidsmedewerker uit naar publiek-private samenwerking op het gebied van ondermijning en niet naar het thema cybercrime. Daarnaast geeft de beleidsmedewerker af en toe voorlichting bij MKB bijeenkomsten in het land.

Een beleidsadviseur van de VeiligheidsAlliantie Rotterdam geeft in het interview aan dat het thema cybercrime veel van zijn beschikbare tijd in beslag neemt. Cybercrime wordt in het Rotterdamse veiligheidsnetwerk opgepakt door twee personen binnen de organisatie. De beleidsmedewerker heeft drie beleidsthema's binnen de organisatie, maar kan de beschikbare tijd ook volledig vullen met het thema cybercrime. Het onderwerp cybercrime vraagt meer aandacht dan er op dit moment mogelijk is binnen de huidige capaciteit van de organisatie.

R17: Dus ik denk dat we ongeveer twee dagen aan cyber kunnen besteden in totaal. (…) We zouden het eigenlijk moeten uitbreiden omdat niet iedere gemeente heel erg actief is. Dus dat het vooral trekken en sleuren is bij veel gemeenten.

Middelen

Een expert van het Expertise Cybercrime en Digitaal Opsporen (ECDO) schuift het capaciteitsvraagstuk af op een politieke afweging. Meer capaciteit is mogelijk als er ook meer budget voor beschikbaar wordt gesteld. Dit betekent volgens de desbetreffende expert dat burgers meer belasting moeten betalen. Afgezien van de politieke keuze betekend dit dat de middelen bij de politie op dit moment ontoereikend zijn.

R18: Dat willen we ook niet, dus je zult een balans moeten zoeken in capaciteit en wat je ervoor over hebt. Dus ik vind niet dat wij te weinig capaciteit hebben.

Het Regionaal Informatiepunt Integrale Veiligheid heeft voor het thema cybercrime/gedigitaliseerde veiligheid geen budget ter beschikking. Uit het projectplan blijkt dat er geen financiële middelen beschikbaar zijn gesteld.

Een expert van het Cybercentrum voor de Maakindustrie geeft aan dat de organisatie beschikt over beperkte financiële middelen vanuit de landelijke subsidieregeling. Deze subsidiegelden worden door het Digital Trust Center ter beschikking gesteld na goedkeuring door een onafhankelijke adviescommissie.

R10: Maar dan met de 2 ton subsidie die je dan krijgt voor de komende drie jaar, dat is gewoon een lachertje. Daar gaat het op dit moment mis.

Een expert van de seniorenorganisatie KBO-PCOB geeft in het interview aan dat de organisatie beschikt over onvoldoende financiële middelen om het thema cybercrime aan te pakken. Enerzijds omdat ze niet beschikken over structurele subsidies en anderzijds omdat er maar een beperkt budget beschikbaar is voor beleidsmedewerkers die enkel worden bekostigd van uit de ledenbijdragen. De respondent geeft aan dat voor sommige projecten wel subsidie beschikbaar is vanuit de overheid.

Maar dat de urgentie soms ontbreekt op het thema cybercrime omdat cyber volgens de respondent niet valt onder de noemer ‘high impact crime’.

R13: En dat is maar een beperkt bedrag en daar moeten we heel veel voor doen. Het is misschien flauw om te beginnen over geld, maar het is wel een belangrijk iets. Dat betekent dat we soms subsidiegelden nodig hebben en dat krijgen we niet.

Beleidsprioriteit

Zeven van de negen organisaties hebben cybercrime/gedigitaliseerde criminaliteit als beleidsthema geprioriteerd. Waarbij de politie en het Openbaar Ministerie ook juridisch is vastgelegd in wet- en regelgeving. Bij een drietal experts uit het werkveld is onbekend of cybercrime daadwerkelijk een beleidsprioriteit is binnen de organisatie.

Tussenconclusie

De capaciteit van zowel gemeenten als experts uit het werkveld laat een zorgwekkend beeld zien. In de volle breedte is er te weinig tijd, middelen of prioriteit bij gemeenten op het gebied van cybercrime. Zes van de zeven gemeenten hebben het thema cybercrime niet geprioriteerd binnen hun eigen organisatie. Daarnaast blijken de middelen van gemeenten bij drie van de zeven gemeenten niet toereikend te zijn, waardoor de gemeente geen budget kan uittrekken voor lokale projecten om inwoners en ondernemers cyberweerbaar te maken. Naast de beperkte middelen heeft bijna de helft van de gemeenten onvoldoende mankracht om daadwerkelijk met cybercrime aan de slag te gaan. Dit geldt eveneens voor vier van de negen experts uit het werkveld. Het thema cyber vraagt om meer capaciteit dan er op dit moment mogelijk is. Naast het beperkte aantal FTE zijn de middelen bij meer dan de helft van de experts ontoereikend voor de aanpak van cybercrime.

5.3 Hoe ziet de huidige samenwerking op het gebied van bedrog en diefstal eruit?

Het volgende onderdeel gaat over huidige samenwerking van organisaties op het gebied van bedrog en diefstal. Respondenten hebben antwoord gegeven op de vraag: met welke andere organisaties werkt uw organisatie samen, wat is ieders taak binnen die samenwerking en hoe wordt deze samenwerking ervaren en zijn er wellicht problemen die de samenwerking bemoeilijken.

5.3.1 Huidige samenwerking

In deze paragraaf wordt het aantal deelnemers van de verschillende samenwerkingsverbanden inzichtelijk gemaakt. Deze paragraaf is omwille van de leesbaarheid opgedeeld in drie verschillende lagen, namelijk: lokaal, regionaal en nationaal niveau. In deze paragraaf wordt duidelijk met welke organisaties gemeenten en experts samenwerken op het gebied van cybercrime.

Lokaal niveau

De meeste gemeenten geven aan dat ze op lokaal niveau samenwerken met de politie en het Openbaar Ministerie. Zo staat er een vast overleg ingepland bij de gemeente Neder-Betuwe met de traditionele strafrechtelijke instituties waarbij het thema cybercrime ook regelmatig wordt geagendeerd. De politie is volgens de gemeente Neder-Betuwe, Deventer en Enschede een belangrijke partner aangezien zij beschikken over de benodigde informatie op lokaal niveau.

R2: Juist met de politie maak ik de afspraak op dit gebied. Want zij zijn de leverancier van de informatie dus zij geven mij de informatie voor bepaalde onderwerpen.

De meeste respondenten benadrukken echter dat de samenwerking geen structureel karakter heeft. Zo pakt de gemeente Renkum het onderwerp ‘cybersecurity’ op met de politie tijdens de Week van de Veiligheid en de gemeente Winterswijk zoekt de samenwerking op met de onder andere de politie en de SNS bank om voorlichting te geven over veilig internetten. In Winterswijk komt het onderwerp cyber incidenteel aan bod bij zorg- en veiligheidscasussen in het RIEC overleg. Ook de gemeente Deventer werkt op projectmatige basis samen met andere organisaties op het gebied van cyber gerelateerde criminaliteit. Zo werken zij samen met de politie, Rabobank, jongerenwerk, Saxion en een advocatenkantoor in de strijd tegen geldezels, waarbij jongeren slachtoffer kunnen worden van identiteitsfraude. Daarnaast werkt de gemeente Deventer samen met verschillende partners rondom het thema Veilig Ondernemen, waarbij zowel de politie als ondernemers bij betrokken zijn.

R3: Daarnaast voeren we ook een aantal acties uit in het project veilig ondernemen: het weerbaar maken van ondernemers, daar verwerken we dit eigenlijk al in. Als je het bijvoorbeeld hebt over phishing, gegevensdiefstal van ondernemers, dan zitten we al wel zijdelings naast ons reguliere pakket.

Regionaal niveau

Op regionaal niveau wordt er op verschillende overleggremia ’s samengewerkt tussen gemeenten, politie, OM en andere partijen. Oost-Nederland beschikt over drie regionale netwerken op het gebied van cybercrime. Het eerste regionale veiligheidsnetwerk betreft het team Cyber van het Veiligheidsnetwerk Oost-Nederland. In dit multidisciplinaire team werken de gemeenten: Winterswijk, Ede, Neder-Betuwe, Nijmegen, Renkum, Zwarte Waterland, Deventer en Bronckhorst samen met de traditionele strafrechtelijke partners politie Oost-Nederland, Openbaar Ministerie, maar ook met het Regionaal Informatiepunt Integrale Veiligheid, Hogeschool Saxion, Space 53, Provincie Overijssel, Veiligheidregio’s IJsselland en Gelderland-Zuid. Eén van de deelnemende organisaties neemt het

voortouw als ambtelijk trekker van het expertteam. Hiermee komt de structuur van de samenwerking het meest overeen met een leiderorganisatienetwerk van Kenis en Provan (2008).

Het tweede regionale samenwerkingsverband op het gebied van cybercrime/gedigitaliseerde criminaliteit behoort tot het Regionaal Coördinatiepunt Integrale Veiligheid (RCIV). Dit is eveneens een regionaal samenwerkingsverband op kleinere schaal in de regio IJsselland. In dit samenwerkingsverband zijn de volgende partijen betrokken: politie, Openbaar Ministerie, Veiligheidsregio IJsselland en de gemeenten Deventer, Zwolle, Zwartewaterland, Steenwijkerland. De coördinator van het Regionaal Coördinatiepunt Integrale Veiligheid geeft aan dat het veiligheidsnetwerk in de toekomst graag commerciële partijen wil betrekken bij de aanpak van digitale criminaliteit in IJsselland.

R8: Samen met de basis, de kern. Maar we hebben ook uitstapjes met private partners, zoals een Rabobank of een… Dat is nu nog niet, maar dat zou ik op termijn wel heel leuk vinden. Maar de vaste kern is gemeenten, politie en OM, Veiligheidsregio, volgens mij.

Het derde veiligheidsnetwerk wat in Oost-Nederland actief is op het gebied van cybercrime bevindt zich in Twente. Het expertteam Cybercrime Twente is onderdeel van het Platform Integrale Veiligheidszorg (IVZ). Het regionale veiligheidsnetwerk in Twente bestaat eveneens uit verschillende gemeenten en veiligheidspartners, zoals politie, Openbaar Ministerie en de gemeenten Enschede, Rijssen-Holten en Wierden. Dit samenwerkingsverband bevindt zich echter nog in de opstartfase.

Onlangs heeft de gemeente Nijmegen in samenwerking met politie en Openbaar Ministerie de samenwerking opgezocht met commerciële partijen. Eind 2017 startte het Openbaar Ministerie, politie en gemeente Nijmegen met het idee van een pilot rondom het ontwikkelen een barrièremiddel tegen accountovername (Gemeente Nijmegen, 2019). Dit betreft het hacken van gebruikersaccounts bij webwinkels en telecombedrijven met als doel het verkrijgen van goederen. Deze pilot leidde tot de projectgroep Aanpak digitale criminaliteit Oost-Nederland. Het doel van dit project was om samen met fraude-experts van commerciële partijen een alliantie mogelijk te maken om '*awareness*' en preventie te creëren. Aan de hand van twee expertsessies met fraude-experts werd het belang duidelijk van een wisselwerking tussen overheid en marktpartijen bij een effectieve bestrijding van online-fraude. Enerzijds is het van belang dat marktpartijen aangiftes doorzetten, zodat politie en OM deze waardevolle informatie kunnen gebruiken voor het in kaart brengen van de problematiek en om te komen tot opsporing en vervolging van daders. En anderzijds is het van belang dat politie en OM hun rollen vervullen om werkelijk verschil te maken met de inzet op specifieke terreinen en naderhand een terugkoppeling geven. Het barrièremiddel is echter niet van de grond gekomen omdat de verschillende partijen te ver uit elkaar lagen en te veel discussie ontstond over de vraag wie welke verantwoordelijkheden heeft en of het initiatief bij de overheid ligt of juist bij de private sector vandaan moet komen.

Het Cybercentrum voor de Maakindustrie werkt ook op regionaal niveau samen met verschillende netwerk- en kennispartners. Onder de netwerkorganisaties vallen bijvoorbeeld brancheorganisaties zoals de Metaalunie, Vereniging van de Maakindustrie in Oost-Nederland (VMO), maar ook met overheidsorganisaties zoals de Provincie Overijssel. De provincie subsidieert een voucherregeling voor de cybersecurityscan voor bedrijven. Het Cybercentrum voor de Maakindustrie werkt ook samen andere regionale partners zoals het MKB Cybercampus in Noord-Holland. Daarnaast werkt het Cybercentrum voor de Maakindustrie samen met kennispartners, waaronder onderwijsinstellingen (Universiteit van Utrecht en Hogeschool Saxion) en cybersecuritybedrijven.

Maar ook met landelijke netwerkpartners zoals het Digital Trust Center (DTC). Het DTC is ontstaan uit initiatief van het Ministerie van Economische Zaken om ondernemers in de niet-vitale sector cyberweerbaar te maken. Ook zij verschaffen subsidie en richten zich met name op het creëren van bewustwording onder MKB'ers.

De VeiligheidsAlliantie Rotterdam werkt samen met 25 gemeenten, politie, Openbaar Ministerie, Platform Veilig Ondernemen en met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Op het gebied van cybercrime werkt de VeiligheidsAlliantie samen met de Veiligheidsregio Rotterdam-Rijnmond, Informatie Beveiligingsdienst en onderwijsinstellingen zoals Hogeschool Saxion en de Haagse Hogeschool.

Tot slot werkt het MKB Cybercampus samen op projectbasis met de Dairy Campus, UWV en verschillende gemeenten, waaronder Leeuwarden en Heerenveen. Ook werken ze samen met de politie, onderwijsinstellingen, het Centrum voor Criminaliteitspreventie en Veiligheid en Platform Veilig Ondernemen.

Nationaal niveau

Op landelijk niveau werkt het Expertisecentrum Cybercrime en Digitale Opsporing van de politie samen met verschillende organisaties en instanties. Zo werkt het Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO) samen met banken bij het tegengaan van aan- en verkoopfraude. De banken hebben immers de monetaire infrastructuur in handen en zien verdachte transacties voorbij komen. Daarnaast werkt het Expertisecentrum Cybercrime en Digitale Opsporing samen met het platform Marktplaats.nl. Op dit handelsplatform werken zij samen om daders te verstoren zodat zij geen slachtoffers meer kunnen maken. Ook werkt het landelijke Expertisecentrum Cybercrime en Digitale Opsporing samen met hosting- en serviceproviders en de Autoriteit Consument en Markt (ACM) bij het opsporen van 'fake webshops', waarbij vormen van fraude aan de orde zijn. De Autoriteit Consument en Markt heeft immers de officiële taak om deze webshops in samenwerking met hosting- en serviceproviders te halen.

