FACULTEIT RECHTSGELEERDHEID
DECANAAT
TIENSESTRAAT 41
3000 LEUVEN
Academiejaar 2018 - 2019

CYBERCRIMINALITEIT VERGELEKEN: Een beschrijvend kwalitatief onderzoek naar cybercriminaliteit en het cyberveiligheidsbeleid van gemeenten in België en Nederland.

Promotor: Prof. L. PAOLI
Begeleider: C. VERSTRAETE

Verhandeling, ingediend door REYHAN CIGDEM, bij het eindexamen voor de graad van MASTER IN CRIMINOLOGY

FACULTEIT RECHTSGELEERDHEID
DECANAAT
TIENSESTRAAT 41
3000 LEUVEN
Academiejaar 2018 - 2019

CYBERCRIMINALITEIT VERGELEKEN: Een beschrijvend kwalitatief onderzoek naar cybercriminaliteit en het cyberveiligheidsbeleid van gemeenten in België en Nederland.

Promotor: Prof. L. PAOLI
Begeleider: C. VERSTRAETE

Verhandeling, ingediend door REYHAN CIGDEM, bij het eindexamen voor de graad van MASTER IN CRIMINOLOGY

Samenvatting

Dit onderzoek tracht inzicht te verwerven in met welke vormen van cybercriminaliteit van verschillende gemeenten in België en Nederland geconfronteerd worden en hoe ze de interne cyberveiligheid binnen de eigen organisatie waarborgen met hun beleid. Ook wordt er onderzocht hoe de gemeenten zich verhouden ten opzichte van elkaar. De volgende onderzoeksvragen zijn voor dit onderzoek geformuleerd:

1. In welke mate worden de verschillende gemeenten geconfronteerd met cybercriminaliteit?
2. Welke maatregelen nemen de gemeenten in het kader van hun cyberveiligheidsbeleid?

De onderzoeksvragen werden beantwoord door middel van kwalitatieve onderzoeksmethoden. Dit onderzoek is een meervoudige beschrijvende casestudy die is uitgevoerd door middel van diepte-interviews en een beleidsdocumentenanalyse. In totaal zijn er 4 gemeenten in België en 5 gemeenten in Nederland onderzocht. Hierbij zijn 15 respondenten geïnterviewd en zijn er 7 beleidsdocumenten van en/of over gemeenten geanalyseerd. Door de gedetailleerde beschrijving van de bestudeerde cases zal dit onderzoek een waardevolle aanvulling zijn op de bestaande literatuur over cybercriminaliteit en cyberveiligheid. De resultaten van dit soort onderzoeken kunnen ook een belangrijke rol spelen met betrekking tot het vormen van een cyberveiligheidsbeleid voor de interne bedrijfsvoering bij gemeentelijke organisaties.

De gemeenten hebben op dagelijkse basis te maken met cybercriminaliteit, vooral *spam* en *phishing* maar ook andere vormen zoals bijvoorbeeld DDoS aanvallen, *cyrptolockers* en *defacing* komen voor. De directe schade voor de gemeenten die hierdoor ontstaat is vrijwel niet uit te drukken in monetaire waarden omdat de gemeenten de schade niet kwantificeren en omdat de gemeenten geen winstoogmerk hebben. Wel hebben de gemeente last van indirecte schade in de vorm van imagoschade die ontstaat nadat (veelal) incidenten met datalekken bekend worden. De proactieve en reactieve maatregelen die de gemeenten nemen zijn opgenomen in het informatieveiligheidsbeleid. De beleidsmedewerkers zijn zich allen bewust van de risico's die cybercriminaliteit met zich meebrengt en proberen met de beperkte middelen die ze hebben de organisatie zo goed mogelijk te beschermen. Verder werken ze in beperkte mate samen op regionaal en nationaal niveau. Echter hebben de organisaties geen uniformiteit in het beleid, die is opgesteld op basis van richtlijnen, en werken ze ook niet internationaal samen waardoor er minder efficiënt wordt omgegaan met de beschikbare middelen. Cyberveiligheid staat

onvoldoende op de politieke agenda van bestuurders en de gemeenten kampen met structurele tekorten in gekwalificeerd personeel. Hierdoor moet vaak externe expertise worden ingehuurd en zijn kwaliteitsvereisten met externe leveranciers vaak onduidelijk. Het vergroten van politiek draagvlak zodat er meer middelen beschikbaar komen voor cyberveiligheid is hierbij essentieel.

Dit onderzoek hoopt aanzet te geven tot meer onderzoek naar cybercriminaliteit en cyberveiligheid omdat het een fenomeen is dat de gehele samenleving raakt. Het risico op ernstige verstoringen moet zo veel mogelijk gereduceerd worden, daarom is het van belang dat organisaties alle mogelijke middelen aangereikt krijgen om de interne cyberveiligheid zo goed mogelijk in te richten door middel van effectief beleid.

Dankwoord

Als eerst wil ik mijn begeleider Cedric Verstraete bedanken die al mijn vragen geduldig heeft beantwoord. Hij stak me een hart onder de riem door me dit advies te geven:

> "Probeer je niet blind te staren op de obstakels, maar probeer te blijven focussen op de weg die voor je ligt. Tijdens slipcursussen raden ze ook altijd aan om weg te kijken van het obstakel en je blik en je stuur te richten op de mogelijke uitgangswegen, anders crash je."

Ook mijn promotor, professor L. Paoli, die me heeft geholpen met het specificeren van mijn onderzoek en als vrouw in de criminologie een ware inspiratie voor mij is, verdiend een woord van lof.

Dank aan alle respondenten, zonder hen was dit onderzoek niet mogelijk geweest.

Tot slot, dank aan mijn familie en vrienden die in me bleven geloven toen ik dat zelf niet meer deed. In het bijzonder wil ik mijn vriend bedanken die zich over me heeft ontfermd en me elke keer weer op weg hielp met kritische feedback en een luisterend oor bood. Hun steun en begrip was goud waard.

Lijst met afkortingen

Engels:

BSG	Baseline Security Guidelines (België)
CBK	Common Body of Knowledge
CERT	(Federal) Computer Emergency Response Team
CIA	Central Intelligence Agency
CISO	Chief Information Security Officer
CISSP	Certified Information Security System Professional
DDoS	Distributed Denial of Service
DPO	Data Protection Officer
EDA	European Defence Agency
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardization
NCSs	National Cybersecurity Strategies
NIS-*Directive*	Network and Information Security Directive
NIST	National Institute of Standards
PDCA	Plan, Do, Check, Act
RFM	(Technologies) Risk Management Framework
UNODC	United Nations Office on Drugs and Crime

Nederlands:

Art.	Artikel

BIG	Baseline Informatie Gemeente
BIO	Baseline Informatie Overheid
BS	Belgisch Staatsblad
CCB	Centrum voor Cybersecurity België
CCV	Centrum voor Criminaliteitspreventie en Veiligheid (Nederland)
EU	Europese Unie
IBD	Informatiebeveiligingsdienst voor Gemeenten (Nederland)
I(C)T	Informatie (- en Communicatie) Technologie
LJN	Landelijk Jurisprudentienummer (Nederland)
MB	Ministerieel Besluit (België)
MvT	Memorie van Toelichting
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum (Nederland)
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
RvE	De Raad van Europa
Sr.	Strafwetboek (België)/Wetboek van Strafrecht (Nederland)
Stb.	Staatsblad van het Koninkrijk der Nederlanden
Sv.	Wetboek van Strafvordering (België & Nederland)
V-ICT-OR	Vlaamse ICT-Organisatie
VN	Verenigde Naties
VNG	Vereniging Nederlandse Gemeenten
VS	Verenigde Staten (van Amerika)
VVSG	Vereniging van Vlaamse Steden en Gemeenten
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

Lijst met bijlagen

Inhoudsopgave

Samenvatting

Inleiding

De laatste jaren is de digitale wereld steeds meer alom vertegenwoordigd in onze maatschappij. In alle lagen van de samenleving is technologie doordrongen in ons dagelijks leven. Hoewel dit onmiskenbaar voordelen met zich meebrengt kleven er ook risico's aan deze digitalisering (Stol, 2018, p. 1). De digitale systemen waar we gebruik van maken hebben een mate van kwetsbaarheid en 'cybercriminaliteit' is dan ook een term die steeds vaker opduikt in deze context. Volgens de Verenigde Naties (VN) waren er in 2011 2,3 miljard mensen, wat gelijk staat aan een derde van de wereldbevolking, die toegang tot het internet hebben (Malby, et al., 2013, p. 1).

Hierbij worden niet alleen individuen en bedrijven bedreigd, ook de overheden staan onder druk (McGuire & Dowling, 2013, p. 4). Dat staten dreiging ondervinden blijkt ook uit het jaarverslag van het Nederlandse Ministerie van Defensie waarin staat dat spionage, beïnvloeding en sabotage in het digitale domein een bedreiging vormen voor Nederland (MIVD, 2018). Grote cyberaanvallen als die van de '*Stuxnet*-worm' die een nucleaire fabriek van de overheid in Iran schade heeft toegebracht in 2009 onderstrepen de noodzaak voor statelijke actoren om hun cyberveiligheidsbeleid op orde te hebben (Collins & McCombie, 2012, p. 88; Porche, Sollinger, & McKay, 2011, p. 1). Zo zijn er staten die hun militaire capaciteiten flink hebben uitgebreid met cyberwapens om internationale conflicten uit te vechten (Benschop, 2013, p. 9). De vraag is dus niet óf er een cyberaanval zal plaatsvinden, maar wanneer en of de getroffene op dat moment de juiste beveiliging heeft (Papelard & Bobbert, 2018, p. 17). Om met deze ontwikkelingen bij te blijven hebben verschillende overheidsorganisaties de laatste jaren dan ook steeds meer geïnvesteerd in cyberveiligheid (Prins, 2013, p. 7).

Op Europees niveau heeft de Raad van Europa (RvE) zich in 2001 al toegelegd op de ontwikkelingen omtrent het digitaliseren van onze maatschappij en kwam met het verdrag van Boedapest.[1] In dit verdrag zijn de risico's van digitalisering erkend en is vastgelegd dat de landen die het verdrag hebben getekend wetgeving hierover implementeren en samen zullen werken om cybercriminaliteit te bestrijden. Ook in de mededeling van de Europese

[1] Verdrag van Boedapest betreffende de computercriminaliteit van 23 november 2001, *Treaty Series of the Council of Europe* – No. 185, *BS* 21 november 2012, 69.093; Hierna: Cybercrimeverdrag.

Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's van 2007 wordt de dreiging benadrukt:

> "Aanvallen op grote schaal tegen informatiesystemen of organisaties en individuen (vaak via de zogenaamde botnets[2]) lijken zich steeds meer voor te doen. Ook werden recentelijk incidenten waargenomen met systematische, goed gecoördineerde en grootschalige rechtstreekse aanvallen tegen de kritieke informatie-infrastructuur van een staat. Dit werd verergerd door de in elkaar overgaande technologieën en het versneld onderling verbinden van informatiesystemen, hetgeen deze systemen meer kwetsbaar heeft gemaakt. Aanvallen zijn vaak goed georganiseerd en worden gebruikt voor afpersing."[3]

Cybercriminaliteit en de daarmee nauw verbonden cyberveiligheid zijn dynamische werkvelden en het is dan ook van belang hier voldoende aandacht aan te besteden. Dit wordt vooralsnog weinig gedaan in de wetenschappelijke literatuur. Dit is zorgelijk omdat de schadelijke gevolgen groot kunnen zijn. Zo berichtte de New York Times recent dat Baltimore samen met andere steden over de gehele Verenigde Staten van Amerika (VS) weken last hebben van een cyberaanval die duizenden computers heeft platgelegd. Hierdoor zijn allerlei diensten, zoals watervoorzieningen, plat komen te liggen (The New York Times, 2019). Dichter bij huis is dezelfde dreiging aanwezig. Zo meldt de website 'Binnenlands Bestuur' (2017) dat de 3 Nederlandse gemeenten Blaricum, Eemnes en Laren in maart 2017 zijn getroffen door cyberaanvallen. Tevens is er ook in België ruimte voor verbetering. Zo zouden 1 op de 5 de gegevens van haar inwoners niet voldoende beschermen (De Morgen, 2017).

Het gebrek aan wetenschappelijke literatuur over hoe lokale overheden omgaan met deze moderne dreiging maakt de noodzaak van dit onderzoek duidelijk. In het kader van deze meesterproef daarom gekozen om dit onderzoek te beperken tot het vergelijken met welke vormen van cybercriminaliteit verschillende gemeenten in België[4] en Nederland geconfronteerd worden en hoe ze de interne cyberveiligheid binnen de eigen organisatie waarborgen met hun beleid. Er wordt namelijk ook op gemeentelijk niveau dreiging

[2] Botnet verwijst naar een verzameling aangetaste apparaten waarop onder een gemeenschappelijk commando programma' s worden gedraaid (Commissie van de Europese Gemeenschappen, 2007).
[3] Eur-Lex. Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's – Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, 22 mei 2007; Hierna: mededeling van de Commissie.
[4] Met België wordt steeds Vlaanderen bedoelt. De keuze hiervoor komt terug in de methodologie.

ondervonden. De resultaten van dit soort onderzoeken kunnen een belangrijke rol spelen met betrekking tot het vormen van een cyberveiligheidsbeleid voor de interne bedrijfsvoering bij gemeentelijke organisaties. Deze meesterproef is opgesplitst in 3 grote delen: De literatuurstudie is het eerste deel en biedt een overzicht van de bestaande literatuur over cybercriminaliteit en cyberveiligheid. Het tweede deel bestaat uit het conceptueel kader en de onderzoeksopzet met daarin onder andere de onderzoeksvragen. Tot slot de resultaten met de discussie, conclusie en de aanbevelingen waarin onder andere de resultaten worden teruggekoppeld naar de bevindingen uit de literatuur.

DEEL A: LITERATUUR STUDIE

De literatuurstudie richt zich op de bestaande wetenschappelijke literatuur over cybercriminaliteit en cyberveiligheid. Het gaat onder ander om boeken die beschikbaar waren in verschillende bibliotheken zoals de universiteitsbibliotheken van de Katholieke Universiteit Leuven, de Erasmus Universiteit Rotterdam en de openbare Bibliotheek Rotterdam. Bij de boeken is voornamelijk gelet op de titel, het jaartal en het specifieke onderwerp. Op die manier is er nagegaan of de inhoud van het boek een meerwaarde zou opleveren aan deze literatuurstudie.

De digitale zoekmethode omhelst het gebruik van verschillende zoekwoorden zoals '*cybercrime'*, 'cybercriminaliteit', 'informaticacriminaliteit', 'computercriminaliteit' en elk van deze zoekwoorden waarin 'criminaliteit' is vervangen door 'veiligheid' of '*security'*. Daarnaast is er gezocht naar 'beleid' en 'overheid' en 'gemeenten' en Engelstalige zoektermen zoals '*local government*'. Deze zoekwoorden zijn gebruikt in databanken zoals, LIMO en Google (Scholar). Dit heeft geleid tot verschillende soorten onlinebronnen zoals pdf-bestanden, digitale boeken, wetgeving en openbare beleidsdocumenten. Tevens bevindt het domein van cybercriminaliteit en cyberveiligheid zich niet alleen in de (wetenschappelijke) literatuur maar ook op het internet zelf. Alles wat met het cyberdomein te maken heeft en is verbonden aan het internet is onderhevig aan snelle veranderingen binnen de technologie (Clough, 2015, p. 4). Om die reden is gekozen om zoveel mogelijk recente literatuur in onderstaand overzicht op te nemen.

Het gebrek aan wetenschappelijke literatuur die specifiek gaat over hoe gemeenten in België en Nederland met cybercriminaliteit en cyberveiligheid omgaan maakte het selecteren een lastig proces. Zo gaat het detail van wetenschappelijk onderzoek in Europa vaak niet verder dan nationale overheden. Een aantal bronnen stippen lokale overheden/gemeenten kort aan als onderdeel van een groter geheel, maar bieden geen diepgaande bruikbare data. Wel zijn een aantal wetenschappelijke artikelen beschikbaar over lokale overheden in de VS. Hetzelfde geldt voor Europese beleidsdocumenten, waarbij het ontbreekt aan documenten die zich richten op gemeenten.

Het enige Belgische onderzoek dat zich wel richt op gemeenten is verkregen van de onderzoekers zelf en is niet openbaar. In Nederlandse context zijn de enige beschikbare

onderzoeken gericht op de Haven van Rotterdam, dat onderdeel is van de gemeente Rotterdam, en op andere kritische infrastructuren.

In hoofdstuk 1 van de literatuurstudie wordt ingegaan op cybercriminaliteit. Het fenomeen wordt als eerste gedefinieerd en er wordt een typologie besproken. Ook komt de oorsprong van en de schade die voortvloeit uit cybercriminaliteit aan bod en wordt er gekeken naar wat er bekend is over cybercriminaliteit bij gemeenten. In het wetgevende kader in hoofdstuk 2 wordt de relevante wet- en regelgeving besproken, ook wel de juridische definiëring. Dit bestaat uit de internationale en de 2 nationale wetgevingen. Hier wordt de VN-wetgeving besproken en het Cybercrimeverdrag dat is geïmplementeerd in nationale wetgevingen komt aan bod. In hoofdstuk 3 volgt er een definitie van cyberveiligheid en een effectief cyberveiligheidsbeleid uiteengezet met een korte weergave van het beleid van overheden. Tot slot wordt er ingegaan op (wetenschappelijk onderzoek over) cyberveiligheid bij gemeenten.

Hoofstuk 1. Cybercriminaliteit ontleed

Om de onderzoeksvragen te kunnen beantwoorden moet het onderwerp worden afgebakend. In dit hoofdstuk wordt er een definiëring gegeven van cybercriminaliteit en er wordt een typologie besproken. Daarna volgt er een kort overzicht van de oorsprong van cybercriminaliteit. Tot slot worden de soorten schade die voortvloeien uit cybercriminaliteit besproken en wordt er gekeken naar wat er bekend is over cybercriminaliteit bij gemeenten.

1.1 Definiëring cybercriminaliteit

Wat betreft de definitie van cybercriminaliteit blijkt uit de literatuur dat die moeilijk te achterhalen is uit zowel academische literatuur als in juridische en beleidsdocumenten (Paoli, Visschers, Verstraete, & van Hellemont, The Impact of Cybercrime on Belgian Businesses, 2017, p. 3). Yar (2006, p. 5) benoemt dat cybercriminaliteit niet zozeer een specifieke handeling is, maar een scala aan verschillende illegale handelingen zijn waarvan de overeenkomst is dat ze zich alleen in de gedigitaliseerde omgeving, ook wel '*cyberspace'* bevinden. *Cyberspace* zou kunnen worden gezien als een vijfde dimensie als variant op de

klassieke 4 dimensies van land, lucht, zee en de ruimte (Kerkhofs & Van Linthout, 2013, pp. 18-19).

Clough (2015, p. 9) beschrijft verschillende termen die worden gebruikt om cybercriminaliteit te beschrijven. Er kan gedacht worden aan bijvoorbeeld 'computercriminaliteit', 'internetcriminaliteit' en '*high-tech* criminaliteit'. Bryant & Bryant (2014) hebben het ook wel over *'digital crime'.* Dit zijn bijna net zoveel mogelijke termen om cybercriminaliteit te beschrijven als dat er verschillende soorten cybermisdrijven zijn. De reden hiervoor heeft te maken met het feit dat het door de bril van verschillende disciplines, zoals de sociale wetenschappen, rechten en informatie- en communicatietechnologie (ICT), wordt bestudeerd (Jaishankar, 2010, p. 27). Zowel Paoli et al. (2017, p. 3) als Clough (2015, p. 10) gaan ook in op de notie, die in 2013 is benoemd door de *United Nations Office on Drugs and Crime* (UNODC), dat veel documenten niet eens zozeer een definitie geven van cybercriminaliteit maar bepaalde acties benoemen die een element van cybercriminaliteit bevatten.