R18: Een website, bijvoorbeeld voor concertkaartjes, waarvan wij constateren dat er fraude wordt gepleegd. Dan bellen wij daarover met de Autoriteit Consument en Markt (ACM).

Brancheorganisatie VNO-NCW werkt met verschillende partners samen aan de Week van de Veiligheid waar ondernemers een veiligheidsontbijt en voorlichting over cybercrime krijgen. Dit doet de brancheorganisatie samen met politie, Openbaar Ministerie en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). VNO-NCW werkt daarnaast op landelijk niveau samen met de politie, Openbaar Ministerie, de Haagse Hogeschool en het Digital Trust Center (DTC).

De seniorenorganisatie KBO-PCOB heeft nauwe contacten met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Slachtofferhulp Nederland en de Fraudehelpdesk. Ook neemt de seniorenorganisatie deel aan het Maatschappelijk Overleg Betalingsverkeer (MOB) waarbij een groot aantal deelnemers zijn vertegenwoordigd. Binnen de MOB bestaat een werkgroep waarin fysieke en digitale veiligheid wordt besproken.

R13: Dat is dan met een aantal brancheverenigingen en met de Nederlandse Vereniging van Banken en de betaalvereniging. Een aantal partijen waar dit soort informatie vaak ter sprake komt.

Tussenconclusie
Op lokaal niveau werken een aantal gemeenten samen met lokale partners en de traditionele strafrechtelijke instituties zoals de politie en het Openbaar Ministerie. De samenwerking op dit niveau is veelal op projectmatige basis en niet structureel van aard. Op regionaal niveau zijn verschillende samenwerkingsverbanden te onderscheiden, waaronder drie regionale veiligheidsnetwerken in Oost-Nederland met een groot aantal deelnemers en gecoördineerd vanuit een administratieve entiteit. Op nationaal niveau is alleen het Maatschappelijk Overleg Betalingsverkeer als administratieve entiteit te onderscheiden.

5.3.2 Taken binnen de samenwerking
In deze paragraaf wordt beschreven in hoeverre er door de regionale veiligheidsnetwerken in Oost-Nederland een vaste taakverdeling is vastgesteld. Een duidelijke verdeling van taken kan immers bijdragen aan de effectiviteit van het samenwerkingsverband (Jacobs e.a., 2016).

Het Veiligheidsnetwerk Oost-Nederland heeft in het uitvoeringsplan cybercrime 2019-2020 (2019) de organisatie van het expertteam Cyber beschreven. Daarnaast worden de doelen uiteengezet en de uit te werken opdrachten geformuleerd voor de komende twee jaar. Het expertteam wordt voorgezeten door een bestuurlijk portefeuillehouder en een ambtelijk trekker en bestaat uit een vijftal werkgroepen. De leden van het expertteam komen op basis van het uitvoeringsplan periodiek bijeen. De werkelijke totstandkoming van het team Cyber blijkt echter weerbarstig te zijn. Het team Cyber is in het verleden driemaal bij elkaar gekomen om gezamenlijk de lijnen uit te zetten. Na de derde bijeenkomst heeft er geen vervolg meer plaatsgevonden. Enkele respondenten binnen het team Cyber geven aan dat dit mede komt door het vertrek van de ambtelijk trekker van het team.

R8: Dat is een beetje doodgebloed door het vertrek van de ambtelijk trekker.
R9: Volgens mij hebben we drie bijeenkomsten met elkaar besproken over waar gaat dit nou over en waar houdt dit nou op.

Uit het uitvoeringsplan 2019-2020 blijkt dat alle werkgroepen verantwoordelijk zijn voor de uitwerking van één van de vijf geformuleerde opdrachten. Een vaste verdeling van taken binnen het team Cyber van het Veiligheidsnetwerk Oost-Nederland is echter niet tot stand gekomen. Er is op dit moment geen sprake van structurele samenwerking tussen de verschillende organisaties. In het verleden zijn de verschillende deelnemers bij elkaar gekomen om kennis uit te wisselen en gezamenlijke doelen vast te stellen. Er is echter sprake van een lage mate van doelconsensus (Provan & Kenis, 2008). Zo merkt een expert op dat de doelstellingen onvoldoende concreet zijn en dat deelnemende gemeenten in beperkte mate betrokken werden.

R8: Dat kwam al niet echt van de grond, het werd heel weinig concreet en ik vond dat gemeente daar onvoldoende bij aangehaakt werden. Dus dat is echt jammer.

Het Regionaal Informatiepunt Integrale Veiligheid (RCIV) in IJsselland beschikt eveneens over een regionale werkgroep. De deelnemers van de werkgroep komen eens per vier weken bijeen en werken in kleinere werkgroepen aan (tussen)producten. Uit het projectplan digitale veiligheid en weerbaarheid van het RCIV (2020) blijkt dat de werkgroep inzet op vijf sporen. Binnen elk afzonderlijk spoor zijn is aantal leden van verschillende gemeenten of veiligheidspartners verantwoordelijk voor een (tussen)product. Binnen deze samenwerking werken gemeenten aan projecten op het gebied van

weerbaarheid, bewustwording en bestuurlijk instrumentarium. Daarnaast werken een tweetal gemeenten aan het onderdeel informatieveiligheid. De politie en het Openbaar Ministerie richten zich met name op de beeldvorming en de informatievoorziening, bijvoorbeeld op het gebied van slachtofferschap en wat de omvang van cybercrime in de regio IJsselland is. Tot slot is de Veiligheidsregio IJsselland betrokken vanuit hun rol in het crisisdomein, zij zijn betrokken op het onderdeel 'continuïteit' binnen de werkgroep.

Tot slot richt het Expertteam Cybercrime Twente van het Platform Integrale Veiligheidszorg (IVZ) zich op de regionale aanpak van cybercrime. De expertgroep richt zich op drie doelen vanuit een centrale werkgroep die maandelijks bij elkaar komen. Binnen de projectgroep bevinden zich werkgroepen die elkaar eveneens maandelijks treffen. Uit de projectomschrijving van het expertteam valt niet af te leiden wie welke taak heeft. Een beleidsadviseur van de gemeente Enschede geeft aan dat het expertteam Cybercrime van het Platform Integrale Veiligheidszorg nog in de kinderschoenen staat.

R16: Dat is eigenlijk nog heel prematuur binnen de samenwerking van het expertteam.

Tussenconclusie

In Oost-Nederland zijn verschillende overleggremia 's waarin cybercrime en/of gedigitaliseerde criminaliteit besproken wordt. Zowel het expertteam van het Veiligheidsnetwerk Oost-Nederland als het expertteam Cybercrime Twente van het Platform Integrale Veiligheidszorg verkeren in een verkennende fase. De taken binnen deze samenwerkingsverbanden zijn tot op heden niet vastgelegd, in tegenstelling tot het de werkgroep van het Regionaal Informatiepunt Integrale Veiligheid. Na het vertrek van de ambtelijk trekker bij het expertteam Cyber het Veiligheidsnetwerk Oost-Nederland bleek onvoldoende bereidheid om een vervolg te geven aan de bijeenkomsten.

5.3.3 Ervaart u dat de andere organisaties voldoende capaciteit hebben voor de uitvoering van deze taken?

Zowel gemeenten als experts geven aan dat de traditionele strafrechtelijke instituties zoals de politie en het Openbaar Ministerie over onvoldoende capaciteit beschikken op het gebied van cybercrime, waardoor zowel de opsporing als de vervolging van verdachten tekortschiet. De meeste zorgen worden geuit over de gebrekkige capaciteit van de politieorganisatie. De politieorganisatie wordt als één van de zwakste schakels binnen de veiligheidsketen gezien. Het OM bevestigt dit beeld, bij zowel de eigen organisatie als de politie.

R5: Nee, OM en politie hebben gewoon gezien het huidige aanbod aan aangiftes, onvoldoende capaciteit om alle zaken op te pakken. Vandaar dat wij selectief moeten zijn en dus ook meer de nadruk willen leggen op preventie om uiteindelijk te voorkomen dat het alleen maar toeneemt, die aangiften.
R6: Het pakken van daders. Het zou mooi zijn als dat kan maar dat… Ik denk dat ze daar veel te weinig capaciteit voor hebben en zij het ook nog niet als prioriteit zien.

Een respondent van de gemeente Neder-Betuwe geeft aan dat slachtoffers van cybercrime serieuzer genomen moeten worden bij het doen van aangifte. Hierdoor ontstaat eveneens een beter beeld van de aard en omvang van de verschillende vormen van cybercrime. Op basis hiervan kan de urgentie van het thema aangetoond worden. Ook Deventer ziet een uitdaging voor de politieorganisatie op het punt van informatievoorziening richting gemeenten.

R3: Als je het bijvoorbeeld hebt over de politie zijn er wel twijfels bij, of: hoe kunnen we dat beeld nu aan de gemeente leveren? Kunnen we die cijfers echt op gemeenteniveau terugbrengen?

Uit een nadere analyse blijkt dat het de hoeveelheid capaciteit niet alleen samenhangt met de hoeveelheid FTE en beschikbare middelen, maar ook met de mate van urgentie en aandacht vanuit de leiding van de politieorganisatie. Het thema cybercrime krijgt volgens meerdere respondenten nog onvoldoende prioriteit bij de politie, waardoor er onvoldoende capaciteit is vrijgemaakt voor dit onderwerp.

R17: Ja, capaciteit en kennis. Ze lopen echt ernstig achter daarin. Dus als we campagnes gaan draaien dan is het echt voor ons een uitdaging en masseren en overhalen om mee te doen, omdat ze de capaciteit en de interesse niet hebben.
R11: Je krijgt bij de politie sowieso amper gehoor. Dat is een ander punt waar een hoop in verbeterd moet worden.

De brancheorganisatie VNO-NCW geeft aan dat ze een gebrek aan capaciteit waarnemen bij alle andere partijen in de samenwerking rondom cybercrime. KBO-PCOB benadrukt dat naast de beperkte capaciteit bij de nationale politie ook het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) kampt met capaciteitsproblemen doordat ze worden gekort op de financiering vanuit het ministerie van Justitie en Veiligheid.

Tussenconclusie
Niet alle organisaties binnen de samenwerking beschikken over voldoende capaciteit. Zowel beleidsadviseurs bij gemeenten als experts ervaren dat de politie over onvoldoende capaciteit beschikt op het thema cybercrime. Niet alleen aan de kant van de opsporing ligt te weinig capaciteit, ook de vervolging van verdachten wordt als een zwakke schakel ervaren. Het Openbaar Ministerie bevestigt dit beeld bij zowel de eigen organisatie als de politie.

5.3.4 Hoe wordt de samenwerking ervaren en welke zaken bemoeilijken de samenwerking?
In deze paragraaf wordt beschreven in hoeverre de samenwerking door de verschillende gemeenten en experts wordt ervaren op basis van het begrip meerwaarde. Daarnaast worden de factoren uitgelicht die de samenwerking bemoeilijken.

Over het algemeen wordt de samenwerking van gemeenten met andere organisaties op het gebied van cybercrime als positief ervaren. Dit geldt niet alleen voor de gemeente Neder-Betuwe waarbij de samenwerking is opgezocht met de politie. Maar ook voor de gemeente Nijmegen waar publiek-privaat is samengewerkt met commerciële partijen.

R2: Dit willen we doen en zijn jullie het daarmee eens? En zien jullie de meerwaarde daarvan? En daar werd mee ingestemd.
R4: Heel positief, alle partijen staan heel erg open. Die willen allemaal iets doen aan fraude in de breedste zin van het woord. Zowel marktpartijen als overheidspartijen.

De gemeente Enschede benadrukt eveneens dat de samenwerking een meerwaarde oplevert. Niet alleen omdat het thema cybercrime nieuw is maar ook vanwege de noodzaak aangezien de bestrijding

van cybercrime vraagt om een gezamenlijke aanpak. Ook VNO-NCW geeft aan dat losse organisaties de aanpak van cybercrime niet kunnen bolwerken. Samenwerken met andere organisaties is volgens VNO-NCW niet alleen nuttig maar ook noodzaak. Zowel gemeenten als experts uit het werkveld geven aan behoefte te hebben aan netwerkcompetenties (Provan & Kenis, 2008).

R16: Ik denk dat als je niet samenwerkt dat je helemaal nergens komt. Dus dat moeten we echt samen doen. Ik ervaar dat wel als prettig, het zijn allemaal mensen die er wel zin in hebben en die er wel van alles voor willen doen. Dus dat is heel positief. Samen bereik je meer op dit thema.
R14: Het is een kwestie van samenwerken van partijen en daar heeft ieder een eigen rol in. Het CCV kan dat niet als er geen geld is en het DTC ook niet, maar ook niet zonder de informatie van brancheorganisaties of de ondernemers zelf van wat er fout gaat.

KBO-PCOB geeft aan dat de samenwerking met andere organisaties een win-win situatie is. Aangezien zij relatief eenvoudig in contact komen met een kwetsbare doelgroep en de seniorenorganisatie informatie komt halen bij andere partijen.

R13: Wij maken daar dankbaar gebruik van. En dat is wederzijds. Omdat wij toch achter de voordeur komen van die kwetsbare senioren.

Samenwerken met andere organisaties is echter ook weerbarstig van aard. De experts merken een aantal punten op die de samenwerking met andere organisaties bemoeilijken. Ook binnen het expertteam Cyber van het Veiligheidsnetwerk Oost-Nederland wordt de samenwerking niet beschouwd als een vanzelfsprekendheid. De deelnemers van het expertteam zijn tot op heden driemaal bij elkaar gekomen. Een respondent geeft aan dat de bijeenkomsten op een te hoog abstractieniveau lagen, waardoor er onvoldoende concrete handelingsperspectieven voor gemeenten uitkwamen. De meerwaarde van samenwerken in het expertteam Cyber dient volgens de respondent echter van beide kanten een win-win situatie te zijn, zodat halen en brengen met elkaar in balans gebracht worden.