Voor dit onderzoek wordt de term 'cybercriminaliteit' aangehouden met als uitgangspunt dat '*cybercrime'* het meest gangbare woord is dat gebruikt wordt en cybercriminaliteit hier het Nederlandstalige equivalent van is. Dit blijkt bijvoorbeeld uit de (eerdergenoemde) mededeling van de Europese Commissie waarbij in het Nederlandstalige document het begrip 'cybercriminaliteit' wordt gebruikt. Als definitie wordt in de mededeling van de Europese Commissie aangehouden:

> "Misdrijven gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen."[5]

Het Cybercrimeverdrag van de RvE definieert cybercriminaliteit als volgt:

> "Alle strafbare gedragingen die gericht zijn tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen en middelen en de strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of met die systemen onderhouden geautomatiseerde processen."[6]

[5] Eur-Lex. Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's – Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, 22 mei 2007; p.2.
[6] Vedrag van Boedapest betreffende de computercriminaliteit van 23 november 2001, *Treaty Series of the Council of Europe* – No. 185, *BS* 21 november 2012, 69.093;

De wetenschappelijke definitie van cybercriminaliteit dat voor dit onderzoek wordt gebruikt is een brede:

> "Cybercriminaliteit is alle vormen criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict." (Leukefeldt, Domenie, & Stol, 2009, p. 2)

1.2 Typologie cybercriminaliteit

Ondanks het gebruik van verschillende termen voor cybercriminaliteit lijken beleidsmakers en onderzoekers het eens te zijn over een onderscheid (Clough, 2015, p. 11 & 31; Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 3; Kerkhofs & Van Linthout, 2013, p. 39). Dit onderscheid bestaat uit enerzijds criminaliteit waarbij de computer als doel wordt gebruikt. Dit worden ook wel 'computergerichte delicten' genoemd (Koops, 2014, p. 214). Hierbij zijn computers of gegevens het doel. Deze soorten van criminaliteit kunnen enkel uitgevoerd worden 'door het gebruik van een computer, van computernetwerken, of andere vormen van ICT' (McGuire & Dowling, 2013, p. 5). Voorbeelden hiervan zijn het verspreiden van virussen of het uitvoeren van *Distributed Denial of Service* (DDoS)[7] aanvallen.

Anderzijds bestaat cybercriminaliteit uit aanvallen waarbij de computer als middel of instrument wordt gebruikt om reeds bestaande criminaliteit uit te voeren. Voorbeeld hiervan zijn *hacken* om gegevens te verkrijgen of *phishing* mails (Leukefeldt, Domenie, & Stol, 2009, p. 257). Deze vormen van criminaliteit kunnen ook gepleegd worden zonder het gebruik van ICT (McGuire & Dowling, 2013, p. 5). Dit worden ook wel 'computer-gerelateerde delicten genoemd (Koops, 2014, p. 214). Deze 2 vormen vallen volgens Leukefeldt et al. (2009, p. 2) onder cybercriminaliteit in enge zin (*sensu stricto).*

Om helemaal volledig te zijn in de typologie is er ook een derde categorie. Dit is niet zozeer cybercriminaliteit, maar criminaliteit die wordt ondersteund door een computer. Deze misdrijven richten zich voornamelijk op personen, het verkrijgen van objecten van waarde dan wel geld en niet zozeer op systemen of data (Malby, et al., 2013, p. 15). Dit zijn delicten waarbij ICT dus geen doelwit op zich is maar in beperkte mate onderdeel van de uitvoering.

[7] Dat is een aanval op een computersysteem vanuit grote hoeveelheden andere computers, met als doel om het systeem plat te leggen door overbelasting.

Hierbij kan bijvoorbeeld gedacht worden aan belastend bewijsmateriaal, zoals kinderpornografie, dat wordt opgeslagen op computers (Clough, 2015, p. 11; Wall, 2007, p. 103). Dit wordt ook wel 'computer-relevante delicten' genoemden kan dus als aparte categorie gezien worden (Koops, 2014, p. 214). Deze vorm wordt door Leukefeldt et al. (2009, p. 2) cybercriminaliteit in ruime of brede zin (*sensu lato*) genoemd. Volgens Clough (2015, p. 11) valt uit deze classificatie de conclusie te trekken dat cybercriminaliteit zowel een nieuwe vorm van criminaliteit is als 'oude' vorm van criminaliteit die op nieuwe manieren worden gepleegd.

In de mededeling van de Europese Commissie komen deze 3 categorieën ook naar voren. Daarin wordt gesteld dat de verschillende "categorieën misdrijven gemeen hebben dat zij op massale schaal kunnen worden gepleegd en met een grote geografische afstand tussen het misdrijf en de gevolgen ervan".[8] Dit uit zich ook in een 'technologie neutrale' typologie door Paoli et al. (2017, p. 31) die de verschillende soorten cybercriminaliteit samenvat aan de hand van het Cybercrimeverdrag, de Belgische strafwet en academische literatuur. Deze 5 types zijn: illegale toegang tot IT-systemen, bedrijfsspionage, gegevens- of systeeminterferentie, cyber afpersing en internetfraude. Illegale toegang tot IT-systemen houdt in dat er ongeautoriseerde modificatie of toegang is. Te denken valt hierbij aan *hacking*, Trojaanse paarden, achterdeuren, *social engineering* zoals het raden van wachtwoorden en *(spear)phishing*. Bedrijfsspionage vindt plaats door pogingen tot binnendringen van bedrijfsnetwerken en het verzamelen van informatie door bijvoorbeeld *phishing* en scannen. Gegevens- of systeeminterferentie bestaat uit sabotage zoals DDoS, malafide materiaal zoals *spam*, *malware* en/of *cryptolockers*. Dat laatste valt ook onder cyber afpersing waarbij *ransomware* wordt ingezet. Internetfraude is fraude in de vorm van illegaal naamgebruik of onrechtmatig gebruik van *resources.* Deze typologie is ook van toepassing op overheden (Paoli, Visschers, & Verstraete, 2018) en wordt om die reden aangehouden in dit onderzoek.

1.3 Oorsprong van cybercriminaliteit

[8] Eur-Lex. Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's – Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, 22 mei 2007; p2.

Cyberaanvallen kunnen van verschillende oorsprong zijn. Zo zijn er statelijke actoren die een bedreiging vormen (denk aan China en Rusland). Een andere groep zijn cybercriminelen, dat zijn 'gewone' criminelen die handig zijn met computers en vooral uit zijn op financieel gewin. Een kleinere groep bestaat uit medewerkers, cybervandalen die uit zijn op wraak en '*script kiddies',* dat zijn veelal jonge daders die plezier hebben in hun kundigheid en vaak niet helemaal beseffen hoeveel schade ze daarmee kunnen aanrichten (Bobbert & Broersma, 2018, pp. 39-48). Ook bestaat er een groep die handelt uit activistische of terroristische overtuigingen (Van Houten, Spruit, & Wolters, 2015, p. 27). Leukefeldt et al. (2009, p. 254) veronderstellen dat cybercriminaliteit dezelfde structuur heeft als het klassieke offline criminaliteit, dus voornamelijk grote groepen daders die relatief kleine delicten plegen op min of meer individuele basis. Georganiseerde criminaliteit wordt gepleegd door een aantal groeperingen die geen monopolie hebben op cybercriminaliteit.

Omdat *cyberspace* niet gebonden is aan landsgrenzen is het lastig voor wetshandhaving en traditioneel strafrecht om hier grip op te krijgen. Zo zitten gebruikers niet alleen over de hele wereld maar is ook de toegankelijkheid toegenomen. Computers zijn gebruiksvriendelijker geworden, wanneer iemand zelf de benodigde kennis niet heeft om een cybermisdrijf te plegen dan kan die expertise snel gevonden worden. Er is ook een toename in de schaal waarop gegevens kunnen worden opgeslagen. Dataopslag wordt steeds efficiënter door verbeterde technologieën (Clough, 2015, pp. 6-8). Daardoor kunnen ook daders zich zowel over de hele wereld bevinden als schade veroorzaken. Ook is het voor autoriteiten lastig om toezicht te krijgen omdat veel digitale infrastructuur bezit is van private partijen. Hierdoor is de pakkans voor daders klein en is samenwerking dus noodzakelijk (Clough, 2015, p. 7; Kerkhofs & Van Linthout, 2013, p. 19).

1.4 Schade van cybercriminaliteit bij organisaties

Criminaliteit levert schade op en die schade wordt vaak uitgedrukt in kosten. Impact kosten en schade van criminaliteit zijn begrippen die geen duidelijke definitie hebben en vaak inwisselbaar worden gebruikt in zowel academische literatuur als in beleid (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 6). Er zijn verschillende manieren om kosten te classificeren vanuit economisch oogpunt. Zo kan het gaan om private kosten, publieke kosten, sociale kosten of opportuniteitskosten. Dat laatste gaat om de kosten die worden

gemaakt voor een bepaalde service of goed. Ook is er een verschil tussen ‘incidentiele’ versus ‘prevalente’ kosten. Het onderscheid hierin zit in dat een enkel incident zowel op korte als op lange termijn kosten kan opleveren (Cohen & Bowles, 2010, pp. 143-145). Imago schade kan bijvoorbeeld een langdurig effect hebben wanneer bekend wordt dat een organisatie is gehackt. In de literatuur over de kosten van criminaliteit wordt een onderscheid gemaakt in 3 types van kosten: De kosten die worden veroorzaakt door crimineel gedrag; die van de maatschappij ter preventie of als reactie op criminaliteit; en de kosten voor de dader (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 6; Cohen & Bowles, 2010, p. 147).

Greenfield & Paoli (2013, p. 868) maken in hun *harm assessment framework* onderscheid tussen verschillende soorten van schade en de dragers van die schade. De dragers kunnen individuen zijn, private-sector entiteiten, overheden of de omgeving. Daarbij noemen zij 4 types van schade. Ten eerste de functionele integriteit die bestaat voor organisaties uit een verlies van operationele integriteit. Ten tweede het materiële belang, ten derde imagoschade en tot slot de privacy schade waarbij gevoelige gegevens buit worden gemaakt. Deze opgetreden schade kan marginaal zijn en maar weinig voorkomen of het kan catastrofistisch zijn en constant voorkomen (Paoli, Visschers, Verstraete, & van Hellemont, The Impact of Cybercrime on Belgian Businesses, 2017, p. 9).

Schade van cybercriminaliteit bestaat dus uit meer dan materiële of monetaire schade alleen. Naast imagoschade kan er bijvoorbeeld ook schade ontstaan aan bestanden die zijn vernield of netwerken die opnieuw beveiligd moeten worden (Leukefeldt, Domenie, & Stol, 2009, p. 51). Ook omzetverlies voor bedrijven en compensatiebetalingen zijn vormen van schade die kunnen voorkomen (Finnerty, et al., 2018, p. 44). Bobbert & Mulder (2018, p. 72) stellen samenvattend dat inbreuken op de beveiliging problematisch zijn omdat het negatieve effecten kan hebben op de continuïteit, de wettelijke aansprakelijkheid, het imago, de inzetbaarheid en de financiële positie van organisaties.

Paoli et al. (2017, p. 47) hebben in hun onderzoek naar cybercriminaliteit bij Belgische bedrijven kosten onderverdeeld in personeelskosten en andere kosten. Personeelskosten zijn de manuren besteed aan het beperken van een cyberincident, het deel dat is uitbesteed en de daaruit voortvloeiende kosten. De andere kosten zijn onderverdeeld in 5 categorieën: (1) vervanging van hardware en software; (2) waarde van andere verloren of beschadigde activa (bijvoorbeeld databestanden); (3) geld betaald aan overtreders; (4) boetes en

compensatiebetalingen en (5) inkomsten verloren als gevolg van een cybercriminaliteitsaanval.

De onderverdeling van kosten (en dus schade) die wordt aangehouden in dit onderzoek is drieledig. De kosten die worden veroorzaakt door crimineel gedrag kunnen namelijk worden onderverdeeld in 3 categorieën, namelijk: directe, indirecte en onopgemerkte kosten. Directe kosten kunnen worden uitgedrukt in monetaire waarden. Indirecte kosten kunnen zich uiten in bijvoorbeeld productiviteitsverlies, imagoschade, privacy schade of verlies van autonomie (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 7; Van Houten, Spruit, & Wolters, 2015, pp. 28-29; Anderson, et al., 2013, p. 269). Net als andere vormen van criminaliteit kent ook cybercriminaliteit een *dark number*, de onopgemerkte kosten. De aangiftebereidheid is lager waardoor de *dark number* hoger is en politie en justitie geen goed beeld hebben van de aard en omvang en schade van daderschap, slachtofferschap en de gevolgen van de verschillende vormen van cybercriminaliteit (Leukfeldt & Weulen Kranenbarg, 2017, p. 287). Extra lastig wordt het ook wanneer ondernemingen niet door hebben dat ze slachtoffer zijn (Wall, 2007, p. 20). Hierdoor is het onmogelijk om alle schade te reduceren tot een enkele monetaire waarde (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 7).

1.5 Cybercriminaliteit bij gemeenten

In dit deel wordt ingegaan op het zeer beperkte materiaal in de wetenschappelijke literatuur en in beleidsdocumenten met betrekking tot cybercriminaliteit bij gemeenten. Hierbij worden de gevonden documenten van en/of over gemeenten overigens zelf buiten beschouwing gelaten omdat die zijn opgenomen in de beleidsdocumentenanalyse. Er zijn geen internationale beleidsdocumenten of onderzoeken van overheidsinstanties zoals bijvoorbeeld ENISA of Europol te vinden die zich richten op cybercriminaliteit bij gemeenten. De internationale wetenschappelijke literatuur is voornamelijk gericht op de VS. Enkele auteurs gaan in op hoe lokale overheden in de VS in toenemende mate slachtoffer zijn van cybercriminaliteit, soms met vergaande gevolgen. Cliff (2017, p. 6) beschrijft hoe lokale overheden in de VS steeds afhankelijker worden van technologie en de risico's die dit met zich meebrengt. Zo is de overheid extra gevoelig voor datalekken als gevolg van *phishing*, hacken, *cryptolockers* of eigen personeel met slechte bedoelingen. De overheid

bezit immers veel persoonlijke data van burgers, maar ook concurrentie gevoelige informatie van bedrijven of bijvoorbeeld lopende strafrechtelijke onderzoeken (Cliff, 2017, p. 8). Meerdere gemeentelijke diensten zoals in Florida, Los Angeles, Collinsville en Cockrell Hill zijn slachtoffer geweest van cybercriminaliteit. De gezamenlijke materiële schade kan oplopen in de miljoenen maar erger dan dat is het verlies van het vertrouwen van de burgers.

Cybercriminaliteit wordt uitgevoerd door zowel statelijke actoren als individuen en het is vaak dan ook moeilijk te zeggen wie de aanvallen uitvoert en wat de motivatie is behalve het financiële gewin (Cliff, 2017, p. 6). Lokale overheden in de VS hebben te maken met dezelfde vormen van cybercriminaliteit als andere sectoren en zullen zich op eenzelfde manier moeten beschermen tegen risico's. Zo moeten ze gedetailleerd beleid hebben waarin de maatregelen en de *best practices* worden opgenomen die zijn opgesteld door IT-professionals. Vervolgens moeten ze ervoor zorgen dat het beleid wordt gecommuniceerd binnen de organisatie zodat iedereen ervan op de hoogte is. Ook heeft de organisatie de verantwoordelijkheid om ervoor te zorgen dat het beleid wordt nageleefd (Cliff, 2017, p. 9). Ook Tully (2018, pp. 9-10) noemt verschillende steden zoals Atlanta en Baltimore die te maken hebben gehad met cyberaanvallen zoals *ransomware.* Het maakt voor cybercriminelen niet uit of een organisatie publiek of privaat is, de essentie blijft hetzelfde.

Norris & Mateczun (2017, pp. 3-4) schrijven over cyberveiligheidsproblemen bij lokale overheden, waaronder gemeenten, in de VS. Daaruit blijken ze regelmatig last te hebben van aanvallen, incidenten of inbreuken. Bijna de helft van de ruim 350 ondervraagde overheden ondervindt die dagelijks, maar opvallender is nog dat een-derde niet weet hoe vaak ze worden aangevallen. Ongeveer de helft houdt de incidenten niet bij. Ook wist een-derde niet te vertellen of de aanvallen van buiten- of van binnenuit kwamen. Daarnaast weten ze vaak niet waarom ze precies het slachtoffer zijn van cybercriminaliteit.

In de Belgische en Nederlandse wetenschappelijke literatuur is vrijwel niets te vinden over cybercriminaliteit bij gemeenten. Er is slechts één onderzoek beschikbaar dat zich richt op de impact van cybercriminaliteit bij de Belgische overheid (Paoli, Visschers, & Verstraete, 2018). Een deel van dat onderzoek gaat specifiek over 2 Vlaamse gemeenten waarbij respondenten zijn geïnterviewd die daar werkzaam zijn. De onderzochte gemeenten geven aan dat de schade van cybercriminaliteit meevalt, ondanks dat ze wel slachtoffer zijn van voornamelijk *phishing.* Verder komt het voor dat er medewerkers zijn die toegang misbruiken, voornamelijk bij overplaatsingen binnen de organisatie, en worden DDoS

aanvallen en *ransomeware* incidenten genoemd. Ook *defacing* schijnt een enkele keer te zijn voorgekomen bij 1 van de 2 gemeenten.

Andere vormen van cybercriminaliteit zijn niet gerapporteerd. *Hard-* en *software* wordt niet altijd vervangen na een incident, hetgeen dan ook geen kosten met zich meebrengt wanneer dat niet gebeurd. Wel kan het voorkomen dat medewerkers enkele uren niet konden werken op hun computers. Die kosten, verlies van arbeidsproductiviteit, kan leiden tot schade aan de efficiëntie van de organisatie omdat processen stil staan. Wat betreft andere vormen van (non-monetaire) schade worden die ook verwaarloosbaar ingeschat door de respondent. Wel verwacht de respondent dat er meer cyberaanvallen zullen plaatsvinden in de toekomst (Paoli, Visschers, & Verstraete, 2018, pp. 20-23). De incidenten worden beheerd door eigen IT-staf, voor zover die beschikbaar is, of door externe experts zoals van de *IT-serviceprovider*. Waar nodig worden meldingen gemaakt bij andere instanties en/of overkoepelende autoriteiten. Hiertoe heeft de Informatiebeveiligingsdienst voor Gemeenten (IBD) een dreigingsbeeld 2019/2020 (hierna: IBD-rapport) opgesteld voor de Nederlandse gemeenten. Daarin worden de risico's en prioriteiten voor gemeenten uiteengezet. Deze wordt tweejaarlijks uitgebracht (IBD & VNG, 2018, p. 2). Dit document is meegenomen in de documenten analyse en wordt daarom hier niet nader toegelicht.

Hoofdstuk 2. Wetgevend kader

Dit hoofdstuk richt zich op de wet- en regelgeving van cybercriminaliteit die momenteel aanwezig is op internationaal niveau, Europees niveau en in België en Nederland. Net als vele andere vormen van criminaliteit is cybercriminaliteit namelijk strafbaar gesteld in de wet. In dit deel wordt dat wetgevend kader daarom uitgewerkt.

2.1 Internationale wet- en regelgeving

Cybercriminaliteit bevindt zich in *cyberspace* en is grensoverschrijdend (Kerkhofs & Van Linthout, 2013, pp. 9-10). Overal waar een internetverbinding te vinden is kunnen zich daders bevinden, en zelfs al zouden dader en slachtoffer zich in hetzelfde rechtsgebied bevinden, de data blijft niet altijd daar (Clough, 2012, p. 365). Om die reden is het zinvol

om te kijken naar hoe cybercriminaliteit is opgenomen in internationale wetgeving. Daarbij wordt een onderscheid gemaakt tussen verschillende niveaus: mondiaal, Europees en nationaal.