R8: *De ene keer geeft je wat en de ander kan je ook nemen. En dat is dan ook praktisch. (…) Het is te weinig nemen. Dat je te weinig terug kon nemen voor je eigen organisatie en dat het te abstract bleef.*

Ontbreken van structurele samenwerking
De gemeente Deventer verkent de mogelijkheden van samenwerkingsverbanden op het gebied van cybercrime. Voor de meeste organisaties is het thema cybercrime een nieuw fenomeen. Gemeenten verkeren in de een verkennende fase als het gaat om het opbouwen van een netwerk. De seniorenorganisatie KBO-PCOB geeft aan dat er geen structurele samenwerking tot stand is gekomen tussen publieke en private partijen. De vertegenwoordiger van KBO-PCOB is voorstander van een gezamenlijk plan van aanpak voor op de langere termijn, waarbij partijen samenwerken vanuit een gemeenschappelijk plan.

R13: Het zou mooi zijn als je dit structureel kan aanpakken zodat je een soort van aanvalsplan kan maken waarin je voor een aantal jaar, of heel lang, gezamenlijk kan optrekken.
R3: Ik ervaar hem tot nu toe als goed. Ik zie wel dat er best wel veel vraagtekens zijn omdat het experimenterend is, van: op welke wijze moeten we dit gaan vormgeven?

De gemeente Deventer zoekt hoe de eigen organisatie met verschillende organisaties structureel kan samenwerken. Ook de pilot 'aanpak digitale criminaliteit' van de gemeente Nijmegen met markt- en telecomproviders laat zien dat samenwerken op het gebied van cybercrime niet structureel van aard is. Inmiddels staat het thema cybercrime in de gemeente Nijmegen zelfs op 'on hold'.

Samenwerken afhankelijk van deelnemers

Samenwerken tussen verschillende organisaties is niet altijd vanzelfsprekend. Zo is de onderlinge samenwerking afhankelijk van de inzet van de desbetreffende personen. Het gaat niet alleen om de juiste partijen bij elkaar om tafel te hebben maar ook om 'goodwill' van deelnemers. Het Regionaal Informatiepunt Integrale Veiligheid benadrukt dat een netwerkorganisatie ook afhankelijk is van de inzet van deelnemers.

R8: En eigenlijk is dat ook de kwetsbaarheid van een netwerk. Dus dat je afhankelijk van elkaar. En als partner ziek is of niet meer komt voor een overleg.

Vooroordelen tussen markt en overheid

Een ander aspect wat de publiek-private samenwerking bemoeilijkt zijn de wederzijdse vooroordelen tussen overheid en marktpartijen. Deze vooroordelen bleken ten grondslag te liggen bij de verkenning tussen publiek-private samenwerking bij de aanpak van digitale criminaliteit in Nijmegen.

R4: Bij de publieke zijde was met name 'hoezo doen jullie er niks aan?' tegen de marktpartijen. En andersom was het 'maar wij kunnen al die informatie leveren, we kunnen nu aanwijzen waar die pakketjes worden bezorgd, waarom houden jullie ze niet aan?'

Ontbreken van een formele structuur

Binnen de samenwerking kan een formele structuur ontbreken. In de samenwerking tussen meerdere organisaties is bijvoorbeeld geen formele leider of regievoerder aangesteld. Hierdoor kan de spreekwoordelijke 'stok achter de deur' ontbreken waardoor deelnemers geen verantwoordelijkheid of besluiten nemen. De expert van het MKB Cybercampus geeft aan dat het in sommige situaties lastig om tot een besluit te komen als geen enkele partij formeel de regie heeft binnen een zelfregulerend netwerk, zonder administratieve entiteit (Provan & Kenis, 2008).

R15: Er is vaak niet echt een formele structuur van zo'n publiek-private samenwerking, dus naar wie luister je dan? (..) Dat zie ik ook bij Apeldoorn IT terug, wie is eigenlijk de baas hier? Dat heb je wel nodig om verder te komen dus. Dat is een lastige.

Ontbreken van structurele financiering

Naast een gebrek aan formele structuur ontbreekt ook de structurele financiering van de samenwerking. Dit geldt bijvoorbeeld voor de MKB Cybercampus en KBO-PCOB waar structurele subsidiering uit blijft. Hierdoor blijven bepaalde projecten liggen en wordt zoveel mogelijk intern binnen de organisatie opgelost met vrijwilligers.

R13: Het is misschien flauw om te beginnen over geld, maar het is wel een belangrijk iets. Dat betekent dat we soms subsidiegelden nodig hebben en die krijgen we niet. Geen structurele subsidie, soms wel projectsubsidies en daar moeten we het van doen.

R15: In welke vorm ga je samenwerken en ook de financiële stroom, los van subsidies.

Tussenconclusie

Zowel gemeenten als experts uit het werkveld geven aan dat samenwerken op het gebied van cybercrime niet alleen maar positieve resultaten oplevert. Geconcludeerd kan worden dat de samenwerking noodzakelijk is om het vraagstuk aan te pakken. De samenwerking wordt als positief ervaren door gemeenten en experts uit het werkveld. Niet alleen overheden zien de meerwaarde in van samenwerken maar ook marktpartijen dragen hun steentje bij aan het verminderen van bedrog en diefstal. Ook zij worstelen met dit vraagstuk en zijn verantwoordelijk voor hun eigen processen. De samenwerking tussen verschillende organisaties blijkt in de praktijk soms weerbarstig te zijn. Zowel gemeenten als experts geven aan dat de samenwerking vaak incidenteel of op projectmatige basis is. Het thema cybercrime vraagt echter ook om een lange termijn aanpak waarbij organisaties weten wat ze aan elkaar hebben en snel contact kunnen leggen. De samenwerking tussen twee of meer partijen is geen vanzelfsprekendheid. Het gaat niet alleen om de juiste partijen aan tafel te krijgen, maar ook om de juiste mensen met voldoende commitment en goodwill te betrekken bij de onderlinge samenwerking. Daarnaast kunnen vooroordelen de onderlinge samenwerking bemoeilijken. Tot slot kampen experts met het ontbreken van structurele financiering en missen een formele structuur binnen de onderlinge samenwerking waardoor besluitenloosheid en een gebrek aan leiderschap op de loer liggen.

5.4 Welke rollen en verantwoordelijkheden hebben de betrokken actoren binnen de veiligheidsketen?

In dit hoofdstuk worden de verschillende organisaties die door de gemeenten en experts zijn benoemd overzichtelijk gemaakt aan de hand van de veiligheidsketen. De respondenten hebben antwoord gegeven op de vraag: welke organisaties zouden volgens u nog meer moeten worden betrokken om inwoners en ondernemers weerbaar te maken tegen bedrog en diefstal? Daarbij moet de veiligheidsketen gezien worden als één geheel. De verschillende schakels moeten niet afzonderlijk van elkaar bekeken worden om zo verkokering en inefficiëntie te voorkomen (Jongejan e.a., 2011). Gezien de hoeveelheid actoren is het overzicht van de actorenanalyse in bijlage 4 inzichtelijk gemaakt.

5.4.1 Proactie

De eerste schakel van de veiligheidsketen betreft proactie. Dit is de schakel waarin structurele oorzaken van bedrog en diefstal worden weggenomen. De respondenten dragen verschillende partijen aan die binnen de eerste schakel een rol hebben of kunnen vervullen. Allereerst wordt er door de respondenten gewezen op de verantwoordelijkheid die eindgebruikers zelf hebben. Inwoners en ondernemers dienen risicobewust te zijn en zelf een inschatting te maken van de gevaren.

R11: Uiteindelijk moeten werknemers en inwoners zich secuur gedragen en bepaalde dingen ook gewoon niet doen. Klaar. En er is niemand die dat voor hen kan wegnemen.
R16: Grote verantwoordelijkheid voor de bedrijven/organisaties zelf. En je moet zelf natuurlijk zorgen dat je weerbaar bent dat is je eigen verantwoordelijkheid. En andere kunnen ondersteunen en faciliteren maar je bent zelf vooral verantwoordelijk.

Naast de eindgebruikers worden de ‘supercontrollers’ door een aantal experts aangedragen, zoals Bol.com en Marktplaats.nl. De respondenten verwachten van de supercontrollers dat zij mogelijke veiligheidsrisico’s uitsluiten en voorkomen dat eindgebruikers kwetsbaar zijn of slachtoffer worden van bedrog en diefstal. Zo werkt het Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO) van de politie samen met Marktplaats.nl om (potentiele) daders te verstoren. Iedereen moet zich op Marktplaats.nl registreren, zowel als koper en als verkoper, waardoor niemand volledig anoniem een dienst of product kan aan- of verkopen.

R18: Dat noemen we dan verstoren. Voorbeelden van verstoren zijn dat je je bij Marktplaats moet aanmelden, je moet lid zijn. Als je daar uit de bocht vliegt, word je eruit gegooid. Mensen kunnen zien hoelang jij al op Marktplaats actief bent.
R17: Maatregelen, dan heb je IT bedrijven die de barrière online kunnen verhogen, en het moeilijker kunnen maken om dat te plegen.

Ook banken spelen een belangrijke rol in deze eerste schakel van de veiligheidsketen. Zij hebben immers tot op zekere hoogte inzicht in de financiële geldstromen en kunnen verdachte transacties opsporen. Deze signalen kunnen aanleiding geven om bankrekeningen nader te onderzoeken en (tijdelijk) te bevriezen voor onderzoek.

R15: En ik denk dat banken daar ook een rol in kunnen spelen. Ook als je kijkt naar het betalingsverkeer, daar hebben banken ook een rol in.

R18: Dus als er gewoon vijf signalen binnenkomen over aan- en verkoopfraude, gaat de bank automatisch contact met jou opnemen en kan het zijn dat ze dan zeggen: we sluiten je bankrekening af en dan heb je geen bankrekening meer bij ons.

De makers van applicaties op mobiele devices dienen eveneens bij te dragen aan het voorkomen van bedrog en diefstal. Bij de applicatieontwikkelaars zal de paradox tussen veiligheid versus gebruikersgemak echter een blijvend vraagstuk zijn. Hoe makkelijker een bepaalde applicatie wordt gemaakt, hoe eenvoudiger het meestal is om slachtoffer te worden. Dit geldt bijvoorbeeld voor het standaard invoeren van tweetrapsverificatie. Deze extra stap gaat ten koste van het gebruikersgemak maar verhoogt de veiligheid. Enerzijds ligt de verantwoordelijkheid bij de gebruiker, zij dienen risicobewust om te gaan met de applicatie. Anderzijds dient de applicatiemaker de app zo te ontwikkelen dat gebruikersgemak in balans is met de veiligheid van de eindgebruiker. Dit kan de appontwikkelaar bijvoorbeeld doen door software updates uit te brengen waarin recente beveiligingslekken zijn gedicht.

R2: Datzelfde geldt voor een WhatsApp of Facebook, als zij zorgen dat de software goed is dat je minder makkelijk gehackt kan worden.
R17: Ik denk ook aan de appbouwers, techbedrijven, marktplaatsen, die kunnen ook barrières opwerpen en maatregelen nemen.

Seniorenorganisatie KBO-PCOB bevestigt het beeld dat veiligheidsmaatregelen over het algemeen niet samengaan met meer gebruikersgemak. De vertegenwoordiger van KBO-PCOB geeft aan dat het nadeel is dat er hoge drempels worden opgeworpen, waardoor sommige doelgroepen die minder digitaal vaardig zijn, afhaken.

Tot slot kan de Autoriteit Consument en Markt (ACM) hosting- en serviceproviders de opdracht geven om bepaalde webshops of websites uit de lucht halen als blijkt dat niet wordt voldaan aan de gestelde wet- en regelgeving.

5.4.2 Preventie

In de preventieve schakel van de veiligheidsketen worden de meeste organisaties of betrokken partijen genoemd. In deze schakel is het van belang dat de partijen maatregelen treffen om incidenten te voorkomen en om bewustwording te creëren bij eindgebruikers. Een aantal gebruikers refereert aan het inmiddels niet meer bestaande communicatiekanaal van Postbus51. Dit overheidskanaal maakte radio en tv campagnespotjes om inwoners te informeren over bepaalde maatschappelijke kwesties of vraagstukken. Die voorlichtende rol hebben is overgedragen aan de lokale overheid. Alle respondenten geven immers aan dat hier een grote rol is weggelegd voor gemeenten om inwoners en ondernemers weerbaar te maken tegen cybercrime. Zij staan dichtbij hun eigen lokale inwoners en ondernemers en vormen een logisch aanspreekpunt.

R7: Gemeenten spelen een sleutelpositie bij het weerbaar maken van inwoners en ondernemers. Denk aan het aanbieden van trajecten en cursussen, zoals het organiseren van cyberconferenties aan ondernemers.
R8: Dat is sowieso preventie. Preventieve maatregelen, bewustwording creëren van bepaalde

criminaliteit. Dat doet de gemeente soms ook bij woninginbraken, gezamenlijk met de politie natuurlijk. Maar ja, ze geven nog heel weinig voorlichting over dat er op je computer kan worden ingebroken.

Zowel gemeenten als experts zien een belangrijke rol weggelegd voor de lokale overheid binnen de preventieschakel. Zij dienen allereerst het thema cybercrime onderdeel te maken van het Integraal Veiligheidsplan (IVP), waarin concrete capaciteit en doelstellingen staan om inwoners en ondernemers bewust te maken van de risico's. Dit kan door middel van adviezen over preventie, voorlichting en het aanbieden van educatie op onderwijsinstellingen. Naast lokale overheden zien gemeenten en experts ook een preventieve rol weggelegd voor de provincie. De provincie kan op regionaal niveau ontwikkelingen op het gebied van cybercrime monitoren en een faciliterende rol vervullen door het verstrekken van subsidie aan bepaalde weerbaarheidsprojecten, zoals het met korting aanbieden van een weerbaarheidsscan door het Cybercentrum voor de Maakindustrie.

R7: Deze bewustwordingsprojecten kunnen vervolgens uitgerold worden naar cruciale sectoren.
R15: Maar ook bewustwording, supporten en randvoorwaarden creëren waardoor partijen zoals wij die bewustwordingacties kunnen doen.

Ook het onderwijs wordt gezien als een belangrijke actor in het weerbaar maken van inwoners. Zo geeft de beleidsadviseur van Renkum aan dat eindgebruikers zelf verantwoordelijk zijn, maar dat deze groep wel gewezen moet worden op zijn verantwoordelijkheden. Dit kan bijvoorbeeld door het op jonge leeftijd bewust maken van de risico's van cybercrime. Ook de politie geeft aan dat het van belang is dat scholen digitaal burgerschap aanbieden, zodat deze kwetsbare doelgroep weerbaar wordt gemaakt voordat ze slachtoffer worden. Scholen zouden volgens de beleidsadviseur van de gemeente Enschede bijvoorbeeld in samenwerking met Bureau Halt een programma kunnen aanbieden aan leerlingen of studenten.

R7: Op scholen wordt wel geleerd dat je bijvoorbeeld je portemonnee bij je moet houden, maar niet hoe je om moet gaan met digitale dreigingen. Het is van belang dat niet alleen de digitale uitdagingen en mogelijkheden uitgemeten worden maar ook juist de kwetsbaarheden.
R18: Mijn grote wens is dat alle jongeren die van school af komen cyberweerbaar zijn. Cyberweerbaar zijn dat ze geen slachtoffer worden, maar ook dat ze geen dader worden.

Bureau Halt heeft lesmateriaal ontwikkeld waarmee basis- en voortgezet onderwijsinstellingen direct aan de slag kunnen met het weerbaar maken van leerlingen. Daarnaast biedt Bureau Halt een informatieblad voor ouders om ook deze doelgroep te betrekken bij het lespakket. In het informatieblad staan tips om kinderen veilig te laten internetten en ook ouders weerbaar te maken (Bureau Halt, z.d.). Ouders hebben immers een voorbeeldfunctie richting kinderen.

De gemeente West-Betuwe, Enschede en de Veiligheidsregio IJsselland zien een taak weggelegd voor de lokale welzijnsorganisaties. Dit geldt bijvoorbeeld voor het sociaal wijkteam en jongerenwerk, zij kunnen in samenwerking met gemeenten voorlichting geven aan jongeren over de mogelijke risico's. Volgens de gemeenten Enschede, Deventer en Renkum moet de preventieve schakel met name ingevuld worden door organisaties die een laag drempel hebben en een logisch aanspreekpunt vormen voor inwoners en ondernemers.

R3: Samen met het jongerenwerk kunnen we nadenken over hoe we dat vorm kunnen geven en het ook daadwerkelijk kunnen uitvoeren.

Bij de ondernemers wijzen de experts ook naar brancheverenigingen zoals VNO-NCW en MKB Nederland. Zij kunnen hun achterban informeren en attenderen op de risico's. Op regionaal niveau is het Platform Veilig Ondernemen (PVO) een partij die nauw betrokken is bij het weerbaar maken van ondernemers in het MKB. Zij kunnen tips en voorlichting geven aan ondernemersverenigingen en lokale bijeenkomsten organiseren.

R14: Dus ja, als ik ergens op zou inzetten dan is het dat soort samenwerkingsverbanden op de regionale niveau. En daar kunnen de PVO's een belangrijke rol inspelen.
R15: Verder kan ik me voorstellen dat je gerichter, denk aan Platform Veilig Ondernemen (PVO), dat je daar verbinding zoekt met andere platforms en programma's ontwikkelt voor ondernemers.

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) wordt eveneens genoemd door een aantal experts, zoals de gemeente Nijmegen, West-Betuwe en VNO-NCW. Zij zijn van mening dat het CCV zowel inwoners als ondernemers kan waarschuwen voor de gevaren van bedrog en diefstal. Een expert van VNO-NCW laat weten dat het CCV voor informatievoorziening en toolkits kan zorgen. Daarnaast kan het CCV subsidie verstrekken, campagnemateriaal ter beschikking stellen en best-practices uitlichten.

R3: Kijk, het CCV zie ik vooral als dat zij ons moeten voorzien van voorbeelden elders in het land: het is het delen van best practices. Zij gaan ook over het delen van subsidies, het zijn hele praktische producten die ze subsidiëren.
R6: Gemeenten die voorop lopen kunnen anderen helpen daarbij. Dus goede voorbeelden maar ook trainingen, dat zou ook kunnen.

Een beleidsadviseur van Nijmegen verwacht dit ook tot op zekere hoogte van de Vereniging Nederlandse Gemeenten (VNG). Ook zij dienen gemeenten op de gevaren te wijzen die de eigen organisatie loopt, maar ook om inwoners en ondernemers weerbaar te maken tegen cybercrime. Dit kan de VNG eveneens doen door het delen van kennis en het uitwisselen van 'best-practices' en 'lessons learned'.
Deze rol is volgens een respondent bij de gemeente Deventer ook op regionaal niveau weggelegd voor het Veiligheidsnetwerk Oost-Nederland. Deze organisatie kan partijen met elkaar verbinden en kennis en expertise uitwisselen waar dat nodig is om de krachten te bundelen. Het Veiligheidsnetwerk Oost-Nederland biedt volgens de respondenten een platform voor gemeenten en andere veiligheidspartners waar andere gemeenten in Oost-Nederland informatie kunnen halen.

R3: Ik zie het vooral als een verbinder, dus dat we het van elkaar kunnen leren. Kijk, jullie zouden inzicht kunnen hebben in wat ze in Apeldoorn, Ede, Arnhem en Enschede doen en die lijntjes moet je aan elkaar verbinden, want wij zitten niet dagelijks samen.
R4: Het Veiligheidsnetwerk heeft ook een rol daarin om kennis delen, samen te werken en lopende zaken te belichten.

R9: Ja, die zou heel goed gemeenten kunnen faciliteren met materialen voor zo'n avond een verhaal. Vooral die achterkant goed op orde hebben. (…) En misschien ook wel voorbeelden kunnen uitwisselen zoals best practices. Dat zou goed kunnen zijn, zodat ze gemeenten ontzorgen.

Ook de politie wordt als actor aangedragen om in de preventieve sfeer tips en voorlichting te geven, zodat inwoners en ondernemers geen slachtoffer worden van bedrog en diefstal. Een expert van de Expertisecentrum Cybercrime en Digitaal Opsporen (CCDO) geeft in het interview aan dat de politie ook inzet op de preventieve schakel door middel van voorlichting. Zo kunnen wijk- en jeugdagenten helpen bij de voorlichting van verschillende kwetsbare doelgroepen.

R3: Ja, de politie denkt ook met ons mee, de wijkagenten en jeugdagenten zijn wel bereid om voor de klas te gaan staan. Dat hebben ze nog niet gedaan, maar dat spreken ze al wel aan: op die manier hebben ze niet het voortouw, maar trekken ze wel samen met ons op.
R6: Een stukje communicatie ook wel met de wijkagent, die dan een berichtje stuurt of toch in de wijk aanwezig is.

Belangenverenigingen hebben eveneens een taak in de preventieve schakel van de veiligheidsketen, zoals de Consumentenbond, ouderenbonden, werknemers- en ondernemersverenigingen. Zo geeft KBO-PCOB aan dat ouderenorganisaties de achterban moeten informeren over de gevaren van cybercrime. Dit doet de KBO-PCOB door tabletcoaches in te zetten die ouderen preventief wijzen op de risico's en digitale vaardigheden aanleren. De Kamer van Koophandel dient zich eveneens in te zetten voor het weerbaar maken van ondernemers die zich inschrijven bij het handelsregister. Ook zij zouden ondernemers kunnen wijzen op de risico's van bedrog en diefstal wanneer de ondernemers hun bedrijf inschrijven.

R17: De Kamer van Koophandel heeft daar een rol in. Die hangt nog achterover. Dat is zonde.
R1: Ik denk dat een Kamer van Koophandel daar een voorlichtende en begeleidende rol in zou hebben richting bedrijven.

Naar aanleiding van de publiek-private samenwerking op het gebied van digitale veiligheid noemt de beleidsadviseur van Nijmegen een aantal online platforms. De eerste is de website: veiliginternetten.nl. Deze website biedt tips, tricks en praktische uitleg voor burgers en ondernemers om veilig te internetten. Ook de website alertonline.nl helpt burgers, ondernemers en organisaties met het vergroten van het risicobewustzijn. Alert Online is in 2012 ontstaan op initiatief van de Nationaal Coördinator Terrorismebestrijding en Veiligheid en wordt gecoördineerd door het Platform voor de InformatieSamenleving. Het platform richt zich op het uitwisselen van communicatiemiddelen die gericht zijn op bewustwording tot het organiseren van online en offline bijeenkomsten (Alert.nl, 2020). Tot slot worden de Fraudehelpdesk en de Fraudeinfodesk nog in de preventieve schakel ingedeeld. Deze partijen moeten slachtofferschap onder burgers en bedrijven voorkomen door praktische tips te geven over de risico's die zij lopen.

5.4.3 Preparatie

In deze schakel van de veiligheidsketen gaat dat aandacht met name naar de voorbereiding op rampen en crisissen om zo de omvang van de gevolgen te beperken. Dit kunnen organisaties doen door het

opstellen van rampenplannen, het oefenen van een ramp of crisissituatie en het trainen van (lokale) bestuurders. De Veiligheidsregio wordt door een aantal respondenten ingedeeld in de preparatie schakel van de veiligheidsketen. Dit geldt echter alleen voor vormen van bedrog en diefstal die binnen de vitale sector kunnen leiden tot maatschappelijke effecten. De Veiligheidsregio kan hierbij een rol spelen in het gezamenlijk trainen en oefenen van cyberscenario's waarin de vitale infrastructuur wordt geraakt. Zo heeft de Veiligheidsregio Fryslân in samenwerking met de gemeente Leeuwarden, MKB Cybercampus, politie en commerciële partijen zoals Vodafone en Ziggo een cybercrisisoefening georganiseerd, waarbij een hack was gepleegd waardoor gevoelige informatie is buitgemaakt (CCV, 2020).

R15: In die GRIP structuur heeft cyber nog niet echt een plek gekregen. Hoe moet je nou met cyber omgaan in het geval van een cybercrisis? Dat is nog heel erg de vraag. Daarom moet je gewoon gaan oefenen en kijken wat er gebeurt.
R17: Wat doe je als wel gehackt wordt? En hoe beperk je die schade? Je zal vooral vooruit moeten denken, scenario denken.

Ook de VeiligheidsAlliantie Rotterdam werkt samen met de Veiligheidsregio Rotterdam-Rijnmond om cybercrisis oefeningen op touw te zetten. Daarnaast voorziet de VeiligheidsAlliantie Rotterdam dat cyber een vast onderdeel moet zijn van het Opleiding Trainen en Oefenen (OTO) programma van de Veiligheidsregio.

R17: En om eens goed inzichtelijk te maken wat de gevolgen kunnen zijn. Dus de veiligheidsregio is wel een goede partner voor ons. Ja, het brongebied is de computer maar het effectgebied is gewoon vele malen groter, daar krijgen zij wel last van.

5.4.4 Repressie

Zowel gemeenten als experts geven aan dat met name eindgebruikers zelf een cruciale rol spelen op het moment dat een incident zich voordoet. Dit hangt samen met de verantwoordelijkheid die eindgebruikers hebben voor hun eigen handelen. Inwoners en ondernemers dienen immers zelf weerbaar te zijn met het nemen van basismaatregelen, zoals het instellen van een back-up en het installeren van antivirus software.

R4: Het blijft een eigen verantwoordelijkheid als MKB'er maar er is zoveel eigen verantwoordelijkheid voor MKB dat wat hulp daarin zou kunnen helpen.
R10: Als jezelf die kennis hebt, dan jezelf. Maar als je het hebt over de gemiddelde ondernemers dan zit je toch echt bij de cybersecurity professionals.

VNO-NCW geeft echter aan dat de verantwoordelijkheid tot bepaalde grenzen reikt. In de repressieschakel gaat het ook om het beëindigen van het incident en het werkelijk oppakken van daders. Het beëindigen van het incident wordt echter niet door alle respondenten gezien als een prominente rol voor de politie in tegenstelling tot het oppakken van daders.

R9: Die taak van de politie zit hem er aan de ene kant in het opsporen. En dus het voorkomen. Maar

ook als er wat gebeurt om dat effectief in te grijpen en dan zit dat dus op de diefstal. Dus opsporen en onschadelijk maken, zeg maar.

De taak om een einde te maken aan een incident is niet alleen weggelegd voor de politie. Het Cybercentrum voor de Maakindustrie wijst bijvoorbeeld naar cybersecurity professionals in het algemeen, zowel publiek als privaat. Ook experts van de gemeente Renkum en het MKB Cybercampus zien niet alleen een rol weggelegd voor het Team High Tech Crime (THTC) van de politie maar met name voor 'partijen die daar verstand van hebben', waaronder een aantal commerciële organisaties. Binnen de gemeente zou dat de taak moeten zijn van een Chief Information Officier (CISO).

R11: Dat zijn Defensie, FOX IT, Nortwave, Hoffman. Er zijn er maar een paar die dat kunnen.
R15: Tegelijkertijd zie je ook partijen die steeds meer een cyberpech hulpdienst faciliteren, als het dan toch misgaat dan komen ze met gillende banden aangereden en gaan je helpen.
R17: Ja, bij gemeenten de CISO als het intern is en bij bedrijven een soortgelijk iemand neem ik aan.

Commerciële partijen zijn volgens de beleidsadviseur van de gemeente Renkum logischer op het moment dat bijvoorbeeld de data van inwoners en ondernemers niet beveiligd zijn. Waardoor er volgens de respondent geen of in beperkte mate sprake is van strafbare feiten. De respondent geeft aan dat wanneer een persoon de deur openzet er ook geen sprake is van inbraak.

R11: Kijk als je helemaal niks aan preventie doet, als je de data los laat slingeren en het misschien niet ziet en iemand die er verstand van heeft wel en daar amper iets voor hoeft te doen zeg maar. Dan is het wel heel ingewikkeld omdat allemaal bij de politie neer te leggen.

Banken hebben binnen de repressieve schakel eveneens een belangrijke taak. Deze actor is relevant op het moment dat er geld door criminelen afhandig wordt gemaakt maar dit geldt niet voor alle vormen van bedrog en diefstal. Een aantal beleidsadviseurs van gemeenten zijn in de veronderstelling dat banken ook geld kunnen terugstorten wanneer iemand is opgelicht. De geleden schade kan echter niet gestorneerd worden.