2.1.1 Mondiaal

Het belang van cyberveiligheid voor de samenleving blijkt uit de bestaande wet- en regelgeving. In de jaren 80' van de vorige eeuw had de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) van de VN al oog voor het bestrijden van computer gerelateerde economische criminaliteit (Kerkhofs & Van Linthout, 2013, p. 21). In de opgestelde lijst van strafbare handelingen werd hier nog geen onderscheid gemaakt tussen 'computer als doel' en 'computer als middel' criminaliteit.

In het Cybercrimeverdrag van de RvE uit 2001 zijn de risico's erkend en is vastgelegd dat de landen die het verdrag hebben getekend wetgeving hierover implementeren en samen zullen werken om cybercriminaliteit te bestrijden. De onderhandelingen voor dit verdrag begonnen in 1997.[9] Clough (2015, pp. 25-26) beschrijft hoe in 2015 alleen Rusland en San Marino als leden van de Raad het verdrag niet hebben getekend. Er zijn ook 2 landen, namelijk Canada en Zuid-Afrika, die geen lid zijn en het verdrag wel hebben getekend, maar niet geratificeerd. Er zijn 6 lidstaten die in dezelfde positie verkeren. Landen zoals de VS en Australië, die ook geen lid zijn, hebben het verdrag zowel getekend als geratificeerd. In totaal zijn er 53 landen die hebben getekend en 45 landen die het hebben geratificeerd.[10] Dit verdrag geldt nog altijd als leidend op internationaal vlak, hoewel binnen het kader van de VN een nieuw juridisch *framework* op zijn plaats zou zijn vanwege veroudering aldus een *Expert Group on Cybercrime* van de VN (UNODC, 2017, p. 4).

Op mondiaal niveau onderscheidt de VN 5 internationale en regionale clusters die zowel bestaan uit bindende als niet bindende instrumenten zoals de *Model Legislative Texts on*

[9] Voorwoord Verdrag van Boedapest betreffende de computercriminaliteit van 23 november 2001, *Council of Europe Treaty Series* – No. 185, *BS* 21 november 2012, 69.093.

[10] Ondertekenaars als leden van de RvE zijn Albanië, Armenië, België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, IJsland, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Moldavië, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Spanje, Zweden, Zwitserland, de Voormalige Joegoslavische Republiek, Macedonië, Oekraïne en het Verenigd Koninkrijk. Ondertekenaars als niet-leden van de Raad van Europa zijn de VS, Canada, Japan en Zuid-Afrika

Cybercrime, e-Crime and Electronic Evidence of 2010 uitgewerkt door de *International Telecommunication Union*, *Caribbean Community* en *Caribbean Telecommunications Union*. Deze zijn gericht op de bestrijding van cybercriminaliteit en dienen ter inspiratie voor de ontwikkeling van nationale wetgevingen (Malby, et al., 2013, pp. 64-65). Het eerste cluster is de RvE en de Europese Unie (EU), die zijn het belangrijkst voor dit onderzoek. De overige 4 zijn het Gemenebest van Onafhankelijke Staten of de Shanghai-samenwerkingsorganisatie, de intergouvernementele Afrikaanse organisaties, de Arabische Liga, en tot slot de Verenigde Naties. Een analyse van de multilaterale instrumenten met betrekking tot cybercriminaliteit laten zien dat de kernbepalingen veelal gelijk zijn maar dat er ook verschillen zijn in de inhoudelijke gebieden (Malby, et al., 2013, p. xix). Het harmoniseren van de verschillende nationale wetgevingen door hervormingen zodat er een internationale consistentie ontstaat wordt dan ook sterk bepleit door de VN. Op die manier zal een internationale aanpak van cybercriminaliteit beter uit te voeren zijn vanwege meer eenheid in wetgevingen (Malby, et al., 2013, p. 58).

2.1.2 Europa

Het Cybercrimeverdrag kan, zoals eerdergenoemd, gezien worden als de belangrijkste internationale wetgeving, zodoende geldt dit ook op Europees niveau. Omdat elk land het verdrag in eigen wetgeving moet implementeren ontstaat er een variatie in de nationale wetgevingen (Koops, 2010, p. 595). In de mededeling van de Europese Commissie[11] wordt het belang benadrukt van het samenwerken binnen de EU vanwege het grensoverschrijdend karakter van informatienetwerken. Sinds 2001 heeft de EU verschillende kaderbesluiten genomen die nu zijn of worden vervangen door richtlijnen. Zo gaat het om onderwerpen als bestrijding van fraude en vervalsing van betaalmiddelen,[12] de bestrijding van kinderpornografie[13] en de bescherming tegen aanvallen op informatiesystemen[14]

[11] Eur-Lex. Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's – Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, 22 mei 2007; p4.
[12] Kaderbesluit 2001/413/JBZ van 28 mei 2001, *betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten*, Pb.L. 2 juni 2001, L 149/1.
[13] Richtlijn 2011/92/EU van het Europese Parlement en de Raad van 13 december 2011, *ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad*, Pb.L. 17 december 2011, L 335/1.
[14] Kaderbesluit 2005/222/JBZ van 24 februari 2005, *over aanvallen op informatiesystemen*, Pb.L. 16 maart 2005, L 69/67.

(Hildebrandt & Koning, 2012, p. 199). Meer recent heeft de Europese Commissie in 2015 een overeenstemming bereikt met de nieuwe *EU Network and Information Security (NIS) Directive*[15]. Deze richtlijn voor cyberveiligheid behelst de regulering van vele gebieden zoals transport, banken, de zorgsector, maar ook digitale services zoals zoekmachines. In mei 2019 moet de richtlijn geïmplementeerd zijn in nationale wetgevingen van lidstaten van de EU. Lidstaten zijn verplicht om extra maatregelen te nemen voor cyberveiligheid zoals het creëren van speciale autoriteiten die zich hierop focussen (Maynard, Ijzinga, & Van Veldhuizen, 2018; Luysterborg, 2016). In België is dit het Centrum voor Cybersecurity België (CCB) en in Nederland is dat het Nationaal Cyber Security Centrum (NCSC).

2.2 Nationale wetgevingen

Gebaseerd op het Cybercrimeverdrag hebben België en Nederland wetgeving geïmplementeerd. In dit deel volgt een beschrijving van de nationale wetgevingen per land.

2.2.1 België

België kent een onderverdeling van het Strafwetboek (Sr.) en het Wetboek van Strafvordering (Sv). In het Sr. zijn de algemene bepalingen, overtredingen en misdrijven opgenomen, ook wel het materieel strafrecht. In Sv. staan de procedurele regels, ook wel het formele strafrecht. Samen vormen zij de basis van het Belgische strafrecht. Hoewel België in 2001 een van de eerste landen was die het Cybercrimeverdrag tekenden zou het nog tot 3 augustus 2012 duren voordat het verdrag ook werd geratificeerd (Kerkhofs & Van Linthout, 2013, p. 21). De regering heeft in 2012 een aantal voorbehouden geformuleerd alsmede een aantal verklaringen gedaan. Deze hadden betrekking op de rechtsmacht die door de lidstaten dient te worden gevestigd ten aanzien van de door het verdrag strafbaar gestelde feiten in art. 22. Het gaat om de restrictievere Belgische benadering van de strafbaarstelling van interne *hacking* en valsheid in informatica, die enkel strafbaar worden gesteld wanneer zij

[15] Richtlijn van het Europese Parlement en de Commissie nr. 2016/1148 van 6 juli 2016, *concerning measures for a high common level of security of network and information systems across the Union,* Pb.L. 19 juli 2016, L 194/2.

gepleegd worden met bedrieglijke opzet of met het oogmerk om te schaden (Kerkhofs & Van Linthout, 2013, p. 53).

Daarvoor heeft België wel met de wet van 28 november 2000 inzake de informaticacriminaliteit[16] dat in werking trad op 13 februari 2001 het Cybercrimeverdrag al voortijdig voorzien en omgezet in Belgisch recht. Op 3 februari 2001 werd de wet gepubliceerd in het Belgisch Staatsblad[17]. Tot die tijd liep het land achter in vergelijking met andere West-Europese landen (Van Eecke & Dumortier, 2003, p. 123). De wet heeft betrekking op informaticasystemen en hanteert de volgende definitie:

> "Elk systeem voor opslag, verwerking of overdracht van data (computers, chipkaarten e.d., maar ook netwerken en delen daarvan, evenals telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT)."[18]

Door die wet ontstonden nieuwe misdrijven met juridische draagwijdte: de valsheid in informatica, het informaticabedrog de interne en externe *hacking* en de datasabotage (Kerkhofs & Van Linthout, 2010, p. 179). Daarnaast kwamen een aantal nieuwe procesrechtelijke bepalingen die het de autoriteiten mogelijk maakten om onderzoeken te verrichten, zoals databeslag,[19] netwerkzoeking,[20] medewerkingsplicht[21] en bewaringsplicht[22] (Van Eecke & Dumortier, 2003, p. 123; Kerkhofs & Van Linthout, Cybercrime, 2013, p. 34). De wet maakt een onderscheid tussen informatica als middel en als doel om cybercriminaliteit te plegen.[23] Informatica als doel van criminaliteit houdt in dat de informatica zowel het instrument als het doel is (Leukefeldt, et al., 2012, p. 8). Dit zijn delicten die specifiek een inbreuk plegen op de vertrouwelijkheid, integriteit en beschikbaarheid van het informaticasysteem (Kerkhofs & Van Linthout, 2013, p. 36). Hieronder vallen hacking en datasabotage.

Hacking staat in het Belgisch Strafwetboek omschreven als:

---

[16] Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001, 02909.
[17] Memorie van toelichting van het wetsontwerp inzake informaticacriminaliteit, *Gedr. St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001.
[18] Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 13 februari 2001, 2.909.
[19] Art. 39*bis* Sv van 8 juni 1867, *BS* 9 juni 1867.
[20] Art. 88*ter* Sv. van 8 juni 1867, *BS* 9 juni 1867.
[21] Art. 88*quater* Sv. van 8 juni 1867, *BS* 9 juni 1867.
[22] Art. 109*ter E* Sv. van 8 juni 1867, *BS* 9 juni 1867
[23] Memorie van toelichting bij het wetsontwerp inzake informaticacriminaliteit, Parl.St. Kamer 1999-2000, nr. 0213/001 en nr. 0124/001.

> "Iemand die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft."[24]

Hierbij kunnen zowel mensen die intern aan de organisatie verbonden zijn als externen toegangsbevoegdheden schaden voor eigen belang (Kerkhofs & Van Linthout, 2013, p. 84).

Informaticasabotage staat in het Belgisch Strafwetboek omschreven als:

> "Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert."[25]

Dit artikel stelt elke kwaadwillige manipulatie van gegevens strafbaar (Kerkhofs & Van Linthout, 2010, p. 188). Hierbij zou gedacht kunnen worden aan de ontwikkeling en de verspreiding van schadelijke gegevens en computerprogramma's zoals virussen.[26]

Informatica als middel houdt in dat informatiedragers zoals laptops gebruikt worden om een misdrijf te kunnen plegen. De informatica is geen doelwit maar is nodig voor de uitvoering (Leukefeldt, et al., 2012, p. 8). Hieronder vallen informaticabedrog en valsheid in informatica.

Informaticabedrog staat in het Belgisch Strafwetboek omschreven als:

> "Iemand die, met bedrieglijk opzet, tracht om een onrechtmatig economisch voordeel voor zichtzelf of voor een ander te verwerven, door gegevens die worden opgeslagen, verwerkt of overgedragen, door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de gegevens in een informaticasysteem te veranderen."[27]

Het gebruik van een gestolen bankkaart of het vervalsen van studieresultaten door binnen te dringen in het informatiesysteem van een school zijn hier voorbeelden van (Leukefeldt, et al., 2012, p. 8)

Valsheid in informatica staat in het Belgisch Strafwetboek omschreven als:

---

[24] Art. 550*bis* Sr. van 8 juni 1867, BS 9 juni 1867.
[25] Art. 550*ter* §1 Sr. van 8 juni 1867, *BS* 9 juni 1867.
[26] Memorie van toelichting van het wetsontwerp inzake informaticacriminaliteit, *Gedr. St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 8.
[27] Art. 504quater §1 Sr. van 8 juni 1867, *BS* 9 juni 1867.

> "Iemand die gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert."[28]

Het vervalsen of namaken van digitale contracten of kredietkaarten zijn hier voorbeelden van.[29] Deze zouden ook strafbaar kunnen zijn als een ander gemeenrechtelijk misdrijf. (Kerkhofs & Van Linthout, 2013, p. 36)

Ook traditionele misdrijven waarbij de computer wordt gebruikt, de computer-relevante delicten, zoals de verspreiding van illegale pornografie[30], aanranding van de eer of de goede naam van personen[31], racistische uitingen[32] zijn strafbaar. Deze staan in het wetboek niet uitdrukkelijk omschreven als soorten van cybercriminaliteit maar hierbij gaat de wetgever ervan uit dat bijvoorbeeld goederen, bedrog of beledigingen ook digitaal in *cyberspace* kunnen plaatsvinden.

2.2.2 Nederland

Ook Nederland kent een onderverdeling van het Wetboek van Strafrecht (Sr.) en het Wetboek van Strafvordering (Sv). In het Sr. zijn de algemene bepalingen, overtredingen en misdrijven opgenomen, ook wel het materieel strafrecht genoemd. In Sv. staan de procedurele regels, ook wel het formele strafrecht. Samen vormen zij de basis van het Nederlands strafrecht. Hierin is de Wet computercriminaliteit opgenomen (Koops, 2010, pp. 596-597).

In 1985 is de Commissie computercriminaliteit opgericht wat leidde tot een uitgebreid rapport dat in 1987 is gepresenteerd. Naar aanleiding van dat rapport werd in 1993 Nederland

[28] Art. 210*bis* §1 Sr. van 8 juni 1867, *BS* 9 juni 1867.
[29] Memorie van toelichting van het wetsontwerp inzake informaticacriminaliteit, *Gedr. St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001, 14.
[30] Art. 383 Sr; Art. 383bis Sr; Art. 386 Sr; Art. 386bis Sr. van 8 juni 1867, *BS* 9 juni 1867
[31] Art. 443 Sr; Art. 444 Sr. van 8 juni 1867, *BS* 9 juni 1867
[32] Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, *BS*, 8 augustus 1981. Gewijzigd op *BS* 12 april 1994, *MB* 7 mei 1999, *BS* 25 februari 2003 *MB* 10 mei 2007, *BS* 17 augustus 2013, en op *BS* 21 december 2018.

de Wet computercriminaliteit ingevoerd[33], die behalve strafbaarstelling van de belangrijkste vormen van cybercriminaliteit ook gerelateerde opsporingsbevoegdheden bevatte (Koops, 2012, p. 12). Toen het Cybercrimeverdrag eenmaal moest worden geïmplementeerd ontstond daaruit de Wet computercriminaliteit II (Koops, 2010, p. 597). Die nationale wet is sinds 2006 van kracht[34] en bevat een uitbreiding ten opzichte van de eerdere wet in beide Wetboeken. Zo werd bijvoorbeeld de definitie van hacken uitgebreid door te stellen dat er ook sprake is van computervredebreuk zonder dat daarbij beveiliging wordt doorbroken (Custers, 2018, p. 103). In die wet is ook het kaderbesluit van de EU over aanvallen op informatiesystemen[35] opgenomen.

Een jaar later is ook het Cybercrimeverdrag in werking getreden (Koops, 2010, p. 598). Op 1 maart 2019 is de wet computercriminaliteit III inwerking getreden (Rijksoverheid, 2019) die in juni 2018 is aangenomen naar aanleiding van het in 2015 ingediende wetsvoorstel[36] (Custers, 2018, p. 104). Deze nieuwe wet dient ervoor om de nieuwe ontwikkelingen adequaat te kunnen aanpakken via het strafrecht en het strafprocesrecht. Zo kwamen er een aantal nieuwe procesrechtelijke bepalingen bij die de autoriteiten bevoegdheden geven die het hen mogelijk maken om onderzoek te verrichten. Opsporingsinstanties lopen aan tegen het gebruik van versleuteling van gegevens, de draadloze netwerken en *cloudcomputing*-diensten.[37] Versleuteling voorkomt dat opsporingsdiensten de internettap effectief kunnen inzetten bij die netwerken en diensten (Custers, 2018, p. 105). De hackbevoegdheid[38] uit de nieuwe wet, die kan worden ingezet in uitzonderlijke gevallen vanwege privacyoverwegingen, zorgt ervoor dat dit probleem wordt gereduceerd (Oerlemans, 2017, p. 354).

De wet geeft een definitie van wat als data kan worden beschouwd, uitgedrukt als ‘gegevens’:

[33] Kamerstukken II, 1989/90, 21 551 (MvT), nr. 1-3.; Wet Computercriminaliteit, *Stb*. 1993, 33.
[34] Rijkswet van 1 juni 2006 tot goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (*Trb*. 2002, 18). *Stb.* 2006, 299.
[35] Kaderbesluit 2005/222/JBZ van 24 februari 2005, *over aanvallen op informatiesystemen,* Pb.L. 16 maart 2005, L 69/67.
[36] Kamerstukken II, 2015/16, 34372 (MvT), nr. 2.
[37] Kamerstukken II, 2015/16, 34372 (MvT), nr. 3, p. 7-15.
[38] Art. 126nba Sv.

> "Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken."[39]

Ook geeft het een beschrijving van de term 'geautomatiseerd werk':

> "Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken."[40]

Deze 2 artikelen zijn opgenomen in de algemene bepalingen en geven betekenis aan sommige in het wetboek voorkomende uitdrukkingen.

In het wetboek wordt onderscheid gemaakt in verschillende soorten van cybercriminaliteit die in lijn zijn met de eerder genoemde typologieën, namelijk het gebruik van de computer als doel of als middel om cybercriminaliteit te plegen. Onder doel vallen misdrijven tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van geautomatiseerde processen (Koops, 2010, pp. 598-612). Daaronder vallen hacken, DDoS of andere soortgelijke aanvallen, illegaal aftappen en vernietigen of beschadigen van data.

Hacken is gelijkgesteld aan huisvredebreuk[41] waarbij het opzettelijk en wederrechtelijk binnendringen van geautomatiseerd werk strafbaar is gesteld en staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
>
> a. door het doorbreken van een beveiliging,
> b. door een technische ingreep,
> c. met behulp van valse signalen of een valse sleutel, of
> d. door het aannemen van een valse hoedanigheid."[42]

[39] Art. 80quinquies Sr.
[40] Art. 80sexies Sr.
[41] Art. 138 lid 1 Sr.
[42] Art. 138ab lid 1 Sr.

Hiervoor hoeven geen ingewikkelde methodes worden toegepast, ook het ongeoorloofd invoeren van iemands wachtwoord om in te *loggen* valt onder dit wetsartikel (Koops, 2010, p. 601).

DDoS of andere soortgelijke aanvallen staan omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden."[43]

Illegaal aftappen staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk."[44]

Vernietigen of beschadigen van data staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Hij die opzettelijk (of: aan wiens schuld te wijten is dat) enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft (…)."[45]

En:

> Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft (…)."[46]

[43] Art. 138b lid 1 Sr.
[44] Art. 139c lid 1 Sr.
[45] Art. 161sexies Sr (; Art. 161septies Sr).
[46] Art. 350a Sr.

In de Nederlandse wetgeving vallen, zoals verplicht gesteld door het Cybercrimeverdrag, onder computer als middel delicten valsheid met geschriften, gegevens en biomedische kenmerken en fraude, afpersing en afdreiging.