R1: Want ja, als je bankaccount geplunderd is dan denk ik dat je eigen bank benadert. Het aanspreekpunt is daar waar jij denkt dat je je geld kunt terughalen met de grootste kans.
R13: De banken zijn natuurlijk wel een belangrijke partij. Juist ook omdat zij het betalingsverkeer ook in de gaten kunnen houden met verdachte transacties die kunnen ze traceren.

De politie geeft aan dat banken en digitale platformen zoals Marktplaats.nl een cruciale rol spelen in het verstoren van de dader(s). Zij kunnen namelijk digitaal ingrijpen voor zover dat mogelijk is en de schade beperken. Een digitaal platform waar goederen worden gekocht kan een bepaalde account volledig afsluiten of tijdelijk bevriezen. Dit geldt tot op zekere hoogte ook voor banken. Zij kunnen rekeningen van zowel daders als slachtoffers blokkeren.

R18: Een bank kan niet iemand veroordelen tot een straf, maar die kan wel bijvoorbeeld zeggen: we sluiten je bankrekening af. Of je mag geen gebruik meer maken van dingen, accounts sluiten bijvoorbeeld, van Marktplaats of wat dan ook.

5.4.5 Nazorg

In de laatste schakel worden maatregelen genomen om terug te keren naar de normale situatie. Een cyberincident op het gebied van bedrog en diefstal kan leiden tot verschillende vormen van schade bij inwoners en ondernemers. Het onderdeel bedrog en diefstal betreft een breed scala aan verschillende vormen van criminaliteit. De impact van deze vormen kan daarin tevens per persoon of organisatie verschillen. Allereerst kan bedrog en diefstal leiden tot financiële schade die daders afhandig maken bij de slachtoffers. Een expert van het Openbaar Ministerie geeft aan dat zij een belangrijke rol vervullen in de vervolging van verdachten en het veroordelen van daders. Daarnaast kan het OM zorgen voor een zekere genoegdoening bij de slachtoffers door het opleggen van een strafbeschikking.

R5: En wij proberen natuurlijk via die rechtszaak, de verdachte veroordeeld te krijgen. Met eventuele financiële compensaties. Ja dat zou je onder nazorg kunnen zien, valt ook een beetje onder repressie.

Ook banken worden door diverse respondenten genoemd als relevante actor waar slachtoffers de schade kunnen verhalen. Mocht de bank de financiële schade niet vergoeden dan is het volgens KBO-PCOB logisch dat de bank ervoor zorgt dat slachtoffers niet nogmaals in dezelfde vorm van bedrog en diefstal trappen. Ook de ouderenbond ziet hier een taak voor de eigen organisatie weggelegd. Ouderen kunnen bellen naar een tiplijn van KBO-PCOB, waarbij de telefoniste kan doorverwijzen naar de juiste instanties, zoals de fraudehelpdesk.

R13: Als de bank alleen zegt: je bent erin geluisd en het is uw eigen verantwoordelijkheid, dan kan ik me voorstellen dat je ook probeert te voorkomen dat het de volgende keer nog een keer gebeurt, als iemand er al iets van geleerd heeft.

Volgens de brancheorganisatie VNO-CNW kunnen ondernemers in het MKB voor de nazorg terecht bij het bedrijf waar de ondernemer een contract mee heeft. Mocht een ondernemer niet kunnen terugvallen op een IT-organisatie dan kan de ondernemer in principe nergens terecht, tenzij deze doelgroep grote commerciële bedrijven inschakelen tegen een hoge prijs. Ook het MKB Cybercampus geeft aan dat zowel inwoners als ondernemers in principe nergens terecht kunnen op het moment dat het echt mis gaat.

R14: De verantwoordelijkheid zou moeten worden opgepakt door het bedrijf waar jij een contract mee hebt. Want als je dat niet hebt dan heb je zelf een probleem. (…) Maar verder is er geen nazorg of een nummer wat je kan bellen. En als je dan ergens probeert aan te kloppen, dan betaal je natuurlijk de hoofdprijs.
R15: Ook voor burgers en ondernemers is er geen pechhulp. In blinde paniek belt iedereen FOX IT op of Orion. Die jongens komen niet voor niets.

Inwoners en ondernemers kunnen, mits zij beschikken over de juiste polisvoorwaarden of verzekerd zijn bij een aantal specifieke verzekeraars, de schade verhalen op de verzekering. Zo kunnen eindgebruikers zich beter indekken op het moment dat een incident heeft plaatsgevonden. Naast de financiële schade kan bedrog en diefstal impact hebben op de mentale gesteldheid van inwoners en ondernemers. Een expert van de gemeente Renkum geeft aan dat de impact van identiteitsfraude zeer ingrijpend kan zijn voor het slachtoffer. Het desbetreffende slachtoffer is vanwege identiteitsfraude

twee maal opgepakt voor hennepteelt in huis zonder dat diegene daar iets van wist. In dat soort schrijnende gevallen kan Slachtofferhulp Nederland een luisterend oor bieden.

R11: Op basis van zijn gestolen identiteit is dat gedaan. Die heeft zeg maar wel iets te verwerken.

Mocht er een onderzoek plaatsvinden na afloop van een ramp of incident dan is de Veiligheidsregio de aangewezen partij die onderzoek doet naar het incident en de 'case' naderhand evalueert.

R17: Dan ligt daar een rol voor de veiligheidsregio om dat te evalueren. Wat de leerpunten zijn en hoe dit voorkomen kan worden of hoe de schade beperkt kan blijven.

Inwoners en ondernemers dienen echter wel gestimuleerd te worden om slachtofferschap te melden. Dit kunnen zij doen door aangifte te doen bij de politie. De gemeente kan hier in samenwerking met de politie een aanjagende functie in hebben. Zonder deze aangifte is het voor de politie niet of beperkt mogelijk een beeld te krijgen van de aard en omvang van cybercrime.

Ook aan de daderkant ligt volgens een aantal gemeenten en experts een taak voor Bureau Halt om jonge daders en '*first offenders'* weer op de rails te krijgen. Bureau Halt werkt met jongeren tussen de 12 en 23 jaar aan een alternatief of aanvullend straftraject, genaamd: Hack_Right. Dit project is bedoelt om recidive te voorkomen en het talent van jonge daders verder te ontwikkelen binnen de kaders van wet- en regelgeving (Halt, 2018). Het traject bestaat uit vier modules, waarin herstel, training, coaching en alternatieve mogelijkheden worden uitgelicht. Tot slot heeft de politie in samenwerking met het Openbaar Ministerie de taak om potentiele daders af te schrikken, door verdachten op te sporen en te berechten. Ook hiervan kan worden gesteld dat dit andere personen weerhoudt om het criminele pad op te gaan.

Tussenconclusie

Inwoners en ondernemers zijn zelf verantwoordelijk voor hun offline en online handelingen. Zij dienen zelf bewust om te gaan met risico's en maatregelen te nemen tegen bedrog en diefstal. De beste antivirus is tenslotte een risicobewuste en zelfbeschermende eindgebruiker. Dit betekend echter niet dat betrokken organisaties geen taak hebben of een rol kunnen vervullen. Zo hebben supercontrollers, appontwikkelaars en hosting- en serviceproviders de taak om software updates beschikbaar te stellen en criminele webwinkels te sluiten. De gemeente in samenwerking met politie en lokale partners de taak om eindgebruikers weerbaar te maken. Op landelijk niveau dienen brancheorganisaties, belangenverenigingen, webwinkels, maar ook verzekeraars en banken hun klanten en leden te wijzen op de risico's van bedrog en diefstal. De Veiligheidsregio is in samenwerking met de betrokken (veiligheids)partners verantwoordelijk voor de voorbereiding op een ramp of crisis in het cyberdomein, waarbij de vitale infrastructuur wordt geraakt en de maatschappelijke effecten groot zijn. Ook in het cyberdomein blijft de politie samen met het Openbaar Ministerie verantwoordelijk voor de opsporing en vervolging van daders. Daarnaast kunnen commerciële diensten de getroffen organisatie of eindgebruikers helpen om de situatie te beëindigen op het moment dat een incident zich voordoet. Tot slot dienen banken, verzekeraars, maar ook Slachtofferhulp Nederland en de Fraudeinfodesk slachtoffers helpen om herhaling te voorkomen.

5.5 Welke kansen/verbeteringen zien gemeenten en experts om de weerbaarheid van inwoners te vergroten?

Agendeer en prioriteer cybercrime op lokaal, regionaal en nationaal niveau
Allereerst is het volgens de gemeente Enschede en meerdere experts van belang het onderwerp cybercrime op de politieke agenda te zetten en te houden. Op het moment dat het thema wordt vastgesteld als prioriteit dan is de verwachting dat er ook meer aandacht en capaciteit beschikbaar voor is. Eindgebruikers komen veelal pas in actie wanneer ze al slachtoffer zijn. Om dit te voorkomen is het van belang om het thema als gemeente en politie te agenderen. Dit kan mogelijk gemaakt worden door inwoners en ondernemers die slachtoffer zijn geworden uit te lichten. Zij kunnen volgens de beleidsadviseur het beste het maatschappelijk belang aantonen en het onderwerp cybercrime op de kaart zetten. De gemeente kan dit proces stimuleren en eventueel faciliteren.

R16: Het belangrijkste en dat wordt denk ik vaak vergeten, dat is om urgentie te creëren. Mensen te laten zien dat het heel dichtbij is en iedereen kan overkomen.

Deze kans is tweeledig, enerzijds is het van belang dat organisaties intern gericht zijn op hun eigen bedrijfsvoering en welke risico's de eigen organisatie loopt, zodat zij maatregelen kunnen treffen. Anderzijds is het van belang om het ook extern uit te dragen, omdat het van publiek belang is om hiermee aan de slag te gaan. Als een organisaties wordt gehackt dan zijn de consequenties ook merkbaar voor de leden, klanten en werknemers van een organisatie. Zo kunnen privégegevens bijvoorbeeld in handen vallen van criminelen.

R7: We zitten nu nog in de verkennende fase. De urgentie is er, alleen door onwetendheid of onverschilligheid kan het op de plank blijven liggen.
R18: Als je het hebt over cybercrime of over dit soort criminaliteit, dan zie je heel vaak dat de gemeente denkt: daar heb ik niks mee te maken. Ook omdat ze het helemaal niet zien, en ook een beetje het nadeel van hoe aangiftes worden opgenomen.

Luister naar behoeften en stem de communicatie af op de doelgroepen
In de communicatie tussen organisaties of richting inwoners en ondernemers is het belangrijk om goed te luisteren naar de behoeften van de doelgroep. Het Cybercentrum voor de Maakindustrie, RCIV, KBO-PCOB en VNO-NCW geven vanuit verschillende achtergronden het belang aan van gerichte communicatie naar specifieke doelgroepen. Daarnaast maken organisaties de communicatie volgens het Cybercentrum voor de Maakindustrie richting inwoners en ondernemers vaak moeilijker dan nodig is. Het is voor deze organisaties juist van belang om het onderwerp cybercrime juist simpel en overzichtelijk te houden. Een aantal experts refereert aan een aantal oude campagnes waarbij de communicatie gericht was op een 'one size fits all' strategie.

R14: En anders kan je kletsen als brugman, maar dan komt het echt niet binnen. Economische Zaken heeft in het verleden, toen ze daar nog iets aan deden, hebben ze miljoenen in het water gegooid, omdat ze dat niet deden.
R10: Spreek de taal van een ondernemer en de taal van de burger. En dat maakt het meteen ook heel

ingewikkeld. Want iedereen is daarin weer anders. En iedereen heeft een ander volwassenheidsniveau. En maak het heel simpel. We zijn allemaal in staat om het heel ingewikkeld te maken.

Zoek de verbinding met andere organisaties op

Een andere ergernis van Saxion, VNO-NCW en het Regionaal Coördinatiepunt Integrale Veiligheid (RCIV) is de verkokering binnen de overheidsorganisaties. Burgers en ondernemers worden op dit moment vanuit verschillende invalshoeken geïnformeerd door langs elkaar heen werkende overheidsorganisaties. De experts geven aan dat het van belang is om inwoners en ondernemers vanuit één overheid te communiceren. De beleidsadviseur van Deventer geeft aan dat het van belang is dat er één centrale organisatie wordt aangewezen om eindgebruikers te informeren en slachtoffers wegwijs te maken.

R1: Maar al die partijen zouden eenzelfde, een up-to-date zijnde bewustwordingsstrategie moeten hebben. Het moet niet zo zijn dat de politie A zegt en de Veiligheidsregio B en de bank C. Dat zou een menukaart moeten zijn die voor iedereen gelijk is.
R14: Ik vind ook dat daar ook meer één overheid de rol zou moeten pakken. Want het zijn natuurlijk nu allemaal departementen die gescheiden zijn door hele hoge muren, ook al zitten ze vlak bij elkaar.

Maak inwoners en ondernemers weerbaar in samenwerking met onderwijsinstellingen

De beleidsadviseurs van de gemeente Renkum en van de MKB Cybercampus geven aan dat er een belangrijke rol is weggelegd voor het onderwijs. Inwoners zijn zelf verantwoordelijk voor hun eigen cyberweerbaarheid, maar gemeenten moeten inwoners wel op die verantwoordelijkheid wijzen, daarnaast moeten inwoners daar ook op onderwezen worden volgens de respondent. Dit geldt niet alleen voor het cyberweerbaar maken van leerlingen of studenten maar ook voor de betrokken ouders. De expert van het MKB Campus ziet daarnaast mogelijkheden voor studenten om burgers te helpen met vragen over hun online veiligheid en cybersecurity.

R15: Dat heb ik ook voorgesteld in Apeldoorn, om studenten achter een telefoon te zetten en als je iets hebt met internet, je vertrouwt het niet. Dan kun je die mensen bellen en die kijken of ze wat informatie kunnen vinden. En dat is een voorbeeld van hoe je collectieve zoekkracht veel gerichter kunt inzetten.

Verzamel best-practices

De gemeenten Winterswijk en West-Betuwe geven aan dat het van belang is om succesvolle interventies, communicatie en instrumentarium samen te brengen, zodat gemeenten weten wat de mogelijkheden zijn op het gebied van cybercrime. De gemeente West-Betuwe geeft aan dat het Centrum voor Criminaliteitspreventie en het Veiligheidsnetwerk Oost-Nederland hierin een faciliterende rol kunnen spelen.