Valsheid met geschriften, gegevens en biomedische kenmerken staat omschreven als**:**

> "Hij die een geschrift dat bestemd is om tot bewijs van enig feit te dienen, valselijk opmaakt of vervalst, met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken, wordt als schuldig aan valsheid in geschrifte gestraft (…)."[47]

Opvallend is dat een computerbestand een 'geschrift' is wanneer het voldoende duurzaam, dus ergens opgeslagen is en als het leesbaar kan worden gemaakt (Koops, Cybercriminaliteit, 2014, p. 223).

Fraude (oplichting) staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft (…)."[48]

Afpersing staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "(Lid 1) Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door geweld of bedreiging met geweld iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt, als schuldig aan afpersing, gestraft (…).
>
> "(Lid 2) Met dezelfde straf wordt gestraft hij die de dwang, bedoeld in het eerste lid, uitoefent door de bedreiging dat gegevens die door middel van een geautomatiseerd

[47] Art. 225 lid1 Sr.
[48] Art. 326 lid 1 Sr.

werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist."[49]

Afdreiging staat omschreven in het Nederlandse Wetboek van Strafrecht als:

> "Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door bedreiging met smaad, smaadschrift of openbaring van een geheim iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt als schuldig aan afdreiging, gestraft (…)."[50]

Ook hier is niet altijd een specifieke omschrijving van cybercriminaliteit maar gaat de wetgever uit van dat goederen, diensten of gegevens digitaal kunnen zijn.

Ook traditionele misdrijven waarbij de computer wordt gebruikt als middel zijn gedekt. Zo is er data diefstal[51], identiteitsdiefstal[52], misdrijven tegen de zeden[53] en uitingen van racisme[54] (Koops, 2010, pp. 607-611; Koops, 2014, p. 215). Deze staan wederom niet specifiek in het wetboek omschreven als soorten van cybercriminaliteit maar hierbij gaat de wetgever ervan uit dat bijvoorbeeld goederen, bedrog ook digitaal in *cyberspace* kunnen plaatsvinden.

Hoofdstuk 3. Cyberveiligheid in organisaties

Dit hoofdstuk begint met een definitie en uiteenzetting van cyberveiligheid. Daarna volgt een beschrijving van wat een effectief cyberveiligheidsbeleid behelst. Daarna volgt er een korte beschrijving van de rol van de overheid en wordt er afgesloten met wat er bekend is over cyberveiligheid bij gemeenten.

[49] Art. 317 lid 1 en 2 Sr.
[50] Art. 318 lid 1 Sr.
[51] Rechtbank Leeuwarden 21 Oktober 2008, LJN BG0939; Gerechtshof Leeuwarden 10 November 2009, LJN BK27764 en BK2773; Rechtbank Amsterdam 2 April 2009, LJN BH9789, BH9790, en BH9791.
[52] Dit is strafbaar onder verschillende andere feiten zoals fraude, diefstal of namaak (Koops, 2010, p. 609).
[53] Art. 240b Sr.
[54] Art 137c Sr.

3.1 Definiëring cyberveiligheid

Ondanks dat er veel minder literatuur te vinden is over cyberveiligheid dan over cybercriminaliteit is het een term die aan populariteit wint. Cyberveiligheid wordt steeds meer gezien als van belang voor de hele samenleving en steeds meer landen houden zich er dan ook mee bezig. Dit wordt geformuleerd in strategisch militaire termen en met een focus op tegenmaatregelen zoals cyberaanvallen, cyberverdediging en cyberafweer. In de huidige discussies ligt er een focus op kritische infrastructuren aangezien de maatschappij daarvan afhankelijk is (Adams, et al., 2015, pp. 15-16). Van oudsher vatten criminologen veiligheid meestal op als een negatief begrip, het gaat dan om *on*veiligheid. Bijvoorbeeld in relatie tot criminaliteit of terrorisme. Hiermee gaat een bepaalde begeerte voor bestrijding samen (Schuilenburg & Van Steden, 2016, p. 3).

Zo ook voor cyberveiligheid, dat wordt gedefinieerd als de pro- en reactieve processen die in plaats zijn om bedreigingen te voorkomen die schade kunnen berokkenen aan vertrouwelijkheid, integriteit of beschikbaarheid van computers, netwerken en informatie (Adams, et al., 2015, p. 15). Dat is de wetenschappelijke definitie van cyberveiligheid dat voor dit onderzoek wordt gebruikt. Proactieve maatregelen bestaan daarbij uit preventieve en detective maatregelen. Cyberveiligheid is dan ook onlosmakelijk verbonden met cybercriminaliteit en is als het ware de tegenreactie erop. Die beschrijving van cyberveiligheid wordt ook gegeven door Bobbert & Broesma (2018, p. 15). Het gaat om de bescherming van de beschikbaarheid, de integriteit en vertrouwelijkheid van systemen en data. Dit wordt ook wel vaak aangeduid met de termen '*confidentiality, integrity and availability'* die afkomstig zijn van de *Central Intelligence Agency* (CIA) van de VS. Zij definiëren cyberveiligheid als "het reduceren van cyberrisico's tot een acceptabel niveau voor de organisatie" (Bobbert & Broersma, 2018, p. 20).

De begrippen informatieveiligheid en cyberveiligheid hangen sterk met elkaar samen. Sommige experts zien cyberveiligheid als een populaire term voor informatieveiligheid waar anderen een duidelijker onderscheid maken (Papelard & Bobbert, 2018, pp. 41-42). Zo wordt er door Bobbert & Broersma (2018, p. 17) wel een onderscheid gemaakt in informatieveiligheid en cyberveiligheid. Zoals de termen doen vermoeden gaat het ene over het beveiligen van informatie en het andere over het beveiligen van ook andere zaken en dus niet enkel informatie. Wanneer het gaat over beveiligen van digitale informatie dan wordt

ook wel de term ‘I(C)T-veiligheid’ gebruikt. Informatie veiligheid wordt gedefinieerd door de *Information Systems Audit and Control Association* (ISACA) als iets binnen een onderneming dat ervoor zorgt dat informatie wordt beschermd tegen de openbaring aan ongeautoriseerde gebruikers, onjuiste wijzingen, en gebrek aan toegang wanneer dat nodig is, ook wel *confidentiality, integrity and availability* genoemd (Papelard & Bobbert, 2018, p. 40). Deze omschrijving komt dus overeen met bovenstaande omschrijving zoals gegeven door de CIA.

Samenhangend met cyberveiligheid is de veelvoorkomende term *cyberressilience*, dat verder gaat dan alleen het beveiligen van processen. *Resilience* zou vertaald kunnen worden als ‘veerkrachtigheid’ van een organisatie. Die moet in staat zijn om verstorende cyberaanvallen op te sporen, zich ertegen te wapenen, er op te reageren en ervan te herstellen (Firth, Ayoub, & Nayaz, 2017, p. 5).

3.2 Effectief cyberveiligheidsbeleid

Net als cybercriminaliteit en cyberveiligheid wordt ook ‘beleid’ in de literatuur op verschillende manieren gedefinieerd. Voor dit onderzoek wordt de definitie van Hoogerwerf (2014, p. 17) aangehouden die ‘beleid’ omschrijft als “het streven naar het bereiken van bepaalde doeleinden met bepaalde middelen en bepaalde tijdskeuzes”. Beleid geeft een antwoord op een probleem, in dit geval cybercriminaliteit. Er zijn 2 grondstructuren die worden genoemd. Ten eerste de doeleinden, waarin wordt omschreven wat er bereikt moet worden. Ten tweede beleidsmiddelen die beschikbaar moeten zijn. Deze 2 moeten verbonden zijn aan een tijdskeuze, dat kan een bepaald tijdstip zijn of een bepaalde volgorde van handelingen (Hoogerwerf, 2014, pp. 17-18).

Om een handreiking te bieden aan beleidsmakers zijn er verschillende grote internationale raamwerken in cybersecurity die een methodologie bieden waarin de belangrijkste onderdelen van cyberveiligheid zijn opgenomen. De belangrijkste zijn: de *International Organisation for Standardization 27000* (ISO) normen, de *National Institute of Standards and Technologies* (NIST) *Risk Management Framework* (RFM) *and special publication 800-53*, de *Council on Cyber Security Critical Controls* en de *Certified Information Security System Professional* (CISSP) *Common Body of Knowledge* (CBK) (Donaldson, Siegel,

Williams, & Aslam, 2015, p. 29; Van Houten, Spruit, & Wolters, 2015, p. 149). Zo weten organisaties aan welke standaarden ze moeten voldoen.

De raamwerken hebben allemaal een andere focus, maar de hoofdlijnen zijn ongeveer hetzelfde. Ten eerste verdelen ze de organisatie en de bescherming ervan in verschillende functionele gebieden die een logische indeling volgen en helpen om het cyberveiligheidsbeleid in zijn geheel te managen. Ten tweede hebben ze allemaal een vorm van risicomanagement. Hierdoor kunnen organisaties de benodigde bescherming identificeren op basis van een objectieve risicoanalyse of evaluatie van de organisatieonderdelen en deze risico's vermijden. Ten derde hebben ze allemaal controles op veiligheid. Het doel hiervan is om de ernst van risico's te reduceren en om eventueel forensische data te verzamelen voor onderzoeken. Tot slot bieden deze raamwerken een mechanisme voor het controleren, evalueren en valideren van de aanwezigheid of afwezigheid van de controles die zijn omschreven in het raamwerk. Dit kan gedaan worden middels gedocumenteerde standaarden voor evaluatie of door audit checklists af te lopen.

De meeste raamwerken hebben een evaluatiemethode opgenomen als gids, of de methode spreekt voor zich en is welbekend. Dit zijn modellen die meten hoe het is gesteld met de huidige staat van de informatiebeveiliging op een schaal van 1 tot 5. Om op te schalen, dus een fase van groei in te gaan is eerst steeds een fase van crisis nodig (Papelard & Bobbert, 2018, pp. 58-60). Bij de levels gaat de houding van het management in gelijke stadia van onbezorgd, onbekend, ontluikend, beheerst tot professioneel. Pas vanaf het niveau van ontluikend waarin beveiligingsproblemen als relevant worden gezien met de noodzaak tot een specifieke aanpak heeft een organisatie voldoende bescherming (Van Houten, Spruit, & Wolters, 2015, p. 45) en kan het worden gezien als 'volwassen'.

Verschillende auteurs (Bennet & Stephens, 2014, p. 64; Wall, 2007, p. 187) stellen dat cybercriminaliteit wordt voorkomen door enerzijds het reduceren van de kwetsbaarheid van het doelwit, in dit geval het slachtoffer ofwel het computersysteem, en anderzijds het reduceren van de aantrekkelijkheid om het criminele gedrag uit te voeren. Deze theorie is direct afgeleid van de traditionele criminaliteitspreventie, namelijk de Routine Activiteiten Theorie. Meer concreet bestaat een effectief cyberveiligheidsbeleid volgens Donaldson, Siegel, Williams, & Aslam (2015, pp. 23-25) uit 4 verschillende onderdelen. Ten eerste is er is een beleid waarin alle maatregelen staan omschreven, ten tweede een programmatische en praktische uitwerking bestaande uit de inzet van mensen, budget en technologie. Ten derde

een IT-levenscyclus die bestaat uit strategie, aanpassingsvermogen en werking van IT-infrastructuur. Ten vierde zijn er beoordelingselementen. De beoordelingselementen dienen ter evaluatie van de effectiviteit van de risicomitigatie en de operationele processen. Hierin wordt tevens gerapporteerd wat de status is van de mate waarin het beleid voldoet aan wet- en regelgeving en internationale raamwerken of standaarden.

Al deze elementen moeten onderdeel zijn van een actieplan waarin alles goed samenwerkt en wat goed gecoördineerd moet worden. Als dit niet het geval is vallen kritische cyberveiligheidsonderdelen weg. Enkel beleid opzetten is dus niet genoeg. De technologie die wordt omschreven in het beleid moet worden geïmplementeerd anders zal het beleid niet effectief zijn. Op dezelfde manier moet daarna het operationele proces in orde zijn voor de werking en het behoud van de technologie nadat het is ingezet. Tot slot zal de status van de effectiviteit constant gemonitord moeten worden om bij te blijven met de snel veranderende dreigingen anders zal het opgestelde programma of beleid namelijk snel verouderen en zijn effectiviteit verliezen. Zo is de beleidscyclus weer rond. Dit alles moet gebeuren op een manier die kosteneffectief is. Er moet een balans zijn tussen technologie, processen, mensen, organisatie, budget en er moet voldaan worden aan wet- en regelgeving. (Donaldson, Siegel, Williams, & Aslam, 2015, p. 27).

Een ander essentieel onderdeel van hoe een organisatie de cyberveiligheid op orde houdt is volgens Paperland & Bobbert (2018, p. 44) *Business Information Security* wat bestaat uit 3 factoren. Ten eerste uit kosten die worden gemaakt door uitgestelde beslissingen. Ten tweede uit risico's die voortkomen uit uitgestelde handelingen/acties, omdat complexiteit handelen bemoeilijkt. Ten derde kan die complexiteit er ook voor zorgen dat de verkeerde beslissingen worden genomen. De impact van deze 3 factoren kan dramatisch zijn. Daarom is het zo van belang deze beslissingen juist en tijdig te maken om zo strategisch voordeel te hebben en de toekomst van de organisatie veilig te stellen. De 'kritische succes factor' is hierin essentieel. Dit is een samenkomst van een beperkt aantal vitale gebieden waarin bevredigend resultaat prestatie verzekert voor een organisatie. De organisatie moet bepalen welke onderdelen absoluut nodig zijn voor de bedrijfsvoering en die veiligstellen in geval van nood. Dit kan een cyberaanval zijn maar ook een brand die uitbreekt en daardoor de hardware vernietigd.

Van Houten, Spruit en Wolters (2015, p. 94) beschrijven verder hoe de menselijke factor een essentieel onderdeel is in cyberveiligheid. Veel beveiligingsincidenten zijn het gevolg van

fouten die mensen maken, omdat bedrijfsprocessen niet foutresistent zijn ingericht. Die fouten kunnen bewust of onbewust plaatsvinden. Een deel van die fouten kan voorkomen worden door beleid te creëren dat daarop inspeelt. Dit kan variëren van programma's opzetten die het minder mogelijk maken om fouten te maken tot bewustwordingscampagnes over hoe die fouten voorkomen kunnen worden. Bewuste fouten kunnen leiden tot misbruik en cybercriminaliteit.

Er zijn verschillende manieren waarop de cyberveiligheid in de praktijk kan worden verhoogd. Beveiligingsmaatregelen zijn gericht op een bepaald moment in de incident cyclus, dat wil zeggen wanneer een incident zich voordoet. Die cyclus bestaat uit 4 stappen; ten eerste is er een bedreiging, dan volgt een incident of verstoring, die resulteert in schade en tot slot is er het herstel. Eventueel volgt er een evaluatie. De maatregelen kunnen vervolgens worden onderverdeeld in preventieve, detective, repressieve en correctieve maatregelen. Preventieve en detective maatregelen vinden plaats om een incident op te sporen en te voorkomen, zoals een *malware* scanner. Repressieve en correctieve maatregelen zijn reactief en vinden plaats nadat een incident is voorgekomen. Hierbij kan gedacht worden aan het isoleren van een systeem na een infectie waarna een *back-up* wordt teruggezet (Van Houten, Spruit, & Wolters, 2015, pp. 31-34).

Ook kan een onderscheid gemaakt worden in beveiligingsmaatregelen op basis van de wijze waarop ze geïmplementeerd worden. Zo zijn er organisatorische maatregelen die betrekking hebben op de organisatie, de mensen en de procedures. Een voorbeeld hiervan is het toekennen van functieonderscheidingen en interne controle om fraude te voorkomen. Daarnaast zijn er logische maatregelen die zijn opgenomen in de programmatuur zoals wachtwoordauthenticatie of encryptie in besturingssystemen en applicaties. Tot slot zijn er fysieke maatregelen zoals een noodstroomvoorziening die voorkomt dat kritieke processen uitvallen (Van Houten, Spruit, & Wolters, 2015, pp. 35-36; Bennet & Stephens, 2014, pp. 70-79). Al deze manieren zijn vormen van risicomanagement. Om voor al die factoren een beleidsstrategie op te stellen en managen werken organisaties veelal met een *Chief Information Security Officer* (CISO). Deze rol is geëvolueerd van een puur technische naar een strategische waar een organisatie zelden nog maar zonder kan (Papelard & Bobbert, 2018, p. 54).

Om cyberveiligheid meer onder de aandacht te brengen heeft de Belgische organisatie *The Cyber Security Coalition* (2016) een gids uitgebracht. Daarin schetsten zij een beeld hoe

organisaties zich kunnen beschermen tegen cybercriminaliteit. Zo zou er bijvoorbeeld een 'incidentresponsplan' opgesteld kunnen worden waarin wordt omschreven wat er beveiligd moeten worden, wie hier verantwoordelijk voor is, hoe de schade beperkt kan worden en de manier waarop er wordt gecommuniceerd. Ook zou een cyberverzekering afgesloten kunnen worden om de schade te dekken die kan oplopen tot honderdduizenden of zelfs miljoenen euro's (The Cyber Security Coalition, 2016, p. 3).

3.3 Cyberveiligheidsbeleid bij de overheid

Om overheidsbeleid te kunnen creëren moet er voldoende erkenning zijn voor het probleem, moet er een beleidsmatig oplossing zijn en moet er voldoende politieke steun voor die oplossing zijn (Hoogerwerf, 2014, p. 58). Deze elementen zijn aanwezig in Europa, België en Nederland. Zo is er in Europa de *European Union Agency for Network and Information Security* (ENISA) dat zich opstelt als centrum van expertise voor cyberveiligheid. Het heeft een nauwe samenwerking met lidstaten van de EU waarbij het advies geeft, helpt met opstellen van beleid en operationeel meewerkt met lokale teams (ENISA, 2019). ENISA brengt op regelmatige basis rapporten en gidsen uit die vrij toegankelijk zijn op de website over de huidige staat van cybercriminaliteit en cyberveiligheid in Europa. Het European Cybercrime Centre dient als het Europese cybercriminaliteit-platform waarbij het inlichtingen verzamelt en cybercriminaliteit bestrijdt. Op het gebied van cyberafweer is er de *European Defence Agency* (EDA) die helpt om capaciteiten van lidstaten te ontwikkelen en vergroten (RAND Europe, 2015, p. 14). Deze Europese organisaties richten zich niet op lagere bestuurslagen zoals lokale overheden. Adams et al. (2015, p. 15) beschrijven hoe cyberveiligheid wordt toegepast bij nationale overheden. Veel van hen hebben *National Cybersecurity Strategies* (NCSs).

In België heeft het CCB voor verschillende sectoren richtlijnen opgesteld. Voor de overheid is er de *Baseline Security Guidelines* (BSG) waarin de minimale richtlijnen, gebaseerd op de ISO-normen, voor de implementatie en evaluatie van informatiebeveiliging zijn verwerkt (CCB, 2019). De operationele dienst van de organisatie is de federale *Computer Emergency Response Team* (CERT) die als opdracht het opsporen, het observeren en het analyseren van online veiligheidsproblemen en het permanent informeren daarover heeft (CERT, 2019). Verder is de Vereniging van Vlaamse Steden en Gemeente (VVSG) een overkoepelende

organisatie die onder andere Vlaamse gemeenten ondersteund met het verhogen van de kwaliteit van de lokale beleidsvoering (VVSG, 2019). Daarnaast kunnen lokale bestuurders lid worden van de Vlaamse ICT-Organisatie (V-ICT-OR) dat een platform biedt voor kennisuitwisseling en andere vormen van samenwerking (V-ICT-OR, 2019). Die organisatie heeft een *tool* opgezet waarmee gemeenten een op maat gemaakte risicoanalyse, volwassenheidsmeting en veiligheidsplan kunnen uitwerken (V-ICT-OR, 2019).