R6: Ik denk dat we als partners de goede ideeën samenbrengen om ook voor cyber een apothekerskast te ontwikkelen zodat we in ieder geval de belangrijkste partners, politie, openbaar ministerie en gemeenten er klaar voor zijn.

Leg taken en verantwoordelijkheden van organisaties vast

Het RCIV, Saxion en de Veiligheidsregio IJsselland geven het belang aan van het vastleggen van verantwoordelijkheden. Op dit moment is het in meerdere schakels van de veiligheidsketen

onduidelijk wie welke verantwoordelijkheden heeft als het gaat om cybercrime. Een expert van Saxion benadrukt dat bedrijven en organisaties en overheden ook een ethische verantwoordelijkheid hebben als het gaat om privé gegevens van eindgebruikers. Organisaties dienen gewezen te worden op hun verantwoordelijkheden en daar zorg voor te dragen.

Ga doelgericht aan de slag met cyberweerbaarheid

De politie en het RCIV geven aan dat het onderwerp cybercrime vaak als lastig en complex wordt ervaren, waardoor de ene gemeente het onderwerp wel oppakt en de ander niet. Het thema heeft al snel de neiging te verzanden in een academische of semantische discussie over wat het precies is. Volgens het RCIV is het van belang om doelgericht aan de slag te gaan om inwoners en ondernemers bewust te maken van de risico's. Bij gemeenten is met name behoefte aan praktische handvaten. Het is daarom van belang om doelgericht aan de slag te gaan op basis van 'trial en error'. Als een bepaalde interventie niet werkt dat moet de interventie bijgesteld worden en opnieuw getest worden. Hierdoor gaan organisaties praktisch en doelgericht aan de slag met het thema cybercrime.

R8: De materie is complex, want het is digitaal. Daar begrijpen we maar heel weinig van. De definitie is heel complex. Dan heb je nog de problematiek dat de partners dat anders beleven en registreren, zoals een politie. Er is bijna geen informatie beschikbaar en niet altijd even goed of betrouwbaar. Maar we zien het wel als een probleem, dus we moeten er wel wat mee. Maar de context is wel super vaag.

Deel verhalen over slachtofferschap

Twee respondenten geven aan dat het van belang is dat slachtoffers van cybercrime een stap naar voren doen. Eindgebruikers schamen zich veelal als ze slachtoffer worden van cybercrime. Ondanks die schaamte is het van belang dat slachtoffer zich durven uit te spreken over wat hen overkomen is. Door het verhaal te delen met omgeving kan daar een preventieve werking vanuit gaan. De gemeente heeft hierbij een faciliterende en stimulerende functie om verhalen over slachtofferschap te delen.

R13: Ik raad iedereen aan om toch zoveel mogelijk de publiciteit te zoeken als je iets is overkomen. De schaamte voorbij zeg maar. Je moet het vooral delen.

Tussenconclusie

Het thema cybercrime dient op lokaal, regionaal en nationaal niveau geagendeerd te worden op de politieke en bestuurlijke agenda's om capaciteit vrij te maken en meer draagvlak te creëren. De focus voor gemeenten ligt enerzijds op de interne processen en het verbeteren van de informatiebeveiliging. Anderzijds dient de gemeente meer inzicht te krijgen in de aard en omvang van cybercrime op lokaal niveau. Op het gebied van communicatie ligt er eveneens een grote uitdaging voor de overheid. Het is van belang om allereerst te luisteren naar de behoeften van kwetsbare doelgroepen en de communicatie hierop af te stemmen. Ook is het van belang dat verschillende organisaties de communicatie richting inwoners en ondernemers op elkaar afstemmen. De kwetsbare doelgroepen dienen vanuit een logische en toegankelijke organisatie benaderd te worden. Op dit moment treden er relatief weinig slachtoffers naar buiten om hun verhaal te doen of anderen te waarschuwen. Deze verhalen zijn echter onmisbaar in de preventieve aanpak van cybercrime. Door slachtofferschap te delen kan de urgentie van het maatschappelijk probleem extra benadrukt worden. Daarnaast is er een belangrijke rol weggelegd voor het onderwijs om eindgebruikers cyberweerbaar te maken. De preventieve aanpak van cybercrime is voor gemeenten een complexe uitdaging. Kleinere gemeenten

voelen de behoefte om doelgericht aan de slag te gaan met praktische handvaten. Zij zijn vanwege capaciteitsgebrek op zoek naar een kant-en-klaar instrumentarium. Grotere gemeente zoals Deventer en Zwolle hebben meer capaciteit en willen het vraagstuk ook op langer termijn borgen. Ongeacht de grootte van de gemeente zijn lokale overheden in het algemeen op zoek naar best-practices.

6. Conclusie, aanbevelingen en reflectie

6. Conclusie, aanbevelingen en reflectie

6.1 Conclusie

Als antwoord op de onderzoeksvraag: '*Welke actoren zijn betrokken bij de aanpak van bedrog en diefstal binnen de cybercrime, welke taken en verantwoordelijkheden hebben deze actoren en in hoeverre verhoudt de samenwerking zich ten aanzien van cybercrime van het Veiligheidsnetwerk Oost-Nederland tot de randvoorwaarden voor succesvolle samenwerking in een governance network?'* met bijbehorende deelvragen kan het volgende geconcludeerd worden.

Het begrip cybercrime laat zich niet eenvoudig definiëren. Het merendeel van de respondenten hanteert een scheiding tussen cybercrime in brede en enge zin. Ondanks deze basale scheiding hebben met name gemeenten meer met het begrip gedigitaliseerde criminaliteit ofwel cybercrime in brede zin. Het Openbaar Ministerie en de politie hanteren een strikte scheiding tussen beide vormen vanwege de juridische basis. Dit in tegenstelling tot organisaties die nauw betrokken zijn bij ondernemers in het midden- en kleinbedrijf, waarbij de focus niet ligt op de cybercrime in brede of enge zin, maar bij de maatschappelijke effecten van deze vormen van criminaliteit voor de onderneming.

Zowel gemeenten als experts geven aan dat ze geen of in zeer beperkte mate zicht hebben op deze vormen van bedrog en diefstal. De meest voorkomende vormen op dit moment zijn: phishing en spoofing. De respondenten geven aan dat spoofing vaak voorkomt in de variant van 'WhatsAppfraude' of 'vriend-in-nood-fraude'. Op de tweede plek staat verkoopfraude, waarbij eindgebruikers worden opgelicht via online webwinkels.

Zowel gemeenten als de experts geven grotendeels identieke redenen aan waarom inwoners en ondernemers kwetsbaar zijn voor bedrog en diefstal. Eindgebruikers beschikken veelal over onvoldoende risicobewustzijn. De risico's worden onvoldoende herkent, veelal vanwege onbewuste onwetendheid. De basismaatregelen worden vaak niet genomen door inwoners en ondernemers, waardoor zij zich onvoldoende kunnen wapenen. De experts geven aan dat de noodzaak om aandacht te besteden aan deze maatregelen veelal ontbreekt.

De gemeente speelt op lokaal niveau een belangrijke rol in het creëren van bewustwording en het cyberweerbaar maken van inwoners en ondernemers. Dit geldt eveneens voor de politie en Openbaar Ministerie, maar ook voor belangenverenigingen en regionale veiligheidsnetwerken. Daarnaast zien gemeenten een taak voor zich weggelegd als het gaat om het nemen van bestuurlijke maatregelen tegen online verstoringen van de openbare orde en veiligheid. De derde taak is gericht op de interne organisatie en betreft het op orde brengen van de eigen informatiebeveiliging. Tot slot dienen gemeenten zicht te krijgen op de aard en omvang van slachtofferschap en daderschap op lokaal niveau. De daadwerkelijke opsporing en vervolging wordt gezien als kerntaak van de traditionele strafrechtelijke instituties. Daarnaast voorzien regionale veiligheidsnetwerken in het inzichtelijk maken van lokale initiatieven, het uitwisselen van kennis en het activeren van gemeenten om met het thema cyber aan de slag te gaan.

De capaciteit van zowel gemeenten als experts uit het werkveld laat een zorgwekkend beeld zien. In de volle breedte is er te weinig tijd, middelen of prioriteit bij gemeenten op het gebied van cybercrime. Het thema cyber vraagt om meer capaciteit dan er op dit moment mogelijk is.

Op lokaal niveau werken een aantal gemeenten samen met lokale partners en de traditionele strafrechtelijke instituties zoals de politie en het Openbaar Ministerie. De samenwerking op dit niveau

is veelal op projectmatige basis en niet structureel van aard. Op regionaal niveau zijn verschillende samenwerkingsverbanden te onderscheiden, waaronder drie regionale veiligheidsnetwerken in Oost-Nederland met een groot aantal deelnemers en gecoördineerd vanuit een administratieve entiteit. In Oost-Nederland zijn verschillende overleggremia 's waarin cybercrime en/of gedigitaliseerde criminaliteit besproken wordt. De taken binnen het Veiligheidsnetwerk Oost-Nederland zijn niet vastgelegd. Na het vertrek van de ambtelijk trekker bij het expertteam Cyber bleek onvoldoende bereidheid om een vervolg te geven aan de periodieke bijeenkomsten.

Zowel beleidsadviseurs bij gemeenten als experts ervaren dat de politie over onvoldoende capaciteit beschikt op het thema cybercrime. Niet alleen aan de kant van de opsporing ligt te weinig capaciteit, ook de vervolging van verdachten wordt als een zwakke schakel ervaren.

Geconcludeerd kan worden dat de samenwerking noodzakelijk is om het vraagstuk aan te pakken. De samenwerking tussen verschillende organisaties blijkt in de praktijk soms weerbarstig te zijn. Zowel gemeenten als experts geven aan dat de samenwerking vaak incidenteel of op projectmatige basis is. Het thema cybercrime vraagt echter ook om een lange termijn aanpak waarbij organisaties weten wat ze aan elkaar hebben en snel contact kunnen leggen. Het gaat niet alleen om de juiste partijen aan tafel te krijgen, maar ook om de juiste mensen met voldoende commitment en goodwill te betrekken bij de onderlinge samenwerking. Daarnaast kunnen vooroordelen de onderlinge samenwerking bemoeilijken. Tot slot kampen experts met het ontbreken van structurele financiering en missen een formele structuur binnen de onderlinge samenwerking waardoor besluitenloosheid en een gebrek aan leiderschap op de loer liggen.

Inwoners en ondernemers zijn zelf verantwoordelijk voor hun offline en online handelingen. Dit betekend echter niet dat betrokken organisaties geen taak hebben of een rol kunnen vervullen. Zo hebben supercontrollers, appontwikkelaars en hosting- en serviceproviders de taak om software updates beschikbaar te stellen en criminele webwinkels te sluiten. De gemeente in samenwerking met politie en lokale partners de taak om eindgebruikers weerbaar te maken. Op landelijk niveau dienen brancheorganisaties, belangenverenigingen, webwinkels, maar ook verzekeraars en banken hun klanten en leden te wijzen op de risico's van bedrog en diefstal. De Veiligheidsregio is in samenwerking met de betrokken (veiligheids)partners verantwoordelijk voor de voorbereiding op een ramp of crisis in het cyberdomein, waarbij de vitale infrastructuur wordt geraakt en de maatschappelijke effecten groot zijn. Ook in het cyberdomein blijft de politie samen met het Openbaar Ministerie verantwoordelijk voor de opsporing en vervolging van daders. Tot slot dienen banken, verzekeraars, maar ook Slachtofferhulp Nederland en de Fraudeinfodesk slachtoffers te helpen om herhaling te voorkomen.

Het thema cybercrime dient op lokaal, regionaal en nationaal niveau geagendeerd te worden op de politieke en bestuurlijke agenda's om capaciteit vrij te maken en meer draagvlak te creëren. Ook door het delen van slachtofferschap kan de urgentie benadrukt worden. De focus voor gemeenten gaat uit naar de informatiebeveiliging, maar ook naar het verkrijgen van inzicht in de aard en omvang van cybercrime op lokaal niveau. Op het gebied van communicatie ligt er eveneens een grote uitdaging voor de overheid. Het onderwijs kan een rol vervullen in het cyberweerbaar maken van eindgebruikers. De preventieve aanpak van cybercrime is voor gemeenten een complexe uitdaging. Kleinere gemeenten voelen de behoefte om doelgericht aan de slag te gaan met praktische handvaten. Grotere gemeente zoals Deventer en Zwolle hebben meer capaciteit en willen het vraagstuk ook op langer termijn borgen. Ongeacht de grootte van de gemeente zijn lokale overheden in het algemeen op zoek naar best-practices.

6.2 Aanbevelingen

Na het theoretische hoofdstuk, resultaten en analyse en conclusie kunnen de volgende aanbevelingen worden geformuleerd:

1. Stimuleer inwoners en ondernemers om verhalen over slachtofferschap te delen, zodat ook anderen gewaarschuwd worden voor de risico's van cybercrime.

2. Maak cybercrime op lokaal niveau onderdeel van het Integraal Veiligheidsplan (IVP) en koppel concrete capaciteit en acties aan het weerbaar maken van inwoners en ondernemers.

3. Maak leerlingen en studenten op onderwijsinstellingen cyberweerbaar door het invoeren van digitaal burgerschap of een digitaal vaardig rijbewijs. Wijs eindgebruikers op hun eigen verantwoordelijkheid.

4. Breng op lokaal niveau de aard en omvang van slachtofferschap en daderschap van cybercrime in kaart. Dit toont niet alleen de urgentie van het probleem aan, maar draagt ook bij aan lokaal maatwerk om concreet aan de slag te gaan met een plan van aanpak.

5. Maak van cyber een vast onderdeel van het Opleiding Trainen en Oefenen (OTO) programma van de Veiligheidsregio. En oefen met elkaar zodat taken en verantwoordelijkheden definitief vast komen te liggen.

6. Investeer in de opsporing en vervolging om verdachten daadwerkelijk op te pakken en te berechten. Ook hiervan gaat een preventieve werking uit richting 'first offenders'.

6.3 Reflectie

Beperkingen van het onderzoek

De praktijk van de bestrijding van de cybercrime loopt achter de feiten aan. Er is gekozen voor een algemene gespreksronde met zowel beleidsadviseurs van gemeenten als experts uit het werkveld. Er is niet gekozen om specifieke vormen bedrog en diefstal nader te onderzoeken. Het beeld dat ontstaat is dat cybercrime slechts bij hoge uitzondering wordt vervolgd. Dat diverse slechtoffers geneigd zijn om te schikken en de gevraagde som over te maken. Deels ook beschroomd omdat ze onveilig gedrag op de digitale snelweg hebben vertoond.

Het onderzoek heeft een sterk beschrijvend karakter gekregen. Dit was onvermijdelijk gelet op het prille niveau waarop de bestrijding van cybercrime zich nog steeds bevindt. Misschien dat in een vervolgonderzoek meer aandacht zou kunnen worden gegeven aan succesvol afgesloten strafzaken waarbij wordt aangegeven hoe het bewijsmateriaal bij elkaar werd gekregen en welke schade deze daders te weeg hebben gebracht.

De theoretische basis van de governance network theorie gaat uit van een samenwerking waarbij organisaties komen tot een concreet uitvoeringsplan. Het expertteam Cyber van het Veiligheidsnetwerk Oost-Nederland is in het verleden echter een beperkt aantal keer bij elkaar gekomen, waarbij er geen concrete resultaten zijn geboekt of concreet is samengewerkt tussen verschillende organisaties. Hierdoor laat de papieren werkelijkheid een ander beeld zien dan de praktijksituatie.

De samenwerking wordt door bijna alle gemeenten en experts als positief ervaren. Wellicht wordt dit antwoord al snel gegeven vanuit de gedachte van een sociaal gewenst antwoord. Anderzijds kan het ook gezien worden als de bereidheid en welwillendheid om onderling samen te werken en om daadwerkelijk iets te doen aan cybercrime.

Een terugkerend thema in mijn onderzoek was de onduidelijkheid over de verantwoordelijkheden van de diverse organisaties. Heeft de burgemeester nu wel een taak bij de zorg voor de digitale openbare orde of niet. Dit is deels een juridische vraag en de kaders rondom wet- en regelgeving in het cyberdomein liggen nog niet definitief vast. Enkele onderzoekers (Bantema, Spithoven, etc.) onderzoeken de mogelijkheden binnen het cyberdomein.

Mogelijkheden voor vervolgonderzoek

Het in kaart brengen van de stand van zaken in de Veiligheidsnetwerk Oost-Nederland was zeer omvangrijk. Het zou goed zijn wanneer in vervolg onderzoek de ervaringen van het veiligheidsnetwerk in Rotterdam wordt vergeleken met die in Oost Nederland. Wellicht dat ook over de grens gekeken zou moeten worden. Met name kan dan worden gedacht aan Vlaanderen waar cybersecurity een thema is dat de nodige aandacht heeft gekregen.

Literatuurlijst

Bantema, W., S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol (2018) *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* Den Haag: Sdu (reeks Politie en Wetenschap).

Banton, M. (1964) The Policeman in the Community. London: Tavistock.

Boeije, H. (2008). *Analyseren in kwalitatief onderzoek*. Denken en doen. Den Haag: Boomonderwijs.

Boerman, F., Grapendaal M., Nieuwenhuis F. & Stoers E. (2017). *Nationaal Dreigingsbeeld georganiseerde criminaliteit 2017*, Politie Nederland. Geraadpleegd op 21 mei 2020, van https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2017/nationaal-dreigingsbeeld-2017.pdf

Bureau Halt (2018). Hack_Right. *Voorkom recidive, ontwikkel talent*. Geraadpleegd op 30 juni 2020.

Bureau Halt (z.d.). *Informatieblad ouders online veiligheid*. Geraadpleegd op 30 juni 2020.

Centraal Bureau voor de Statistiek (CBS). (2017). *Een op vijf bedrijven slachtoffer van cyberaanval*. Geraadpleegd op 20 maart 2020, van https://www.cbs.nl/nl-nl/nieuws/2017/39/een-op-vijf-bedrijven-slachtoffer-van-cyberaanval

Centraal Bureau voor de Statistiek (CBS). (2018a). *1,2 miljoen slachtoffers van digitale criminaliteit* Geraadpleegd op 20 maart 2020, van https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit

Centraal Bureau voor de Statistiek (CBS). (2018b). *Jongvolwassenen vaker verslaafd aan social media.* Geraadpleegd op 20 maart 2020, van https://www.cbs.nl/nl-nl/nieuws/2018/20/jongvolwassenen-vaker-verslaafd-aan-sociale-media

Centraal Bureau voor de Statistiek (CBS). (2019). *Veiligheidsmonitor slachtofferschap criminaliteit.* Geraadpleegd op 20 maart 2020, van https://longreads.cbs.nl/veiligheidsmonitor-2019/slachtofferschap-criminaliteit/

Cuyper, R.H. de & Weijters G. (2016). *Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices.* Memorandum 2016-1. WODC, Den Haag.

Delden, P. J. van, (2009). *Samenwerking in de publieke dienstverlening: ontwikkelingsverloop en resultaten*, Delft: Eburon. Proefschrift Universiteit van Tilburg. Geraadpleegd op 21 mei 2020, van https://pure.uvt.nl/ws/files/1111121/samenwerking_in_de_publieke_dienstverlening_definitief_6_aug.pdf

Digital Trust Center. (2018). *Factsheet Digital Trust Center*. Geraadpleegd op 25 mei 2020, van https://www.digitaltrustcenter.nl/sites/default/files/201912/Factsheet%20Digital%20Trust%20Center.pdf

Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen en W. Ph. Stol (2013). Slachtofferschap in een gedigitaliseerde samenleving, een onderzoek onder burgers naar e-fraude, hacken en ander veel voorkomende criminaliteit. Den Haag: Boom Juridische uitgevers.

Dunn, W.N. (2008). *Public policy analysis: An introduction.* New Jersey: Pearson Prentice Hall.

European Commission. (2016, 6 december). *Cybercrime. Migration and Home Affairs - European Commission.* Geraadpleegd op 15 mei 2020, van https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

Gemeente Nijmegen. (2019). *Pilot aanpak digitale criminaliteit Oost-Nederland. Veiligheidsnetwerk Oost-Nederland.* Geraadpleegd op 10 mei 2020, van https://veiligheidsnetwerkon.nl/go/download/?id=355

Gray, B. (1985). *Conditions Facilitating Interorganizational Collaboration. Human Relations*, 38(10), p. 911-936.

Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. C. (2004). A Behavioral Model of Digital Music Piracy. Journal of Organizational Computing and Electronic Commerce, 14(2), 89–105. https://doi.org/10.1207/s15327744joce1402_01

Grijpink, J.H.A.M. (2003). *Identiteitsfraude als uitdaging voor de rechtsstaat. Privacy en Informatie*, 6, 28-31. Geraadpleegd op 10 juni 2020, van https://docplayer.nl/16170311-Identiteitsfraude-als-uitdaging-voor-de-rechtstaat-1-prof-dr-mr-j-h-a-m-grijpink-2.html

Helsloot, I. (2007). *Voorbij de symboliek: over de noodzaak van een rationeel perspectief op fysiek veiligheidsbeleid.* Den Haag: Boom Juridische uitgevers.

Helsloot, I. en J. Groenendaal (2014). *Naar meer inzicht in de politiële netwerkpraktijk in de casus cybercrime, zeehavens en veiligheidshuizen.* Working paper BSK14-01. Radboud University Nijmegen

Higgins, G. E. (2007). *Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value,* International Journal of Cyber Criminology, 1 (1), 33-55

Holt, T.J., & Bossler, A.M. (2014). *An Assessment of the Current State of Cybercrime Scholarship. Deviant Behavior* 35(1), 20-40.

Hulst, van der R.C. & Neve, R.J.M. (2008). *Hightech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders*. Den Haag: WODC.

Jongejan, R. B., Helsloot, I., Beerens, R. J. J., & Vrijling, J. K. (2011). *How prepared is prepared enough? Disasters,* 35(1), 130–142. https://doi.org/10.1111/j.1467-7717.2010.01196.x

Klijn, E.H. & Koppejan J.F.M. (1994). *Beleidsnetwerken als theoretische benadering: Een tussenbalans.* Beleidswetenschap, 11(2), 143-167.

Klijn, E.H. & Koppenjan, J.F.M. (2016). *Governance network in the public sector.* Geraadpleegd op 1 april 2020, van https://www.researchgate.net/publication/284158898_governance_networks_in_the_public_sector

Leukfeldt, E.R., Domenie, M.M.L. & Stol, W.Ph. (2010). *Verkenning cybercrime in Nederland 2009.* Den Haag: Boom Juridische uitgevers.

Leukfeldt, E.R. & M. Yar (2016). *Applying routine activity theory to cybercrime. A theoretical and empirical analysis.* Deviant Behavior. DOI:10.1080/01639625.2015.1012409.

Madden, M., & Rainie, L. (2015). *Americans' Attitudes About Privacy, Security and Surveillance.* van http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Ministerie van Justitie en Veiligheid. (2019). *TK Voortgang integrale aanpak cybercrime.* Geraadpleegd op 10 juni 2020, van https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/12/tk-voortgang-integrale-aanpak-cybercrime

Ministerie van Justitie en Veiligheid. (2020). Cybercrime bestrijden. Geraadpleegd op 20 maart 2020, van https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/cybercriminaliteit-bestrijden

Moser, A., Kruegel, C., & Kirda, E. (2007). Limits of Static Analysis for Malware Detection. *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, 421–430. https://doi.org/10.1109/acsac.2007.21

Motivaction (2019). *Nationaal Cybersecurity Bewustzijnsonderzoek 2019, Cyberbewustzijn en vaardigheid Nederlandse (beroeps)bevolking*. Amsterdam: Motivaction.

Nationaal Cyber Security Centrum. (2019a). *CSBN 2019: ontwrichting van de maatschappij ligt op de loer*. Geraadpleegd op 20 maart 2020, van https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/nieuws/2019/juni/12/csbn-2019-ontwrichting-ligt-op-de-loer

Nationaal Cyber Security Centrum. (2019b). *Cybersecuritybeeld Nederland 2019*. Geraadpleegd op 20 maart 2020, van https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

Nationaal Cyber Security Centrum (NCSC). (2016). *Cybersecuritybeeld Nederland 2016. Nationaal Cöordinator Terrorismebestrijding en Veiligheid.* Geraadpleegd op 5 juni 2020, van https://www.nctv.nl/binaries/nctv/documenten/publicaties/2016/09/05/cybersecuritybeeld-nederland-2016/CSBN+6-2016+NL.pdf

Nederlands Studiecentrum Criminaliteit en Rechtshandhaving & Erasmus Universiteit. (2020). *Slachtoffer van onlinecriminaliteit, wat nu?* Geraadpleegd op 3 mei 2020, van https://www.politieenwetenschap.nl/cache/files/5f42a7b577f74PW120.pdf

Ngo, F.T., & Paternoster, R. (2011). *Cybercrime Victimization: An examination of Individual and Situational level factors.* International Journal of Cyber Criminology, 5(1), 773.

Stol, W., Tielenburg, C., Rodenhuis, W., (2016). *Basisboek integrale veiligheid.* Den Haag: Boom Criminologie.

Sociaal Cultureel Planbureau (SCP). (2020). *Hoe dachten Nederlanders dat hun leven eruit zou zien in 2020?* Geraadpleegd op 20 maart 2020, van https://www.scp.nl/actueel/nieuws/2019/12/31/hoe-dachten-nederlanders-dat-hun-leven-eruit-zou-zien-in-2020

Smith, J. R., & Louis, W. R. (2008). Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude-behaviour relationship. *British Journal of Social Psychology*, 47(4), 647–666. https://doi.org/10.1348/014466607x269748

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce. Proceedings of the 3rd ACM conference on Electronic Commerce - EC '01, 1–10. https://doi.org/10.1145/501158.501163

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Den Haag: Boom Criminologie.

Politie. (z.d.). *Malware*. politie.nl. Geraadpleegd 20 maart 2020, van https://www.politie.nl/themas/malware.html

Politie. (z.d.) *Stalking.* politie.nl Geraadpleegd op 20 maart 2020, van https://www.politie.nl/themas/Stalking.html

Teeffelen, K. (2020). Universiteit Maastricht over de hack: we konden niet anders dan betalen. Trouw. Geraadpleegd op 21 juli 2020, van https://www.trouw.nl/nieuws/universiteit-maastricht-over-de-hack-we-konden-niet-anders-dan-betalen~bb2f0c13/

Terpstra, J. (2001). Netwerken en samenwerking bij de uitvoering van beleid. Beleidswetenschap, 2(15), 141-168.

Terpstra, J. & R. Kouwenhoven. (2004). *Samenwerking en netwerken in de lokale veiligheidszorg.* Zeist: Kerckebosch (uitgave Commissie Politie en Wetenschap).

Thiel, S. (2010). Bestuurskundig onderzoek (2de editie). Bussum, Nederland: Coutinho.

UNODC. (2013). *Draft Comprehensive Study on Cybercrime.* United Nations Office on Drugs and Crime (UNODC). Geraadpleegd op 2 mei 2020, van

https://www.unodc.org/e4j/data/_university_uni_/draft_comprehensive_study_on_cybercrime.html?lng=en&match=Draft%20Comprehensive%20Study%20on%20Cybercrime

Provan, K., & Kenis, P. (2008). *Modes of Network Governance: Structure, Management, and Effectiveness. Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015

Politie. (z.d.). *Voorschotfraude*. Geraadpleegd op 1 mei 2020, van https://www.politie.nl/themas/voorschotfraude.html

Politie. (2020). *Ondanks grote druk presteerde de politie goed; scherpe keuzes en schouders eronder in 2020*. politie.nl. Geraadpleegd op 15 mei 2020, van https://www.politie.nl/nieuws/2020/januari/8/02-ondanks-grote-druk-presteerde-de-politie-goed-scherpe-keuzes-en-schouders-eronder-in-2020.html

RTV Oost (2020). *'Vriend-in-nood-app-fraude' in Overijssel sinds corona verdrievoudigd.* Geraadpleegd op 26 mei 2020, van https://m.rtvoost.nl/nieuws/330230/Vriend-in-nood-app-fraude-in-Overijssel-sinds-corona-verdrievoudigd

Van Steden, R. (2011). *Sturing van lokale veiligheid: een achtergrondstudie, in: Strategieën van lokale veiligheid, een achtergrondstudie en 3 reflecties,* onder redactie van Van Steden. Amsterdam: Amsterdam University Press.