Het NCSC moet de cyberveiligheid verhogen in Nederland (Rijksoverheid, 2018). In de Nederlandse Cybersecurity Agenda (NCSA) zijn de doelen en maatregelen opgenomen die de overheid heeft vastgelegd voor publieke en private partijen (Rijksoverheid, 2018). Het NCSC werkt samen met het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) en het onafhankelijke Centrum voor Criminaliteitspreventie en Veiligheid (CCV) op de onderwerpen cybercriminaliteit en cyberveiligheid (CCV, 2019; WODC, 2019). Voor de gemeenten heeft de Vereniging Nederlandse Gemeenten (VNG) met als uitvoerende/operationele organisatie de IBD, dat de sectorale CERT is voor gemeenten in Nederland, de Baseline Informatie Gemeente (BIG) opgesteld (VNG, 2019). Deze wordt vanaf 1 januari 2020 vervangen door de Baseline Informatie Overheid (BIO) en is net als in België gebaseerd op de ISO-normen (IBD, 2019). De VNG heeft samen met een aantal ministeries de *tool* Eenduidige Normatiek Single Information Audit (ENSIA), opgezet waarmee gemeenten een eenmalige IT-audit kunnen uitvoeren aan het eind van de planning en control-cyclus. ENSIA kan zo helpen horizontale verantwoording af te leggen aan de gemeenteraad (VNG, 2019).

Uit het ‘Cybersecuritybeeld Nederland 2018’ van de NCTV (2018, pp. 9-39) blijkt dat de digitale weerbaarheid van Nederland onder permanente druk staat en dat cyberaanvallen met eenvoudige methoden succesvol worden uitgevoerd. Uit de dreigingsmatrix blijkt dat de overheid vooral risico loopt op spionage of informatiemanipulatie van andere overheden en verstoringen door criminelen. Omdat Nederland een ICT-intensieve economie is liggen de belangen voor de nationale digitale veiligheid erg hoog. Vitale processen zijn gedigitaliseerd en analoge alternatieven ontbreken waardoor de stabiliteit in het land sterk ontwricht kan raken. Daarom is het van het uiterste belang dat organisaties de basismaatregelen op orde hebben, afgestemd op hun specifieke behoeften.

3.4 Cyberveiligheid bij gemeenten

Zoals eerder benoemd zijn beleidsdocumenten over cyberveiligheid van en/of over gemeenten zelf, zoals de BSG en de BIG, niet inhoudelijk opgenomen in de literatuurstudie maar worden bestudeerd in de documentenanalyse. Daarom gaat dit deel enkel in op wetenschappelijke onderzoeken. Wetenschappelijke literatuur over cyberveiligheid bij gemeenten richt zich vrijwel uitsluitend op de VS. Daar lijkt het belang van cyberveiligheid op lokaal niveau beter te zijn doordrongen. Echter is ook die literatuur beperkt en is de focus ervan vaak niet helemaal hetzelfde als in dit onderzoek. Hieronder volgt een overzicht.

Macmanus, Caruson, & Mcphee (2016) laten een belangrijk punt zien in hun onderzoek. Lokale overheden hebben vaak grote hoeveelheden privacygevoelige informatie opgeslagen. Dit conflicteert vaak met de verwachting dat de overheid ook transparant moet zijn. Des te meer reden om het vertrouwen in de overheid te waarborgen. Echter blijk ook uit hun onderzoek naar lokale overheden in Florida dat de balans tussen transparantie tegenover privacy en de daarbij behorende cyberveiligheid lastig voor ze is. Het garanderen van een veilige betrouwbare overheid terwijl cyberaanvallen en dus risico's op datalekken toenemen én tegelijkertijd ook transparant blijven is voor veel lokale overheden erg lastig. Hiervoor zijn duidelijke standaarden nodig voor cyberveiligheid, betere trainingen, betere software, meer personeel en betere *oversight* (Macmanus, Caruson, & Mcphee, 2016, p. 466).

Het bij cybercriminaliteit eerder genoemde onderzoek van Norris & Mateczun (2017, p. 3) stelt vast dat gemiddeld genomen de meeste lokale overheden onvoldoende maatregelen nemen om een voldoende mate van cyberveiligheid te garanderen. De belangrijkste reden hiervoor is dat ze onvoldoende financiële middelen hebben om te kunnen concurreren met salarissen van bedrijven. Dit heeft als gevolg dat er onvoldoende gekwalificeerd personeel aanwezig is om deze taken op te pakken. Ook Tully (2018, pp. 9-10) noemt hierbij dat het lastig is, omdat er te weinig experts zijn op het gebied van cyberveiligheid om aan de vraag te voldoen en dat lokale overheden vaak niet voldoende budget hebben om de juiste mensen aan te trekken. Dit vraagt om een verandering op bestuurlijk niveau, met cyberveiligheid hoog op de (politieke) agenda zodat er meer middelen en essentiële maatregelen beschikbaar komen zodat een goed beleid kan worden opgesteld en worden uitgevoerd (Norris & Mateczun, 2017, pp. 5-6).

White (2017) gaat ook in op hoe gemeenten in de VS onder toenemende druk staan om hun cyberveiligheid op orde te brengen. We zijn afhankelijk geworden van onze IT-systemen die een onmisbaar onderdeel uitmaken van kritische IT-structuren (White, 2017, p. 52). Hierbij onderstreept White ook het belang van het nemen van fysieke maatregelen om bepaalde plekken, zoals overheidsgebouwen, te beschermen. Dit kan gedaan worden door toegangsbeleid te creëren, waarbij niet zomaar iedereen wordt binnengelaten. Ook het afgeschermd houden van data, zoals computers die niet onbeheerd en onbeveiligd worden achtergelaten zijn vormen van fysieke bescherming die een gemeente kan nemen. Volgens White kunnen gemeenten verschillende andere dingen om hun cyberveiligheid te vergroten. Zo kunnen ze additioneel beleid en regelgeving ontwikkelen om veilig te werken, denk hierbij aan werken buiten kantoor, maar zich bijvoorbeeld ook richten op publiek-private samenwerkingen.

Nussbaum & Park (2018, pp. 3-5) wijzen er op dat lokale overheden moeten oppassen met het uitbesteden van cyberveiligheid aan externe partijen. Zij benoemen dat dit vaak wordt gedaan vanwege het complexe veld dat cyberveiligheid behelst, waarbij het niet alleen gaat om het hebben van voldoende gekwalificeerd personeel en/of budget maar ook het hebben van de juist apparatuur. Hierbij moet vooral gelet worden op de kwaliteitseisen die worden gesteld in contracten en het evalueren van de werkzaamheden wanneer eenmaal is uitbesteed.

De Vlaamse overheid heeft in een recent rapport genaamd ‘Thema-audit Informatiebeveiliging’ (hierna: Audit-rapport Vlaanderen) vastgesteld dat lokale overheden, waaronder verschillende gemeenten, hun vertrouwelijke en (persoons)gevoelige informatie onvoldoende beveiligen (Audit Vlaanderen, 2018, pp. 5-7). Omdat dit document is meegenomen in de documentenanalyse wordt hier verder niet op ingegaan. Voor Nederlandse gemeenten is het volgens de VNG & CCV (2017, p. 2) van belang om de gemeentelijke en regionale systemen en digitale dienstverleningen te beschermen tegen hacken, cyberaanvallen en datalekken. Verder moeten het veiligheidsbewustzijn worden opgebouwd en tot slot moet er een vlotte incident detectie en coördinatie plaatsvinden. Dit document is echter zo summier dat het uit de analyse is gelaten.

Er is vrijwel geen wetenschappelijke literatuur te vinden over cyberveiligheid bij gemeenten in België en Nederland. Veel wetenschappelijke literatuur gericht op België en Nederland gaat niet verder dan cyberveiligheid op nationaal niveau. Eerdergenoemd onderzoek van

Paoli et al. (2018) over 2 Vlaamse gemeenten gaat wel in op cyberveiligheid. Voor de eerste stad is het belang van cyberveiligheid iets wat steeds beter wordt onderkend. Er is zelfs een eigen IT-organisatie/*serviceprovider* ontstaan vanuit de voormalige IT-afdeling. Die organisatie maakt op zijn beurt wel weer gebruik van externe expertise. De *serviceprovider* zorgt voor maatregelen zoals een spamfilter, *back-ups, firewalls*, antivirussoftware en zorgt ook voor de uitgifte van mobiele apparaten. De werknemers van de gemeente zelf krijgen geen additionele cyberveiligheidstrainingen, dat is alleen voorbehouden aan de werknemers van de *serviceprovider*. De tweede stad maakt ook gebruik van een *serviceprovider* die formeel geen onderdeel is van de gemeente, dus een compleet externe partij, maar in de praktijk wel. Daarnaast hebben ze ook eigen IT-experts. Ook deze gemeente maakt gebruik van verschillende maatregelen, zoals antivirussoftware, die worden bepaald door een bepaald risico. De software en digitale infrastructuur worden verder regelmatig getest op zwakheden.

In Nederland ontbreekt zulk onderzoek. Wat er wel is gaat over kritische infrastructuren. Van der Meulen (2015) heeft onderzoek gedaan naar kritische infrastructuren in Nederland en hoe zij hun cyber/informatieveiligheid hebben ingericht. Daaronder vallen zaken zoals energie, drinkwatervoorzieningen, financiële dienstverleners en ook overheden. Haar conclusies zijn dat organisaties bang zijn voor reputatieschade, waarbij ze opmerkt dat dit een gevolg is van een incident. Om de schade daarvan te beperken is het dus van belang dat incidenten zoveel mogelijk worden voorkomen. Echter zijn incidenten de sterkste motivatie voor cyberveiligheidsmaatregelen en niet zozeer wet- en regelgeving zoals de *Network and Information Security Directive (*NIS-*Directive)* (Van der Meulen, 2015, pp. iv-v). Verder merkt ze op dat het ontbreekt aan data die duidelijk maakt hoeveel er wordt geïnvesteerd in cyberveiligheidsmaatregelen bij de kritische infrastructuren. Het meten van die investeringen wordt bemoeilijkt door het ontbreken van een eenduidige definitie voor cybercriminaliteit, er geen modellen zijn om mee te meten, cyberveiligheid verweven is in producten, processen en projecten en cyberveiligheid voornamelijk vanuit een kwalitatief perspectief wordt benaderd (Van der Meulen, 2015, p. 51). Deze conclusies zijn zonder meer ook toepasselijk op gemeentelijke organisaties.

Van Erp (2017) schrijft over cyberveiligheid in de haven van Rotterdam, waarbij het Havenbedrijf een (verzelfstandigd) onderdeel is van de gemeente (Port of Rotterdam, 2019). Buiten het Havenbedrijf zijn er veel andere bedrijven en organisaties actief zoals rederijen of de douane. De haven is een kritische infrastructuur die extra goed beschermd moet worden

vanwege de gevolgen die een ontregelende cyberaanval kan hebben. In de haven werken publieke en private actoren samen, niet alleen om de goederen te verwerken maar ook om de haven (digitaal) veilig te houden. Van de bedrijven in de haven wordt verwacht dat ze hun verantwoordelijkheid nemen in de bedrijfsvoering met veiligheid als essentieel onderdeel van het werk. Toch is er overheidsregulering voor nodig om normen en standaarden te bepalen (Van Erp, 2017, pp. 81-82). Dit is nodig om de risico's, die niet altijd helder voor ogen liggen bij het management, zo veel mogelijk te mitigeren (Van Erp, 2017, p. 90).

Besluit

In deel A is de bestaande literatuur, wetgeving en beleid op het gebied van cybercriminaliteit en cyberveiligheid uiteengezet. Belangrijk hierbij is dat het cyberdomein vele verschillende aspecten omvat en dus erg breed is. Zo is er ook geen eenduidige definitie van deze begrippen. De wetenschappelijke definitie van cybercriminaliteit dat voor dit onderzoek wordt gebruikt is: "Cybercriminaliteit is alle vormen criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict" (Leukefeldt, Domenie, & Stol, 2009, p. 2). Cyberveiligheid wordt in dit onderzoek gedefinieerd als de pro- en reactieve processen die in plaats zijn om bedreigingen te voorkomen die schade kunnen vormen voor vertrouwelijkheid, integriteit of beschikbaarheid van computers, netwerken en informatie (Adams, et al., 2015, p. 15). België en Nederland hebben allebei het Cybercrimeverdrag, dat gezien kan worden als de belangrijkste internationale wetgeving geïmplementeerd in nationale wetgevingen. Hierdoor zijn cyberdelicten strafbaar gesteld in beide landen.

Het cyberdomein is daarnaast ook aan snelle veranderingen onderhevig, waarbij het onderzoeksveld ook relatief nieuw is. Dit maakt het een lastig onderwerp om te onderzoeken, des te meer omdat de literatuur over hoe gemeenten in België en Nederland specifiek omgaan met cybercriminaliteit en cyberveiligheid zeer beperkt is. Dit gegeven onderstreept het belang van dit onderzoek. Door te richten op literatuur en beleidsdocumenten die breder zijn, zowel qua onderwerp als qua locatie is toch gepoogd het veld zo goed mogelijk in kaart te brengen. Zo is er beleidsmatig gekeken naar wat de België en Nederland doen op nationaal niveau om de cyberveiligheid te vergroten en hoe dit kan gelinkt worden naar regionaal niveau. De VVSG en VNG spelen daarbij een rol, waarbij ze gemeenten helpen met het uitvoeren van het beleid.

In de VS lijkt de dreiging van cybercriminaliteit en het belang van cyberveiligheid beter te zijn doordrongen en zijn er enkele wetenschappelijke onderzoeken te vinden die deze kwetsbaarheden blootleggen. In België toont het onderzoek van Paoli et al. (2018) hetzelfde aan, namelijk dat de onderzochte gemeenten onvoldoende beschermd zijn. In Nederland blijkt uit onderzoek naar kritieke infrastructuren dat het onduidelijk is wat er precies wordt gedaan aan het waarborgen van de cyberveiligheid.

DEEL B: HET CONCEPTUEEL KADER EN DE ONDERZOEKSOPZET

Deel B bevat het conceptueel kader en de onderzoeksopzet. In hoofdstuk 4 komen de probleemstelling, onderzoeksvragen en het conceptueel kader aan bod. Dan volgt hoofdstuk 5 met een beschrijving van kwalitatief onderzoek en de verantwoording van methodologische keuzes. Vervolgens een beschrijving van de onderzoekseenheden, de contactopname en de respons. Daarna de dataverzameling en data-analyse. Tot slot sluit dit hoofdstuk af met de kwaliteit van het onderzoek inclusief de beperkingen van de onderzoeksmethode.

Hoofdstuk 4. Probleemstelling, onderzoeksvragen en conceptueel kader

In dit deel volgt de probleemstelling die wordt gepresenteerd samen met de volledige onderzoeksvragen en het conceptueel kader.

4.1 Probleemstelling en relevantie van het onderzoek

Hoewel zowel bedrijven, overheden, als onderzoekers zich al in beperkte mate bezighouden met cybercriminaliteit, blijkt de wetenschappelijke relevantie van dit onderzoek uit het gebrek aan literatuur naar hoe lokale overheden in België en Nederland, zoals gemeenten, omgaan met dreigingen van cybercriminaliteit en hoe ze de cyberveiligheid waarborgen met hun beleid. Een recent afgenomen survey onder ICT-*security managers* laat blijken dat ze moeite hebben met het controleren en beheersen van de risico's van cybercriminaliteit (Papelard & Bobbert, 2018, p. 31). Grote cyberaanvallen als die van de '*Stuxnet*-worm' die een nucleaire fabriek in Iran schade heeft toegebracht in 2009 laten zien dat het van belang is dat overheden cyberveiligheid serieus moeten nemen (Collins & McCombie, 2012; Porche, Sollinger, & McKay, 2011). Gemeenten mogen hierbij niet vergeten worden. Er wordt namelijk ook op gemeentelijk niveau dreiging ondervonden. Zo berichtte de New York Times recent dat Baltimore samen met andere steden over de gehele VS weken last hebben van een cyberaanval die duizenden computers heeft platgelegd. Hierdoor zijn allerlei diensten, zoals watervoorzieningen, plat komen te liggen (The New York Times, 2019).

Dichter bij huis is dezelfde dreiging aanwezig. Zo meldt de website 'Binnenlands Bestuur' (2017) dat de 3 Nederlandse gemeenten Blaricum, Eemnes en Laren in maart 2017 zijn getroffen door cyberaanvallen. Tevens is er ook in België ruimte voor verbetering. Zou zouden een op de 5 de gegevens van haar inwoners niet voldoende beschermen (De Morgen, 2017).

Het doel van dit onderzoek is het achterhalen met welke vormen van cybercriminaliteit verschillende gemeenten in België en Nederland geconfronteerd worden en hoe ze de interne cyberveiligheid binnen de eigen organisatie waarborgen met hun beleid. Daarvoor is er gekeken naar welke vormen van cybercriminaliteit zij te maken hebben en welke schade daaruit voortvloeit. Ook is er gefocust op de maatregelen die zij nemen in het kader van hun cyberveiligheidsbeleid. Beleidsrelevant onderzoek kan 2 verschillende doelen dienen. Enerzijds is dat het exploreren van een fenomeen of domein waar nog niet zo veel kennis over is. Anderzijds kan het bestaand beleid evalueren door de maatregelen te bestuderen (Mortelmans, 2013, p. 107). In dat laatste geval wordt met het onderzoek nagegaan of de doelstellingen van de maatregelen die zijn genomen gerealiseerd worden in de praktijk en kunnen ze aangepast worden waar dat nodig is (Mortelmans, 2013, p. 107). Dit onderzoek heeft dan ook een praktisch doel, namelijk een bijdrage leveren door te staven waar de verschillende gemeenten staan en kijken waar de verbeterpunten liggen om zo het beleid te optimaliseren**.** De resultaten van dit soort onderzoeken kunnen een belangrijke rol spelen met betrekking tot het vormen van een cyberveiligheidsbeleid voor de interne bedrijfsvoering bij gemeentelijke organisaties.

Al eerder is benoemd dat cybercriminaliteit een grensoverschrijdend fenomeen is. Om die reden is gekozen om een vergelijking te doen van 2 landen. De keuze voor België en Nederland ligt in de gemeenschappelijke taal (in Vlaanderen) en vergelijkbare westerse cultuur. Ze zijn allebei lid van de RvE, de EU en de Benelux. Daardoor laat een vergelijking zien hoe deze landen Europese wetgeving op verschillende wijze hebben geïmplementeerd naar de eigen nationale situatie. De Europese context brengt overeenkomsten met zich mee maar ook de verschillen zijn interessant om te onderzoeken. Door te focussen op 2verschillende landen zijn er duidelijkere verschillen naar voren gekomen in vergelijking met wanneer binnen één land zou worden gekeken, omdat de bevindingen niet op dezelfde manier tegenover elkaar uitgezet zouden kunnen worden. Op die manier kan men ook van elkaar leren. Daarnaast zijn er ook pragmatische redenen geweest. Door de geringe omvang

van beide landen is het onderzoeken van de verschillende gemeenten op locatie haalbaar met beperkte tijd en middelen.