Van Steden, R., & Boutellier, J. (2010). *Versnipperde regie: de positie van de gemeente in een lokaal veiligheidsnetwerk.* Tijdschrift voor veiligheid, 9(3), 21-33.

Van Der Zee, S. (2018*). Cyber Security Paradox: When knowing what's right does not lead to doing what's right.* In *Security & Human Behavior workshop 2018.* Geraadpleegd op 26 februari 2020, van https://www.lightbluetouchpaper.org/2018/05/24/security-and-human-behavior2018/

Veenstra, R., Lindenberg, S., Oldehinkel, T., de Winter, A., Verhulst, F. C., & Ormel, J. (2005). *Pesten: Over daders, slachtoffers, dader/slachtoffers en niet-betrokken leerlingen.* Kind en Adolescent, 26(3), 305- 317.

Veiligheidsnetwerk Oost-Nederland. (z.d.). *Cybercrime en gedigitaliseerde criminaliteit*. Geraadpleegd op 15 maart 2020, van https://veiligheidsnetwerkon.nl/kennisbank/cybercrime/cybercrime-en-gedigitaliseerde-cr/

Verhagen, H. (2016). *De economische en maatschappelijk noodzaak van meer cybersecurity. Nederland digitaal droge voeten.* Geraadpleegd op 15 maart 2020 van https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf.

Vereniging Nederlandse Gemeenten (VNG). (2018*). Inventarisatie Cyberveiligheid geeft overzicht.* Geraadpleegd op 9 maart, 2020 van https://vng.nl/nieuws/inventarisatie-cyberveiligheid-geeft-overzicht

Vereniging Nederlandse Gemeenten (VNG). (2020). *Agenda Digitale Veiligheid 2020-2024.* Geraadpleegd op 9 maart, 2020, van https://vng.nl/publicaties/agenda-digitale-veiligheid-2020-2024

Wilsem, J. van (2013). *'Bought it, but never got it': Assessing risk factors for online consumer fraud victimization.* European Sociological Review, 29(2), 168-178.

Wetenschappelijke Raad voor Regeringsbeleid (WRR). (2020, 9 maart). *Voorbereiden op digitale ontwrichting*. Geraadpleegd op 25 maart 2020, van https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). (1998). Stalking. *Slachtoffers, daders en maatregelen tegen deze vorm van belagen.* Geraadpleegd op 25 mei 2020, van https://www.wodc.nl/onderzoeksdatabase/w00210-stalking.aspx

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). (2006). *Cybercrime in cijfers*. Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices. Geraadpleegd op 25 mei 2020, van https://www.wodc.nl/binaries/mem2016-1-volledige-tekst_tcm28-74175.pdf

Bijlagen

Bijlage 1: Respondentenlijst

In de onderstaande tabel staan de respondenten van de verschillende organisatie die deel hebben genomen aan het onderzoek. Daarnaast staat de datum en de duur van het gesprek. De interviews zijn genummerd en komen aan de hand daarvan terug in het onderzoek.

Nr.	**Organisatie**	**Datum**	**Duur gesprek**
1	Hogeschool Saxion	26-06-2020	01:25:58
2	Gemeente Neder-Betuwe	30-06-2020	44:12
3	Gemeente Deventer	20-07-2020	45:54
4	Gemeente Nijmegen	01-07-2020	01:31:17
5	Openbaar Ministerie	02-07-2020	34:21
6	Gemeente West-Betuwe	03-07-2020	33:10
7	*Anoniem	20-07-2020	55:06
8	Regionaal Informatiepunt Integrale Veiligheid	21-07-2020	43:25
9	Gemeente Winterswijk	22-07-2020	38:57
10	Cybercentrum voor de Maakindustrie	24-07-2020	48:00
11	Veiligheidsregio IJsselland	29-07-2020	51:55
12	Gemeente Renkum	03-08-2020	49:34
13	Ouderenbond KBO-PCOB	11-08-2020	52:10
14	Ondernemersorganisatie VNO-NCW	30-08-2020	01:24:18
15	MKB Cybercampus	31-08-2020	59:56
16	Gemeente Enschede	21-09-2020	01:03:43
17	VeiligheidsAlliantie Rotterdam	17-09-2020	43:45
18	Politie, Expertisecentrum Cybercrime en Digitaal Opsporen (ECDO)	18-09-2020	01:04:14

* = Organisatie bekend bij scriptant/stagebegeleider

Bijlage 2 : Topiclist

1. Wat verstaat u onder cybercriminaliteit?

→ Neem de definitie van (I) cybercriminaliteit, (II) cyber-enabled crime en (III) diefstal en bedrog door om op een lijn te komen

I. Cybercriminaliteit
Cyber-criminaliteit betreft het gebruiken van het internet of andere computertechnologie ten behoeve van het faciliteren van criminaliteit of ander normoverschrijdend gedrag (Spithoven 2020, op basis van Kleve, De Mulder & Van Noortwijk, 2010; Holt & Bossler, 2013; Leukfeldt, 2016, 2018; Holt, Bossler & Seigfried-Spellar, 2018)**.**

II. Cyber-enabled crime

Onder *cyber-enabled criminaliteit* worden meer klassieke vormen van criminaliteit verstaan, die door middel van ICT op een grotere schaal kunnen worden uitgevoerd (Leukfeldt, 2016, 2018).

III. Diefstal en bedrog

'Het stelen van informatie of het illegaal verkrijgen van voorwerpen van waarde van individuen of organisaties' (Holt en Bossler 2013, p. 25), hieronder vallen bijvoorbeeld:

- verkoopfraude
- betalingsfraude
- identiteitsfraude
- voorschortfraude
- gegevensdiefstal
- gegevensheling
- spoofing
- skimming
- phishing

Deel 1 - Eigen praktijk

1. Welke vormen van 'bedrog en diefstal' als cyber-enabled criminaliteit ziet u vooral in uw praktijk voorbij komen? Welke doelgroepen treffen deze vormen van diefstal en bedrog volgens u vooral?
2. Hoe ontstaat volgens u de gelegenheid voor deze vormen van bedrog en diefstal als cyber-enabled criminaliteit?
3. Wat is uw taak en wat is de taak van uw organisatie in het tegengaan van deze vormen van bedrog en diefstal als cyber-enabled criminaliteit? Indien niet besproken → voert u of uw organisatie op dit moment ook taken uit om inwoners en ondernemers weerbaar te maken tegen diefstal en bedrog?
4. Hoeveel capaciteit is er voor deze taken vrijgemaakt en is dit voldoende volgens u?

Deel 2 - Huidige samenwerking

5. Met welke andere organisaties werkt uw organisatie momenteel samen in het tegengaan van deze vormen van bedrog en diefstal als cyber-enabled criminaliteit?

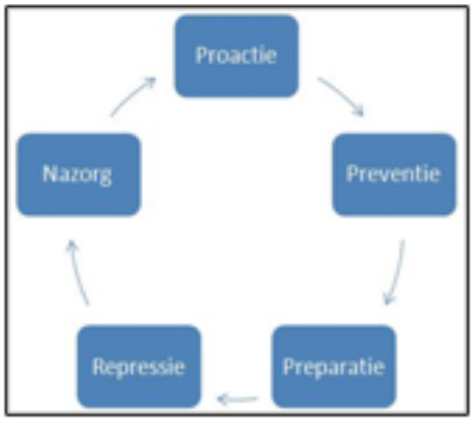
6. Wat zijn ieders taken in deze samenwerking?
7. Ervaart u dat deze andere organisaties voldoende capaciteit hebben voor de uitvoer van deze taken?
8. Hoe ervaart u deze samenwerking? Zijn er zaken die het samenwerken bemoeilijken?

Deel 3 - Naar cyberweerbaarheid

We spreken in de rest van dit interview over cyberweerbaarheid:
De combinatie van risicobewustzijn en zelfbeschermend gedrag onder inwoners en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen (Spithoven, 2020; Misana-ter Huurne et al., 2020):

9. Welke organisaties zouden volgens u nog meer moeten worden betrokken om inwoners en ondernemers weerbaarder te maken tegen *diefstal en bedrog* als cyber-enabled criminaliteit?

10. Bent u bekend met de veiligheidsketen? Voor de zekerheid nemen we de stappen van deze keten kort en bondig door.



Proactie: Wegnemen van structurele oorzaken.
Preventie: Nemen van maatregelen.
Preparatie: Voorbereiden om effectief op te treden als het misgaat.
Repressie: De onveilige situatie beëindigen en schade te beperken
Nazorg: Aandacht besteden aan de schade, deze herstellen en gang van zaken evalueren

11. Wat zou er volgens u idealiter in per fase van de veiligheidsketen om de weerbaarheid van inwoners en ondernemers ten opzichte van diefstal en bedrog als cyber-enabled criminaliteit te vergroten?
12. Welke partijen kennen idealiter welke verantwoordelijkheden per fase?
    ➔ Maak een matrix samen met de respondent!

Deel 4 - Afsluiting

13. Welke kansen/verbeteringen om de weerbaarheid van inwoners en ondernemers tegen diefstal en bedrog als cyber-enabled criminaliteit te vergroten ziet u voor de toekomst?
14. Hebben wij in dit interview nog iets gemist dat u wilt meegeven?

Bijlage 3: Informed consent formulier

SAXION
UNIVERSITY OF APPLIED SCIENCES

Postbus 70.000
7500 KB Enschede

Handelskade 75
7417 DH Deventer

Internet: www.saxion.nl

Academie Bestuur, Recht & Ruimte
Lectoraat Maatschappelijke Veiligheid
Behandeld door:
Dr. Remco Spithoven (lector)
Telefoon direct: 06 - 12618471
E-mail direct:
r.spithoven@saxion.nl

Aan professionals die betrokken zijn bij het onderzoek naar de governance van cybercriminaliteit

Datum 13-05-2020
Pagina 1 van 2
Onderwerp Onderzoek naar rollen en verantwoordelijkheden in de aanpak van cybercrime.

Geachte deelnemers aan de interviews bij het onderzoek 'governance van cybercriminaliteit',

U bent gevraagd om deel te nemen aan een interview bij het onderzoek van de Hogeschool Saxion in samenwerking met het Veiligheidsnetwerk Oost-Nederland en Bureau Regionale Veiligheidsstrategie. Dit interview wordt uitgevoerd door Jelle Kuiper van het Veiligheidsnetwerk Oost-Nederland. Het onderzoek wordt begeleid door lector Remco Spithoven. Het doel van het onderzoek is om in kaart te brengen welke actoren betrokken kunnen worden in de aanpak van cybercrime en welke verantwoordelijkheden zij daarbij hebben.

Het betreft een semigestructureerd interview waarbij veel ruimte is voor eigen invulling van het gesprek. Er zal een geluidsopname van dit interview worden gemaakt. Deze geluidsopname wordt op onderdelen letterlijk uitgewerkt om tot een goede verslaglegging van het interview te komen. Als u wilt kan het verslag van het interview aan u worden nagezonden. In de periode na het dit interview wordt u gecontacteerd om eventueel deel te nemen aan een focus group sessie. Deelname aan dit onderzoek is volledig *vrijwillig*. Alle informatie uit dit interview en de focus group sessie zal *anoniem* worden verwerkt. De geluidsopname en de verslaglegging zijn alleen bestemd voor het onderzoek en zullen niet beschikbaar zijn voor anderen dan de afstudeerders die het interview afnemen, lector Remco Spithoven en eventuele ondersteunende collega's van het lectoraat Maatschappelijke Veiligheid.

De resultaten van het onderzoek worden gebruikt voor praktijkpublicaties en wetenschappelijke publicaties van Remco Spithoven en eventuele ondersteunende collega's van het lectoraat Maatschappelijke Veiligheid en/of samenwerkingspartners. In al deze publicaties zal ervoor worden gezorgd dat herkenning van de deelnemers aan de interviews volstrekt onmogelijk is. U kunt uw medewerking aan het interview op ieder moment stop zetten of na het interview uw toestemming voor het gebruik van de informatie intrekken. Ook kunt u aangeven op specifieke vragen niet te kunnen of willen antwoorden. Mocht u na het interview nog vragen hebben of het verslag willen inzien, dan kunt u contact opnemen met Remco Spithoven, via telefoonnummer 06 12 61 84 71.

Ik heb dit formulier gelezen en stem er mee in,

Datum	Plaats	Handtekening deelnemer

Ik verklaar op deze wijze te werk te gaan,

Datum	Plaats	Handtekening afstudeerder

Datum	Plaats	Handtekening hoofdonderzoeker

Bijlage 4: Actorenanalyse

ACTORENANALYSE

Proactie	*Preventie*	*Preparatie*	*Repressie*	*Nazorg*
- Eindgebruikers - Banken - Supercontrollers - Hosting- en serviceproviders - Appontwikkelaars - Autoriteit Consument en Markt (ACM)	- Eindgebruikers **Lokaal:** - Gemeenten - Onderwijsinstellingen - Politie - Welzijnsorganisaties - Jongerenwerk - Ondernemersverenigingen - Studentenverenigingen **Regionaal:** - Platform Veilig Ondernemen (PVO) - Provincie - Veiligheidsnetwerk Oost-Nederland **Landelijk:** - Ouderenbonden - Brancheorganisaties - Banken - Digital Trust Center (DTC) - Centrum voor Criminaliteitspreventie en Veiligheid (CCV) - MKB Cybercampus - Fraude Infodesk - Alert Online - Surf NL - Politie - Openbaar Ministerie - Kamer van Koophandel - Vereniging Nederlandse Gemeenten (VNG) - Consumentenbond - Verzekeraars - Webwinkels	- Veiligheidsregio i.s.m. (veiligheids)partners	- Eindgebruikers - Politie - Openbaar Ministerie - Banken - FOX IT - Orion - Nortwave - Hoffman	- Eindgebruikers - Slachtofferhulp Nederland - Bureau HALT - Verzekeraars - Fraude Infodesk - Banken

Bijlage 5: Interview transcripten

Alle interviews zijn volledig getranscribeerd, digitaal gecodeerd en uitgewerkt voor dit onderzoek.