4.2 Omschrijving van de onderzoeksvragen

De onderstaande hoofd- en deelonderzoeksvragen zijn geformuleerd voor dit onderzoek en hebben telkens betrekking op de verschillende gemeenten in België en Nederland. In de eerste onderzoeksvraag wordt getracht om in kaart te brengen welke vormen van cybercriminaliteit de gemeenten ondervinden en welke schade daaruit voortvloeit. Als logisch gevolg op de eerste vraag focust de tweede onderzoeksvraag zich op hoe de gemeente zich beschermen tegen deze vormen door middel van de maatregelen die ze hebben opgenomen in hun beleid. De laatste deelonderzoeksvraag van iedere hoofdonderzoeksvraag focust zich op de verschillen en overeenkomsten die naar voren komen in de cases. Dit gaat zowel om verschillen tussen de individuele cases, maar ook om overkoepelende verschillen die naar voren komen tussen de landen.

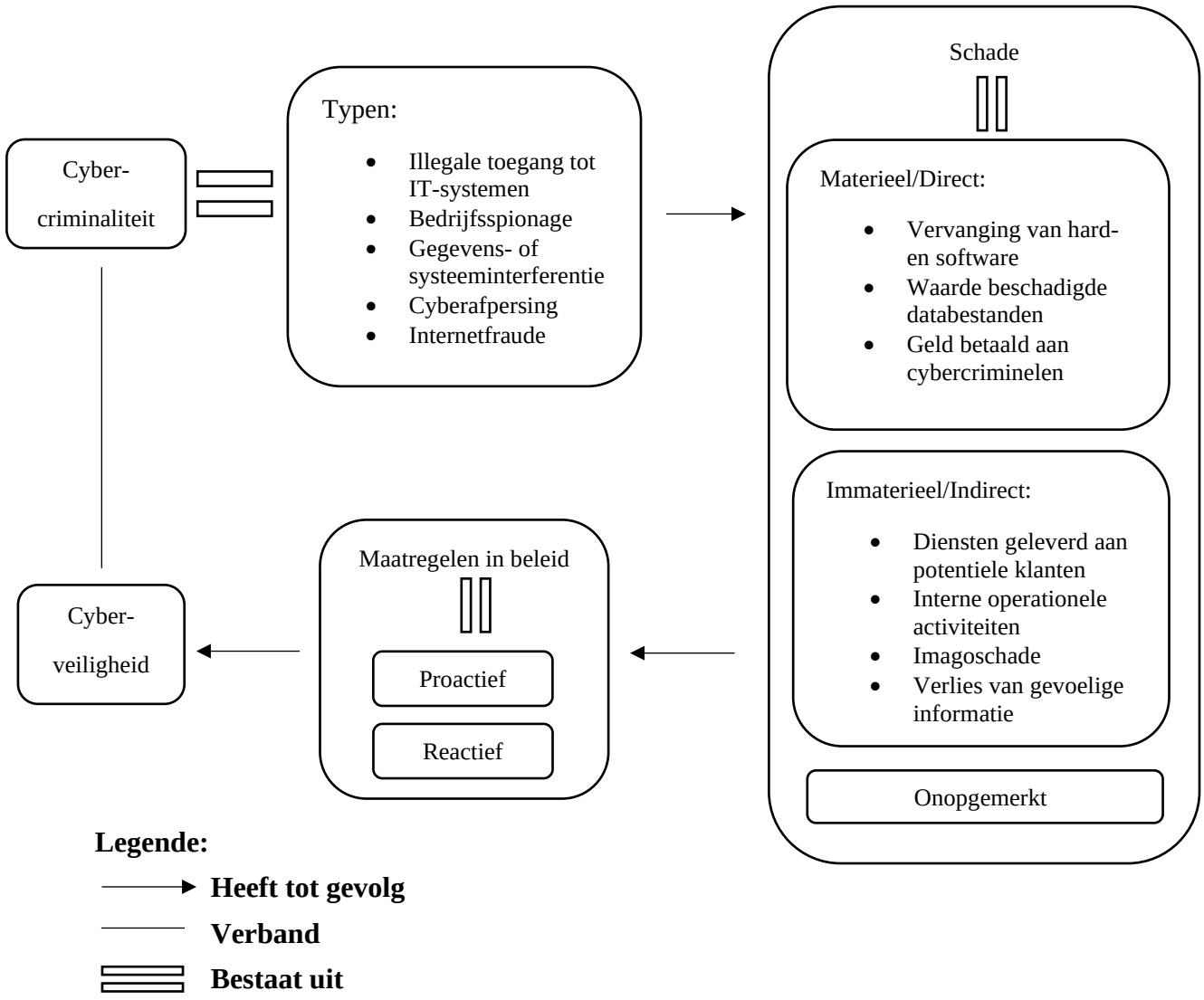
1. In welke mate worden de verschillende gemeenten geconfronteerd met cybercriminaliteit?
   1.1 Met welke vormen van cybercriminaliteit hebben zij te maken?
   1.2 Welke soorten schade vloeien voort uit cybercriminaliteit?
   1.3 Wat zijn de overeenkomsten en verschillen die naar voren komen in de cases?

2. Welke maatregelen nemen de gemeenten in het kader van hun cyberveiligheidsbeleid?
   2.1 Welke middelen hebben zij ter beschikking?
   2.2 Welke proactieve maatregelen nemen zij?
   2.3 Welke reactieve maatregelen nemen zij?
   2.4 Hoe doeltreffend zijn de maatregelen?
   2.5 Welke verbetermogelijkheden zijn er in het beleid?
   2.6 Wat zijn de overeenkomsten en verschillen die naar voren komen in de cases?

Alle onderzoeksvragen richten zich op de ervaringen van de beleidsmedewerkers en op de bevindingen uit de beleidsdocumenten. Dat wil zeggen dat de bevindingen subjectief kunnen zijn en er geen feitelijke weergave van de werkelijkheid wordt gegeven. De uitspraken van de respondenten zijn niet getoetst, maar wel aangevuld met de analyses van de beleidsdocumenten. Die documenten kunnen echter ook een vertekend beeld geven van de werkelijkheid, omdat organisaties ervoor kunnen kiezen een beperkt, rooskleurig, beeld op te tekenen voor de buitenwereld (Mortelmans, 2013, p. 206). Beyens & Tournel (2016, pp. 218-219) menen echter dat waarheidsvinding in onderzoek niet het hoogste goed is en niet nodig is. De beleving van de respondenten vindt zijn weerslag in de werkelijkheid. Uit de interviews en de beleidsdocumentenanalyse kunnen trends en categorieën worden onderscheiden die een waardevolle aanvulling kunnen zijn op dit vakgebied.

4.3 Conceptueel kader en visuele representatie

Om antwoord te kunnen geven op de onderzoeksvragen moet empirisch onderzoek worden uitgevoerd. Om dit toe te lichten is een visuele representatie van het conceptueel schema opgesteld die de onderzoeksvragen reflecteert. Een conceptueel schema is volgens Miles, Huberman en Saldaña (2014, p. 20) een grafische voorstelling van de hoofzaken die bestudeerd zullen worden en de relaties ertussen. De concepten zijn gevormd aan de hand van bestaande literatuur.



Figuur 1: visuele representatie conceptueel schema

Cybercriminaliteit en cyberveiligheid zijn de 2 hoofdthema's van dit onderzoek en deze begrippen hangen met elkaar samen. De wetenschappelijke definitie van cybercriminaliteit die voor dit onderzoek wordt gebruikt is: "Cybercriminaliteit is alle vormen criminaliteit waarbij ICT een wezenlijke rol speelt in de realisatie van het delict." (Leukefeldt, Domenie, & Stol, 2009, p. 2). Cybercriminaliteit bestaat uit 5 verschillende typen (Paoli et al., 2017, p. 31). Die 5 typen leiden tot directe, indirecte en onopgemerkte schade (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 7; Leukfeldt & Weulen Kranenbarg, 2017, p. 287; Wall, 2007, p. 20). Die schade voorkomen en herstellen leidt vervolgens tot proactieve en reactieve maatregelen opgenomen in het beleid tegen cybercriminaliteit en voor het

vergroten van cyberveiligheid (Adams, et al., 2015, p. 5). Cyberveiligheid wordt in dit onderzoek gedefinieerd als de pro- en reactieve processen die in plaats zijn om bedreigingen te voorkomen die schade kunnen vormen voor vertrouwelijkheid, integriteit of beschikbaarheid van computers, netwerken en informatie (Adams, et al., 2015, p. 15).

Hoofdstuk 5. Onderzoeksopzet

Dit hoofdstuk bevat een uiteenzetting over de kwalitatieve methodologie die is gehanteerd in deze meesterproef.

5.1 Methodologische verantwoording

Dit onderzoek maakt gebruik van de kwalitatieve onderzoeksmethode, omdat het onderzoek gericht is op een beschrijving van de ervaringen van de gemeenten met cybercriminaliteit en hun cyberveiligheidsbeleid. Silverman (2013, pp. 86-87) beschrijft dat kwalitatief onderzoek gaat over percepties van respondenten. Waar kwantitatief onderzoek gaat om de hoeveelheid van een bepaald verschijnsel gaat kwalitatief onderzoek meer over de manier waarop een bepaald verschijnsel plaatsvindt (Bijleveld, 2018, p. 70). Dat is precies het doel van dit onderzoek en op deze manier ontstaat een genuanceerd beeld van het fenomeen. Deze onderzoeksopzet is geschikt om hedendaagse verschijnselen te beschrijven (Mortelmans, 2013, p. 96). Cybercriminaliteit is immers iets waar de laatste jaren steeds meer aandacht voor is en wat hoger op de politieke agenda is komen te staan.

De onderzoeksvragen lenen zich voor een beschrijvend onderzoek (Baarda, et al., 2013, p. 35). Het beschrijvend onderzoek wordt door Mortelmans (2013, p. 103) omschreven als een van de doelen van het kwalitatief onderzoek. Het “gaat over het in de diepte begrijpen van processen van betekenisgeving en een van de wijzen om tot een dergelijk begrijpen te komen is het omstandig beschrijven van een case”. Onder kwalitatieve onderzoeksmethoden kunnen verschillende typen onderzoekstechnieken vallen (Mortelmans, 2013, p. 137). Dit onderzoek heeft als grondvorm een meervoudige *casestudy*, ook wel gevalstudie genoemd, waarbij gebruik is gemaakt van diepte-interviews en een beleidsdocumentenanalyse. De cases zijn in dit geval de verschillende gemeenten, of overkoepelend ‘de gemeente’ in algemene zin.

Diepte-interviews zijn de meest voorkomende vorm van de kwalitatieve survey. De onderzoekseenheden zijn doorgaans individuen (Mortelmans, 2013, p. 138).

In dit onderzoek is gebruik gemaakt van datatriangulatie, waarbij meerdere bronnen worden gebruikt in het onderzoek. (Bijleveld, 2018, p. 98; Maesschalck, 2016, p. 147). Het afnemen van interviews en de geanalyseerde beleidsdocumenten zorgden ervoor dat er een diepgaand inzicht is verkregen in hoe de gemeenten omgaan met cybercriminaliteit en cyberveiligheid. De diepte-interviews waren semigestructureerd zodat alle aspecten van de onderzoeksvragen aan bod kwamen en er tevens ruimte was voor eigen invulling van de respondenten. De bevindingen uit de beleidsdocumenten dienen als aanvulling op de bevindingen uit de interviews.

De casestudy is in het algemeen lastig definieerbaar, maar lijkt te bestaan uit 2 dimensies. De eerste dimensie gaat over de empirische realiteiten en de tweede over de aard van de case (Mortelmans, 2013, pp. 146-148). In andere woorden: Het gaat om een studie van een afgebakend onderzoekseenheid, zoals die zich manifesteert in de sociale werkelijkheid (Leys, Zaitch, & Decorte, 2016, p. 162). De kern van de casestudy is dat de onderzoeker een gedetailleerd inzicht wil krijgen in de case door middel van dataverzameling. De focus ligt op meerdere cases om zo uitspraken te kunnen doen over die groep. In dit geval: gemeenten (Mortelmans, 2013, pp. 146-148). Leys, Zaitch & Decorte (2016, p. 168) zeggen over de collectieve gevalstudie dat die dient om een fenomeen, populatie of omstandigheid beter te begrijpen. De meervoudige casestudy bestaat als het ware uit meerdere enkelvoudige casestudies waarbij aan het eind een vergelijking zal worden gemaakt. In dit onderzoek zijn cases geselecteerd die met elkaar verwant zijn. Dit wordt ook wel casecontaminatie genoemd (Mortelmans, 2013, p. 181). Ze zijn eerst individueel bestudeerd en dan onderling vergeleken in een zogenaamde ‘iteratieve cyclus’. Hierbij zijn ze aan elkaar getoetst om inzichten te verfijnen, ze te valideren en de externe validiteit te vergroten (Leys, Zaitch, & Decorte, 2016, p. 165).

5.2 De selectie van de onderzoekseenheden, contactopname en respons

In dit deel wordt een beschrijving gegeven van wat en wie de onderzoekseenheden zijn, hoe daar contact mee is opgenomen en wat de respons was.

5.2.1 Afbakening van de onderzoekspopulatie en de steekproeftrekking

Bij een kwalitatief onderzoek is slechts een beperkt aantal analyse-eenheden mogelijk. Dit maakt dat de steekproef niet willekeurig maar doelgericht moet zijn (Mortelmans, 2013, p. 153). Om de steekproef te maken moeten eerst de cases, en de daarbij behorende onderzoekseenheden, besproken worden. (Silverman, 2013, p. 142). Er is gebruik gemaakt van een doelgerichte steekproef met vooraf opgestelde criteria die een inzicht geven in cybercriminaliteit en cyberveiligheidsbeleid. Alle relevante aspecten van het onderwerp moeten worden afgedekt waarbij er rekening wordt gehouden met voldoende variatie binnen de opgestelde criteria zodat de data ook voldoende variatie heeft voor een diepgaande analyse (Mortelmans, 2013, p. 153). Meer specifiek gaat het om een criterium-gebaseerde steekproef waarbij vooraf is bepaald aan welk criterium iemand moet voldoen om te vallen onder de typische case (Mortelmans, 2013, pp. 156-161). Het moet gaan om informatierijke cases, namelijk expertinterviews met professionals die deskundigen zijn op het gebied cybercriminaliteit en cyberveiligheid(sbeleid) bij de gemeenten (Baarda & Van der Hulst, 2017, p. 27).

In dit onderzoek zijn de beleidsmedewerkers, die werken voor of met de gemeente (en de beleidsdocumenten), de onderzoekseenheden. De reden voor het selecteren van deze personen was omdat zij tot de antwoorden kunnen leiden die zijn opgesteld in de onderzoeksvragen. Het gaat hier dan ook om de functie van personen en hun directe betrokkenheid met het interne cyberveiligheidsbeleid van de gemeente. Alle respondenten moeten direct of indirect werkzaam zijn voor de gemeente. De verwachting hierbij was dat grotere gemeenten een beter ontwikkeld cyberveiligheidsbeleid hebben waardoor die zoveel mogelijk zijn meegenomen in het onderzoek.

Belangrijk bij de omvang van de steekproef is dat er een balans is tussen de haalbaarheid van het onderzoek en het verzamelen van voldoende relevante data om de onderzoeksvragen volledig te kunnen beantwoorden (Mortelmans, 2013, p. 168). Er moeten voldoende interviews worden afgenomen zodat theoretische saturatie wordt bereikt (Mortelmans, 2016, p. 121). Dit is het geval wanneer nieuwe cases weinig tot geen nieuwe informatie meer opleveren. Idealiter dekt de helft de Nederlandse situatie en de andere helft de Belgische, waar in dit onderzoek zoveel mogelijk naar is gestreefd. Er zijn logischerwijs ook mensen

die niet behoren tot de onderzoekspopulatie. Zo is dit onderzoek niet gericht op de manier waarop bestuurders bepalen in welke mate cyberveiligheid op de politieke agenda komt, waardoor de achterliggende processen niet geheel in kaart zijn gebracht. De bestuurders zijn dan ook niet geïnterviewd en hun inzichten betreffende cybercriminaliteit en cyberveiligheid bij hun gemeenten zijn dus niet bevraagd.

5.2.2 Contactopname en respons

Om toegang te krijgen tot de juiste mensen is in eerste instantie contact opgenomen met de gemeenten. De methode die is toegepast om bij de juiste individuen uit te komen bestond in eerste instantie uit het e-mailen[55] van in totaal 28 gemeenten en andere gemeentelijke dan wel overheidsorganisaties waarvan een samenwerking werd vermoed, met uitleg over het onderzoek en het verzoek tot medewerking voor het afnemen van interviews. De reden dat er contact is opgenomen met zoveel organisaties is omdat de respons erg laag was. Alleen door een groot aantal verzoeken uit te sturen is het uiteindelijk gelukt om voldoende respondenten te vinden voor het onderzoek. Bij het selecteren van de gemeenten is gepoogd om zoveel mogelijk grote gemeenten aan te schrijven. De kans dat zij voldoende budget hebben voor een cyberveiligheidsbeleid met voldoende werknemers die konden deelnemen aan het onderzoek is immers groter. In Vlaanderen is het aantal grotere gemeenten echter beperkt dus daar zijn ook relatief kleine plaatsen aangeschreven.

Omdat het van tevoren niet te bepalen was welke individuen exact bij de interne aanpak van cybercriminaliteit en cyberveiligheid betrokken zijn hebben de organisaties zelf aangegeven wie de geschikte respondenten waren. Hierbij is verder gelet op of de desbetreffende personen daadwerkelijk een functie had die te maken heeft met dit beleid en of zij de juiste informatie kunnen verschaffen. Waar nodig werd er om doorverwijzingen gevraagd om zo bij de juiste personen uit te komen Dit wordt ook wel de sneeuwbalmethode genoemd (Kleemans, Korf, & Staring, 2008, p. 328; Mortelmans, 2013, p. 159). Uiteindelijk bleek dat een groot deel van de aangeschreven organisaties geen onderdeel uitmaakten van de gemeente en/of geen specifieke samenwerking hadden. Dit was bijvoorbeeld het geval bij enkele Bibliotheken, Politiediensten, openbaarvervoersbedrijven, luchthavens en de overkoepelende instanties waarbij de gemeenten zijn aangesloten. Een andere gehanteerde

[55] Zie bijlage 1.

methode is het via LinkedIn benaderen van beleidsmedewerkers van verschillende organisaties. Voor de *Port of Antwerp* (Havenbedrijf) heeft dit geresulteerd in een medewerking aan het onderzoek door middel van een afgenomen interview. Het Havenbedrijf en Digipolis in Antwerpen zijn eigendom van de Gemeente Antwerpen maar het zijn losse organisaties met hun eigen structuur. Digipolis verzorgt niet alleen de ICT-behoeften van Antwerpen maar ook die van Gent. Echter kwam vanuit Gent een negatieve reactie voor deelname aan het onderzoek.

Niet alle contactverzoeken resulteerden dus in een (positieve) reactie. Van een deel van de organisaties kwam geen respons, zoals van het Havenbedrijf van Rotterdam. Een aantal organisaties gaf een afwijzing vanwege werkdruk of het niet kunnen faciliteren van de grote aantallen van studentenaanvragen. Een enkele keer kwam het voor dat een gemeente, naar eigen zeggen, geen beleid of expert had. Tweemaal is het voorgekomen dat respondenten moesten afzeggen vanwege vervroegd verlof. Met één respondent moest het interview vroegtijdig worden afgebroken toen bleek dat de vraag niet goed was begrepen en het onderwerp van dit onderzoek buiten zijn functie viel. Collega's naar wie vervolgens werd doorverwezen gaven geen reactie tot medewerking aan het onderzoek.

Dit proces heeft uiteindelijk geleid tot een lichte willekeur in de respondenten. Omwille van anonimiteit zijn de respondenten genummerd, voor België zijn dit de 'BE' respondenten met hun nummer, voor Nederland de 'NL' en 'NLx' (digitaal) respondenten met hun nummer. In totaal zijn er in België 7 respondenten (BE 1 t/m 7) geweest in 5 afgenomen interviews bij 4 gemeenten. In Nederland zijn er 8 respondenten (NL 1 t/m 8) geweest in 6 afgenomen interviews bij 5 gemeenten. Bij 2 Nederlandse gemeenten is gesproken met respondenten die weinig zicht hadden op de technische maatregelen die de gemeente nam en is er voor enkele vragen digitaal gecorrespondeerd met voor elk desbetreffend interview 1 andere beleidsmedewerker (NLx 1 & 2). Dat zijn in totaal dus 17 respondenten (15 interviews) bij 9 verschillende gemeenten.

De gemeenten die hebben meegewerkt zijn in alfabetische volgorde: Aarschot, Amsterdam, Antwerpen (Havenbedrijf en Digipolis), Den Haag, Maastricht, Mechelen, Rotterdam, Turnhout, en Utrecht. De respondenten hadden veelal niet alleen een uitvoerende rol maar vaak ook een adviserende en/of leidinggevende rol. Dit kon zijn in de Rol van CISO of ISO maar ook als ICT-*manager*, afdelingshoofd of *Data Protection Officer* (DPO).

5.3 Dataverzameling: Beleidsdocumentenanalyse en interviews

In dit deel van de onderzoeksopzet wordt er ingegaan op documentenanalyse en interviews en als dataverzamelingsmethoden.

5.3.1 De gehanteerde dataverzamelingsmethode

De beleidsdocumenten[56] zijn deels verkregen door de respondenten en deels zelf verzameld door te zoeken in openbare bronnen op het internet. Er is gekozen om enkel beleidsdocumenten mee te nemen in de analyse die gaan over cybercriminaliteit en cyberveiligheid bij gemeenten. Meer specifiek zijn er beleidsdocumenten geanalyseerd van 2 gemeenten die ook hebben geparticipeerd in interviews, waarbij is gekozen voor een Belgische gemeente 'X' en een Nederlandse gemeenten 'Y'. Ook zijn er documenten opgenomen die zich op gemeenten in het algemeen richten, zoals de BSG en de BIG (de BIO is nog niet beschikbaar). Dit is gedaan als aanvulling omdat de beschikbare documenten van/over de specifieke gemeenten zelf zeer beperkt waren. Er is niet gekozen om andere specifieke gemeenten mee te nemen vanwege de haalbaarheid van het onderzoek. Het verkrijgen van relevante beleidsstukken van andere gemeenten is namelijk niet gelukt.

Van de Belgische gemeente 'X' is het informatieveiligheidsbeleid meegenomen in de analyse. Lastig bij het verkrijgen van de documenten was het feit dat de gemeenten niet alle beschikbare beleidsdocumenten konden of wilden delen. Enerzijds lag dit aan de afwezigheid van de documenten (ze waren er simpelweg niet), anderzijds werden bepaalde documenten niet beschikbaar gesteld voor het onderzoek vanwege de gevoeligheid van de informatie. Voorbeelden hiervan zijn (interne) rapportages over effectieve cijfers en maatregelen. Om dat gat op de vullen is het Audit-rapport Vlaanderen opgenomen dat gaat over cyberveiligheid bij Vlaamse gemeenten in het algemeen. Verder bevatten niet alle vindbare documenten de benodigde informatie, zo is de jaarrekening van 2017 van de gemeente bekeken. Hoewel daarin wordt gespecificeerd hoeveel van het budget beschikbaar is gemaakt voor de bedrijfsvoering rondom ICT-zaken (ongeveer 2,5 miljoen euro) is er geen verdere specificatie van die kosten beschikbaar. Het is dus onduidelijk hoe die kosten zijn

[56] Zie bijlage 2.

verdeeld, wat er precies onder valt en wat de link is met het informatieveiligheidsbeleid. Ook is hieruit niet duidelijk op te maken hoeveel personeel er beschikbaar is. Het bestuursakkoord 2019 mist die informatie ook. Het niet bevatten van bruikbare informatie in de beschikbare/vindbare documenten geldt overigens ook voor andere onderzochte Vlaamse gemeenten. Om die reden is er maar één Belgische (en één Nederlandse) gemeente meegenomen in de documentenanalyse.

Voor de Nederlandse gemeente was het verkrijgen van de documenten makkelijker. Zowel online als via de respondenten waren de documenten beschikbaar. In de analyse is van een gemeente het informatieveiligheidsbeleid meegenomen en een Rapport Informatiebeveiliging (gemeente 'Y') uit 2017. Ook is het IBD-rapport voor Nederlandse gemeenten als aanvulling opgenomen in de analyse. Dit laatste document is opgesteld aan de hand van een analyse van incidentrapportages van gemeenten, meldingen aan de IBD en een analyse van bronnen zoals het 'Cybersecuritybeeld Nederland'. Ook zijn er voor het IBD-rapport interviews afgenomen bij gemeenten en de CERT's van andere organisaties en enkele leveranciers van gemeentelijke ICT-diensten (IBD & VNG, 2018, p. 2). Jaarverslagen en bestuursakkoorden zijn ook voor Nederland buiten beschouwing gelaten omdat de Belgische documenten ontbreken en er daardoor geen vergelijking mogelijk is. Zodoende zijn er wat dat betreft geen bevindingen opgenomen in de resultaten.

Het kwalitatief interviewen heeft als doel om diepte te krijgen in het verhaal van respondenten. Daarom is het van belang het natuurlijke verloop van het gesprek te volgen en in te spelen op wat er gezegd wordt. Er moet enkel gewaakt worden dat het interview niet te ver afdwaalt van het onderwerp (Mortelmans, 2013, p. 229). De interviews zijn zo veel mogelijk *face-to-face* afgenomen om data te verzamelen. Een telefoongesprek, e-mailuitwisseling, videogesprek of chatsessie bemoeilijkt de afname. Dit kan liggen aan simpele dingen als een slechte verbinding of aan de bereidwilligheid van de respondent zijn antwoord uitgebreid op te schrijven. Deze problemen kunnen eenvoudig worden voorkomen door de respondenten op te zoeken. Dit was ook mogelijk gezien de afstand van de steden uit de steekproef. Een bijkomend voordeel van het interviewen op hun werk is dat de kennismaking al begint bij de ontvangst. Op die manier was het ijs al gebroken voordat het interview daadwerkelijk begonnen was. De respondent kon zelf makkelijk een ruimte uitzoeken die geschikt is voor het interview, zoals het eigen kantoor, wat het gevoel van vertrouwen kan vergroten. Door persoonlijk contact is ruim de tijd genomen voor het gesprek, die plaatsvonden tijdens werktijden van de respondenten. Desondanks is er 1

interview telefonisch afgenomen om zo tijd te besparen, omdat die respondent er pas laat in het onderzoek is bijgekomen.

De dataverzameling voor dit onderzoek heeft plaatsgevonden door middel van diepte-interviews. In een diepte-interview worden een aantal onderwerpen nauwkeurig en langdurig besproken (Baarda & Van der Hulst, 2017, p. 20). Met interviews kunnen onder andere gedachten, opinies en kennis van respondenten in kaart worden gebracht. Dit is van belang om een genuanceerd beeld te krijgen van de ervaringen van de gemeenten met cybercriminaliteit en hun cyberveiligheidsbeleid. Hierbij is gebruik gemaakt van een semigestructureerd-interviewschema/vragenprotocol[57] dat bestaat uit een logisch opgebouwde lijst met vragen. Er is dus van tevoren bepaald worden welke thema's aan bod moesten komen. Deze methode biedt als voordeel dat de vragen tijdens het interview aangepast kunnen worden (Beyens & Tournel, 2016, pp. 194-195). Er zijn verschillende varianten mogelijk van de mate van gestructureerdheid. De meest open, ongestructureerde vorm is enkel een topiclijst. De meest gesloten, gestructureerde vorm is een lijst met vragen waarvan er niet wordt afgeweken (Beyens & Tournel, 2016, p. 197). Voor dit onderzoek is er gebruik gemaakt van het vragenprotocol. Dat ligt in de lijn van de topiclijst, maar waar een topiclijst enkel de onderwerpen of thema's die aan bod komen weergeeft heeft het vragenprotocol volledig uitgeschreven vragen. Dit biedt als voordeel dat de afname meer gestructureerd wordt, de antwoorden beter vergelijkbaar zijn en dus de analyse wordt vergemakkelijkt (Mortelmans, 2013, p. 223). De interviews zijn opgenomen om de verwerking te vergemakkelijken. Zo liepen de gesprek vlotter omdat de volle aandacht op het voeren van het gesprek lag.

5.3.2 Verloop van interviews

Voor dit onderzoek is gekozen voor een interviewschema met volledige vragen omdat op die manier de meeste informatie kan worden verworven. De volgorde verschilde per interview en ter plekke zijn er aspecten weggelaten of toegevoegd. Het precieze verloop van de interviews werd dus deels bepaald door de respondenten en was verschillend per respondent, omdat ieder de focus heeft gelegd op de onderwerpen die voor hem of haar het belangrijkst zijn. Er was voldoende ruimte binnen het interview om hierop in te spelen. Op

[57] Zie bijlage 3.

die manier is wat daadwerkelijk relevant was volgens de respondenten besproken. Baarda et al. (2013, p. 35) beschrijven dat als de ecologische validiteit. Ook is het interviewschema in beperkte mate aangepast nadat er een aantal interviews zijn afgenomen toen daaruit bleek dat bepaalde concepten onvoldoende waren uitgewerkt. Mortelmans (2013, p. 234) beschrijft deze werkwijze als flexibel. Tijdens het interview is er ook op een open manier doorgevraagd naar onderwerpen die niet voorkomen in het vragenprotocol. Hierdoor kon een gewenste richting gegeven worden aan het gesprek en zijn zaken verduidelijkt (Beyens & Tournel, 2016, p. 197). Tussendoor is er samengevat en aan de respondent gevraagd of de samenvatting klopt. Dit diende ervoor om zaken helder te krijgen en waar nodig aanvullingen of correcties te geven door de respondent wat leidde tot rijkere data. Tevens is zo de betrokkenheid getoond waardoor de respondent wist dat er goed geluisterd werd (Mortelmans, 2013, p. 239).

De algemene lijn van de afgenomen interviews is als volgt. Als eerste is er een korte uitleg gegeven over het doel van het onderzoek en is er gevraagd of de respondent toestemming geeft om het interview op te nemen. Dit laatste wordt ‘geïnformeerde toestemming’ genoemd (Beyens & Tournel, 2016, p. 217). Daarna volgden de eerste effectieve vragen die relevant waren voor het onderzoek namelijk de rol van de respondent binnen de gemeente en hoe lang de functie al wordt vervuld. Dit zijn de inleidingsvragen en dienen ervoor om het gesprek op gang te laten komen (Mortelmans, 2013, p. 237). Daarna volgde de vraag of ze een opleiding hebben gevolgd die betrekking heeft op cybercriminaliteit. Dat was de transitievraag die peilt naar de persoonlijke ervaring van de respondent met het onderwerp (Mortelmans, 2013, p. 238). Daarna volgden de sleutelvragen die de onderzoeksvragen weerspiegelen. Dat zijn de vragen waar het onderzoek om draait en die werden gebuikt in de analyse (Mortelmans, 2013, p. 238).

De sleutelvragen gingen over cybercriminaliteit en cyberveiligheid in het algemeen. Hierbij is er gepeild naar hoe de respondenten cybercriminaliteit en cyberveiligheid omschrijven en vervolgens met welke vormen ze geconfronteerd worden in hun werk. Ook is er gevraagd naar de ondervonden schade van cybercriminaliteit binnen hun organisatie. Daarna volgde er een tussenvraag/transitievraag over de aanwezigheid van cybercriminaliteit en cyberveiligheid in de samenleving. De tussenvraag dient om het onderwerp verder uit te diepen en helpt de respondent breed na te denken over de antwoorden om zo meer data te verzamelen. Vervolgens is er gefocust op welke proactieve en reactieve beleidsmaatregelen er in plaats zijn voor het bevorderen van de cyberveiligheid. Ook is er een tussenvraag die

gaat over de samenwerking met andere professionals. De antwoorden op deze vraag zijn meegenomen in de sneeuwbalmethode om nieuwe respondenten te werven waar dat mogelijk was. Daarna volgde de vraag of ze zelf denken dat er een verschil is in het beleid van de gemeente ten opzichte van andere gemeenten of organisaties. Vervolgens volgden nog 2 tussenvragen over internationale wetgeving en richtlijnen in het beleid en het volwassenheidsniveau van de organisatie. Tot slot is de vraag gesteld of de respondenten zelf nog aanvullingen hebben. Dit was de eindvraag die peilde naar elementen die niet aan bod zijn geweest (Mortelmans, 2013, p. 239).

5.4 Data-analyse

Bij de analyse is gebruikt gemaakt van de procedurele principes van de *Grounded Theory* waarbij onderzoeksvragen worden beantwoord door middel van empirisch materiaal. Centraal hierbij staat cyclische werken waarbij het interviewen en de fasen van analyseren elkaar afwisselen (Decorte, 2016, p. 472). Hierdoor ontstaat een steeds verdere verfijning in de analyse. Deze methode wordt ook wel de methode van 'constante vergelijking' genoemd. De data wordt herhaaldelijk bestudeerd en elementen worden vergeleken met elkaar (Mortelmans, 2013, p. 399; Thomas, 2016, p. 205). Het doel hiervan is om conceptuele gelijkenissen en patronen te ontdekken (Decorte, 2016, p. 456). Deze methode is toegepast door na het afnemen van de interviews de opnames te transcriberen. Hierdoor werd een analyse mogelijk, dat al begon tijdens het transcriberen zelf, omdat er op die manier een eerste blik geworpen is op de onderzoeksresultaten. Het transcriberen is gedaan met behulp van betaalde software afkomstig van het bedrijf AmberScript dat zich heeft gespecialiseerd in het omzetten van spraak naar tekst. Zij bedienen professionals en studenten in vele vakgebieden en garanderen absolute vertrouwelijkheid van de bestanden.[58] Die tekst is vervolgens waar nodig handmatig gecorrigeerd, wat aanzienlijk scheelt in de kosten tegenover het volledig uitbesteden van het transcriberen. Dit is zo snel mogelijk nadat de interviews zijn afgenomen gedaan. De methode die is gehandhaafd is het woordelijk opschrijven. Hierbij wordt er wel opgeschreven wat er wanneer gezegd is, maar niet hoe dat is gezegd waardoor intonatie nuances wegvallen. Niet-verbale elementen zoals gezucht en niet-relevante tekst zoals gestotter, herhalingen en tussenwerpsels zijn ook niet

[58] Zie de punten 4 en 15 op de site: https://www.amberscript.com/nl/faq.

meegenomen. Dit maakt het transcriberen eenvoudiger. Daarnaast is de meerwaarde ervan niet heel groot voor de analyse. Taalfouten zoals kromme zinnen of dialect blijven wel zoals ze zijn en zijn dus niet gecorrigeerd.

Na het transcriberen is de data van de interviews en van de verzamelde beleidsdocumenten gecodeerd met behulp van het programma Atlas.ti, bedoeld voor kwalitatieve analyses. Het coderen vond plaats in verschillende fasen, te beginnen met open coderen. Mortelmans (2013, p. 403) beschrijft dit als "de fase van het opdelen van de gegevens in kleinere gehelen. Deze fase bestaat uit het geven van namen/labels aan stukken tekst in de data". Er is geen gebruik gemaakt van een vooraf openstelde lijst met codes, wat past bij de *Grounded Theory* methode (Decorte, 2016, p. 468). Wel zijn de onderzoeksvragen in het achterhoofd gehouden tijdens het coderen om te zien wat relevant was. Dit resulteerde in een computerbestand met een uitgebreide set van codes. Wat volgde was axiaal coderen waarbij losse labels die dubbel voorkomen of een relatie met elkaar hebben werden samengevoegd en overbodige codes werden verwijderd. Tot slot is er nog selectief gecodeerd waarbij concepten met elkaar werden verbonden. Deze fase is van belang voor een goede en volledige beantwoording van de onderzoeksvragen (Mortelmans, 2013, p. 404).

Om betekenis te vinden in de data zijn verschillende tactieken toegepast die door Miles, Huberman, en Saldaña (2014, pp. 275-293) worden beschreven. Hierbij kan bijvoorbeeld gedacht worden aan het clusteren van bepaalde concepten zoals bepaalde handelingen. Een ander voorbeeld is het kijken naar tegenstellingen en overeenkomsten die naar voren komen uit de interviews. Door deze tactieken toe te passen is de validiteit van de analyse vergroot. Met de bevindingen uit deze data-analyse zijn de onderzoeksvragen beantwoord. Ook is gekeken naar of de antwoorden van de respondenten overeenkomst vertonen met de bevindingen uit de literatuur. Bijvoorbeeld door te kijken naar of de respondenten dezelfde typen en schade van cybercriminaliteit noemen. Dat laatste wordt verder toegelicht in de discussie.

5.5 Kwaliteit, beperkingen en ethiek van de onderzoeksmethode

Het werd hierboven al kort benoemd dat analysetechnieken de validiteit beïnvloeden. In dit deel wordt daar verder op ingegaan. Ook volgt er een stuk waarin de ethische overwegingen en de beperkingen van het onderzoek worden besproken.

5.5.1 Kwaliteit: Validiteit en betrouwbaarheid

In kwalitatief onderzoek zijn er 2 hoofdkwaliteitscriteria waarover nagedacht moet worden: validiteit en betrouwbaarheid (Silverman, 2013, p. 284). Deze kunnen allebei opgesplitst worden in interne en externe validiteit en betrouwbaarheid. Daarnaast is er een vijfde criterium: authenticiteit en relevantie, dat inherent is aan kwalitatief onderzoek (Maesschalck, 2016, p. 139).

De betrouwbaarheid gaat over de mate van toeval in het onderzoek. De onderzoeksresultaten zouden dus consistent moeten zijn wanneer het onderzoek herhaald wordt. Interne betrouwbaarheid verwijst naar de mate waarin 'anderen' tot dezelfde conclusies komen (Maesschalck, 2016, p. 139). Door opnameapparatuur te gebruiken is de kwaliteit van de data verhoogd. Ook zijn de antwoorden van de respondent samengevat tijdens het interview om te controleren of de respondent goed is begrepen (Silverman, 2013, p. 299; Maesschalck, 2016, p. 145). Externe betrouwbaarheid verwijst naar de mate waarin de resultaten gelijk zijn wanneer nieuwe data verzameld zou worden door het uitvoeren van een nieuw onderzoek naar hetzelfde fenomeen. Dat is lastig voor dit type onderzoek omdat de interactie tussen respondent en onderzoeker elke keer uniek is en niet perfect gereproduceerd kan worden. Wel kan gesteld worden dat de grote lijnen van het onderzoek gelijk zullen blijven. Een hoge mate van betrouwbaarheid van een onderzoek geeft echter geen garanties voor de validiteit.

De validiteit van het onderzoek gaat over of de informatie een juiste afspiegeling van de werkelijkheid vertoont (Silverman, 2013, p. 287). Interne validiteit gaat over de geloofwaardigheid van causaliteit in uitspraken. Hier moet mee opgepast worden in beschrijvend onderzoek omdat causale uitspraken al snel richting verklaren gaan (Maesschalck, 2016, p. 140). De interne validiteit wordt in dit onderzoek verder versterkt door het gebruik van datatriangulatie (Maesschalck, 2016, p. 147). Externe validiteit gaat om het generaliseren van de bevindingen. Hoewel statistische generaliseerbaarheid per definitie onmogelijk is bij kwalitatief onderzoek, is het wel mogelijk om te spreken van *case-to-case* overdracht. Hierbij wordt een case grondig beschreven, er wordt een *thick description,* ook wel gedetailleerde beschrijving gegeven, wat de lezer in staat stelt de informatie te generaliseren naar andere cases (Maesschalck, 2016, pp. 141-143). Dit wordt toegepast in dit onderzoek door meerdere cases op deze manier te beschrijven waardoor ook

iets gezegd kan worden over gemeenten in België en Nederland die niet zijn meegenomen in dit onderzoek. De validiteit van het onderzoek kan verder verhoogd worden door vragen zo concreet mogelijk te stellen (Baarda & Van der Hulst, 2017, pp. 32-33; Silverman, 2013, p. 287). Deze methoden zijn zoveel mogelijk toegepast door in de literatuurstudie documenten op te nemen die wijzen in de richting van hoe gemeenten omgaan met cybercriminaliteit en cyberveiligheid en de vragen tijdens de interviews zo concreet mogelijk te stellen.

Silverman (2013, p. 289) noemt deze methoden feilbaar en beschrijft nog andere manieren om de validiteit te verhogen. Een relevante methode is de eerdergenoemde 'constante vergelijking'. Bij deze methode wordt er gelet op overeenkomsten en verschillen tussen bepaalde cases. De onderzoeker zal moeten proberen om vergelijkbare cases te vinden om te kijken of er tot dezelfde onderzoeksresultaten zal worden gekomen (Silverman, 2013, p. 290; Decorte, 2016, p. 467). In dit onderzoek was dit het geval omdat het een meervoudige casestudy betreft en waarbij de gemeenten met elkaar vergeleken zijn. Er is gestreefd naar *pattern recognition*, waarbij er wordt gekeken of er patronen te herkennen zijn tussen de cases (Leys, Zaitch, & Decorte, 2016, p. 182).

Een andere methode is een uitgebreide dataverwerking. Dit houdt in dat in de data-analyse zo uitgebreid mogelijk wordt gedaan en dat er vanuit de analyse vaste schema's ontstaan. Die vaste schema's kunnen vervolgens leiden tot generaliseerbare uitspraken omdat ze terugkomen in elke case (Silverman, 2013, p. 291). Wanneer dus blijkt dat de verschillende professionals vergelijkbare ervaringen en percepties hebben met cybercriminaliteit kan wel degelijk iets gezegd worden hoe gemeenten lijken om te gaan met cybercriminaliteit en cyberveiligheid. Uit de beschrijving van deze methoden van Silverman kan geconcludeerd worden dat validiteit en betrouwbaarheid sterk met elkaar samenhangen. Door deze methoden toe te passen zal het onderzoek beter wetenschappelijk onderbouwd zijn en van meer waarde zijn voor professionals in het werkveld, beleidsmakers en de maatschappij in het algemeen. Zo kan worden voorkomen dat het onderzoek wordt afgedaan als slechts de mening van de onderzoeker (Silverman, 2013, p. 207). Bij het analyseren van de gegevens is hier dan ook extra aandacht aan besteedt.

5.5.2 Beperkingen en ethiek

Elke onderzoeksmethode heeft te maken met beperkingen (Mortelmans, 2013, p. 112). In dit onderzoek is er beperkt gebruik gemaakt van datatriangulatie, waarbij meerdere databronnen worden gebruikt in het onderzoek (Bijleveld, 2018, p. 98). Er is in dit echter onderzoek alleen gekozen voor het afnemen van interviews en een analyse te doen van een beperkte selectie van beleidsdocumenten om het onderzoek behapbaar te houden.

Andere beperkingen hebben te maken met ethiek. Kwalitatief onderzoek kan gevoelige informatie naar boven brengen (Mortelmans, 2013, p. 190). Het was lastig om voldoende respondenten te vinden voor informatierijke cases. De bereidbaarheid van respondenten voor moeilijke onderwerpen is volgens Mortelmans (2013, p. 115 en 245) echter geen bezwaar voor het onderzoek wanneer de juiste voorbereiding met een flinke portie geduld wordt gehanteerd. In dit geval was het vooral een kwestie van de vraag uitzetten bij voldoende verschillende organisaties en regelmatig contact onderhouden met de mogelijke respondenten. Desondanks bleek uit de contactopname dat respondenten soms huiverig waren voor deelname. In dit onderzoek werden respondenten gevraagd om informatie te delen over het beleid van de gemeente wat ze kwetsbaar kan maken voor beter afgestemde cyberaanvallen. Soms kwam het verzoek om meer informatie te verstrekken over de risico's die waren verbonden aan deelname en een enkele keer is er een vertrouwelijkheidsovereenkomst getekend.

Ook het verzamelen van beleidsdocumenten werd bemoeilijkt door de beperkte toegankelijkheid ervan. Zo zijn niet alle gevraagde documenten, zoals interne audits, beschikbaar gesteld voor het onderzoek. Hierdoor is het doen van de analyse bemoeilijkt, omdat de toetsing van het beleid niet vastgesteld kan worden. In documenten die wel openbaar en beschikbaar zijn is het ook vaak zo dat organisaties ervoor kiezen om een beperkt, rooskleurig, beeld op te tekenen voor de buitenwereld (Mortelmans, 2013, p. 206).

Deze nadelen zijn deels opgevangen door de respondenten duidelijk te laten blijken dat de gegevens vertrouwelijk worden behandeld en enkel gebruikt worden voor academische doeleinden. De resultaten van de interviews met het Havenbedrijf en het externe gemeentelijk bedrijf Digipolis zijn niet gespecificeerd als zodanig om de anonimiteit te waarborgen. Ook de overige interviews en de beleidsdocumenten van de gemeenten zelf zijn geanonimiseerd zodat de resultaten niet specifiek te herleiden zijn naar een specifieke gemeente. Daarnaast wordt er geen beschrijving gegeven van de specifieke technische maatregelen (logische en fysieke netwerkschema's, IP-adressen, etc.) die de gemeenten al dan niet hebben geïmplementeerd. Die worden waar relevant enkel in algemene termen

besproken. Ook is de opname een enkele keer stopgezet om bepaalde informatie *off te record* te houden en hebben enkele respondenten ervoor gekozen om niet alle vragen te beantwoorden.

DEEL C: RESULTATEN EN DISCUSSIE

In dit deel worden in hoofdstuk 6 de onderzoeksvragen beantwoord aan de hand van de bevindingen uit de analyse van de interviews en de documentanalyse. In hoofdstuk 7 volgt de discussie met conclusies waarbij de resultaten worden gestaafd met de bevinden uit de literatuur met daaropvolgend de (praktische) aanbevelingen die worden gedaan.

Hoofdstuk 6. Beantwoording van de onderzoeksvragen

Hoofdstuk 6 is een bespreking van de resultaten die volgt uit de empirische data waarmee de onderzoeksvragen worden beantwoord. De indeling is in lijn met de volgorde van de onderzoeksvragen en de eerder gekozen definities.

6.1 Mate van confrontatie met cybercriminaliteit

De bespreking van cybercriminaliteit bij gemeenten valt uiteen in een drietal onderdelen. In het eerste deel komen de vormen van cybercriminaliteit aan bod die naar voren komt uit het IBD-rapport en die worden genoemd door de beleidsmedewerkers/respondenten. Dan volgt de schade en tot slot wordt er gekeken naar de overeenkomsten en verschillen in de cases.

6.1.1 Vormen

De gemeenten hebben last van een grote verscheidenheid aan vormen van cybercriminaliteit. Echter, veel voorbeelden van de respondenten zijn vaak anekdotisch of meer beschreven in algemene zin dan dat ze precies weten te vertellen of ze bepaalde vormen al dan niet (vaker) daadwerkelijk hebben ondervonden bij de gemeente waar ze werkzaam zijn. Cijfermatige data die inzicht geeft in de incidenten is vrijwel niet beschikbaar. De gemeenten houden de incidenten veelal niet bij en als ze het al doen, zoals 3 respondenten aangeven wel te doen, zijn die gegevens of rapportages niet beschikbaar gesteld voor dit onderzoek. Zo geeft een respondent aan software te gebruiken die bepaalde incidenten bijhoudt. In 4 maanden tijd

zijn daar 400.000 *phishing*- en *spammails* geblokkeerd. De andere gemeenten hebben wel een algemeen idee van welke incidenten vaker voorkomen dan anderen, maar hebben (of geven) geen harde cijfers. Het Audit-rapport Vlaanderen biedt verder ook geen inzicht in hoe vaak incidenten voorkomen. Geen enkele van de respondenten maakt verder een onderscheid in verschillende typen van cybercriminaliteit.

Het IBD-rapport biedt wel enigszins inzicht in de aantallen en vormen. Daaruit blijkt dat gemeenten regelmatig cyberaanvallen ondervinden De typen incidenten die worden genoemd tussen oktober 2017 en juli 2018 zijn opgedeeld in verschillende soorten. Zo zijn sabotage en *DDoS* samen ondergebracht in de categorie 'beschikbaarheid' en vallen illegaal naamgebruik en onrechtmatig gebruik van *resources* onder de categorie 'fraude'. In totaal zijn er 429 incidenten gemeld in die tijdsperiode bij het IBD. De meest frequente zijn 70 meldingen van ongeautoriseerde toegang (categorie 'informatiebeveiliging'), 35 meldingen van exploitatie kwetsbaarheid (categorie 'succesvolle inbraak') en 27 *phishing* incidenten (categorie 'verzamelen van informatie'). Andere incidenten worden minder vaak gemeld, wat natuurlijk niet per definitie betekent dat deze ook minder vaak voorkomen. Zo zijn er slechts 10 meldingen van spam (categorie 'malafide materiaal'), 8 meldingen van misbruik kwetsbaarheid (categorie 'poging tot binnendringen') en 2 meldingen distributie van *malware* (categorie '*malware*'). Van alle incidenten wordt 49% onbewust en 8% bewust door een medewerker gepleegd, 20% door een derde partij zoals een leverancier, 13% door criminelen en voor 10% is het niet bekend wie de dader is (IBD & VNG, 2018, pp. 6-9).

Het rapport levert echter geen beeld van de frequentie van de daadwerkelijk ondervonden vormen van cybercriminaliteit. Niet alle incidenten worden immers gemeld en de cijfers uit het rapport vertonen grote verschillen met de aantallen die worden genoemd door enkele respondenten. Een van de respondenten geeft wel aan dat het rapport een goed beeld schetst van de ondervonden incidenten bij die gemeente. Die gemeente zou wat betreft vormen en schade op dezelfde lijn zitten als andere gemeenten in Nederland. Hierdoor wordt het beeld geschetst dat gemeenten als organisaties overeenkomsten vertonen.

Illegale toegang tot IT-systemen

Een deel van de gepleegde cybercriminaliteit is bewust crimineel en technisch zoals de meer klassieke vormen van *phishing* en *spam* waar elke gemeente last van heeft. Zo melden 3 respondenten dat een groot deel van de mails, vaak meer dan de helft, niet functioneel zijn:

> "Wij zijn een van de duizenden, maar wij zijn iets groter dus de kans is ook groter dat er wordt toegehapt." (Respondent BE7)

Die mails zijn vaak zo geavanceerd dat het lastig is om ze te herkennen als frauduleus. Ze zijn geschreven in correct Nederlands en bevatten de juiste namen, logo's of andere specifieke zaken afgestemd op de organisatie. Dit wordt ook wel *spear phishing* genoemd en is zeer lastig te herkennen. In die mails wordt gevist naar informatie die de getroffene ergens moet invullen en dan per ongeluk op die manier data lekt. Wanneer het cybercriminelen lukt om data te achterhalen door middel van *hacks* kunnen ze die inzetten om heel gericht mails te sturen die afkomstig leken te zijn van partners van de gemeente, zoals softwareleveranciers, waardoor het nog realistischer over komt. Die mails lijken dan op een offerte en wanneer iemand dan klikt op de bijlage om de zogenaamde offerte te openen installeren ze daarmee *malware* die daarin verstopt zit. *Phishing* komt op grote schaal voor bij de gemeenten. Alle respondenten noemen deze vorm van cybercriminaliteit als veelvoorkomend. Een groot deel daarvan wordt ondervangen door *firewalls*. Een tweetal respondenten geeft aan dat die *firewalls* bij houden hoeveel aanvallen dat zijn. Dat gaat dan om aanvallen op dagelijkse basis.

Een ander voorbeeld dat wordt gegeven door 1 respondent is dat een document zogenaamd gedeeld wordt via een *cloudservice* waarbij de medewerker naar een login pagina wordt geleid die bijna niet van echt is te onderscheiden. Deze documenten lijken dan afkomstig te zijn van een bedrijf of een collega, waarbij het kan zijn dat desbetreffende accounts zijn gehackt. Zodra iemand dan inlogt krijgt die persoon een nietszeggend document te zien, zoals een brochure. Ondertussen heeft de cybercrimineel de inloggegevens van de medewerker buit gemaakt. Ook kan het zijn dat het document *malware* bevat en de computer infecteert. Die gegevens kunnen vervolgens weer misbruikt worden om grote hoeveelheden *spam* mee te versturen.

Bedrijfsspionage

Wat betreft illegale toegang tot IT-systemen kan de dreiging van binnen en van buiten de organisatie komen. In een gemeente was er een geval bekend waarbij er een oud-medewerker is geweest die data lekte naar een tijdschrift over inwoners met een hoog inkomen:

> "We hebben wel wat akkefietjes gehad hoor op het gebied van de criminaliteit. Bijvoorbeeld een interne medewerker. Die zo bij de afdeling of de dienst burgerzaken. Die sluisde gegevens door van inwoners (…)." (Respondent NL7)

Een andere respondent geeft ook aan dat het opvallend is wanneer onregelmatigheden worden gesignaleerd bij een van de medewerkers. Dit soort incidenten worden opgespoord met software. Het kan dan voorkomen dat een medewerker een geïnfecteerd pdf-document heeft geopend waardoor de computer besmet is geraakt met *malware* en zodoende toegang heeft tot de gegevens van de medewerker. Die toegang wordt dan vervolgens misbruikt en het lijkt dan alsof de medewerker bijvoorbeeld een connectie probeert te maken naar een server waar normaal gezien geen toegang tot is verleend. Deze gegevens kunnen dan worden gebruikt voor bedrijfsspionage.

Gegevens- of systeeminterferentie

Twee respondenten meldden dat simpele virussen in mindere mate voorkomen en dat die door virusscanners worden opgepikt. Dit betekent niet dat de dreiging geheel niet meer aanwezig is:

> "Vroeger waren virussen *signature based* dus eigenlijk een traditioneel een antivirus scant maar een beperkt aantal zaken dus wat doen heel veel men of malafide personen te wijzigen naar een klein beetje aan de handtekening eigenlijk die bij het virus pakket of virus hoort zodanig dat eigenlijk uwen antivirus dat niet meer kan herkennen en zo is dat eindelijk een eeuwige strijd tussen… Ze passen die een klein beetje aan dus dat verandert weer uwen traditionele antivirus scant dat niet dus die en laat dat gewoon mee door en zo kan er dan toch tijdelijk iets toegang tot uw pc genomen worden. En zo zijn er bijvoorbeeld *advanced persistant threats,* dat zijn de te veel moeilijker is dingen om te detecteren dan bijvoorbeeld in een in een simpel pdfje." (Respondent BE1)

Verder komen DDos aanvallen die blokkades opwerpen weleens voor bij de gemeenten. Het is voor gemeenten niet zo heel erg om een tijd niet bereikbaar te zijn waardoor het minder urgent is om specifiek beleid te maken voor dit soort vormen. Een van de gemeenten heeft een DDoS aanval ondervonden waardoor het een dag lang uit bedrijf was. Opvallend was dat ze daar gebruik maken van 2 verschillende internetproviders en dat beiden werden aangevallen. De aanval was te herleiden naar een universiteit in de VS die hoogstwaarschijnlijk was gehackt.

Cyber afpersing

Regelmatig worden computers ook geblokkeerd voor de gebruiker door *cryptolockers* waarbij een bepaald bedrag, ook wel *ransomware*, in *Bitcoins* moet worden overgemaakt naar de cybercrimineel voordat de gebruiker weer toegang krijgt. Zeker 4 respondenten noemen dit als veelvoorkomend incident, overigens zonder aantallen te geven. In geen van de gevallen gaven respondenten aan dat het bedrag betaald werd omdat dat het de cybercriminelen alleen maar meer redenen zou geven om zulk soort blokkades in te zetten:

> "(…) we betalen in geen geval. Want dan is de beer los. Om nog veel meer aanvallen uit te voeren o jongens dat levert wat op. En ja het is een kwestie van wie heeft de langste adem." (Respondent NL7)

Daarbij is er geen garantie dat de toegang daadwerkelijk weer wordt verleend. Enkele respondenten menen zelfs dat het bij wet verboden is om er wel aan toe te geven. Een respondent geeft aan dat omdat deze vorm erg opvalt en niet effectief is cybercriminelen zijn overstapt naar het direct *minen* van *Bitcoins* op computers van medewerkers. Dit gebeurt vaak op de achtergrond waardoor iemand hoogstens opmerkt dat de computer wat trager is geworden maar niet direct gealarmeerd is dat er iets mis is.

Internetfraude

Andere vormen van illegaal naamgebruik is CEO-fraude. Deze vorm van fraude houdt in dat een algemeen directeur een mail met spoed lijkt te verzenden naar een persoon binnen het financieel beheer. Die voelt zich onder druk gezet om snel te reageren en zo kunnen grote geldbedragen buitgemaakt worden. In een aantal gemeenten is dit al voorgekomen en bij een aantal gemeenten worden hier specifieke maatregelen tegen getroffen. Om dit soort gegevens te achterhalen worden ook *brute-force attacks* ingezet waarbij *botnets* toegang tot een site of systeem proberen te krijgen door het veelvuldig uitproberen van combinaties van gebruikersnamen en wachtwoorden tot ze er een beet hebben. Vaak maken ze daarbij gebruik van gegevens die al beschikbaar zijn zoals gelekte wachtwoorden die te vinden zijn op het *dark web*. In een van de gemeenten kreeg de burgemeester dreigmails waarin stond vermeld dat er belastend beeldmateriaal zou worden prijsgegeven als er geen betaling werd gedaan. In dit geval wist de burgemeester dat die beelden niet bestonden en is niet ingegaan op de dreigementen.

Ook meldde een respondent *defacing* waarbij er wordt ingebroken op een webserver en de gehoste website vervangen werd door een eigen website van de cybercrimineel. Het is over het algemeen bedoeld als een soort elektronische graffiti en wordt, net als andere vormen

van vandalisme, ook gebruikt om berichten te verspreiden door politiek gemotiveerde hacktivisten.

6.1.2 Schade

Uit het IBD-rapport wordt de impact van die incidenten slechts voor 4% hoog ingeschat, voor 12% gemiddeld en voor het overgrote deel, 84%. Uit het rapport blijkt echter niet hoe dit is gemeten en hoe de categorieën zijn gedefinieerd (IBD & VNG, 2018, p. 9).

Directe schade

Financiële schade is moeilijk uit te drukken voor de gemeenten omdat het niet duidelijk is wat de criteria zijn, dus wat er wel en niet onder valt, en hoe dat te berekenen valt. Het tijdsverlies kwantificeren is lastig en wordt om die reden ook niet precies bijgehouden. Zo geeft een respondent bijvoorbeeld aan dat na een verstoring oude systemen moeten worden teruggezet of dat er andere technische maatregelen moeten worden genomen voordat medewerkers weer terug aan de slag kunnen. Maar wat dan de kosten zijn voor het hebben en terugplaatsen van *back-up* systemen, de arbeid van het (ingehuurde) IT-personeel of de verloren arbeidstijd van de gebruikers van die systemen is onduidelijk. Er lijkt daardoor geen sprake te zijn van ‘echte’ financieel economische of commerciële schade. Deze vorm van schade lijkt mee te vallen omdat een overheidsorganisatie “niet echt leeg te trekken valt” (Respondent BE3). Een gemeente heeft geen winstoogmerk en kan niet failliet kan gaan. Die tegenstelling met bedrijven wordt door 6 respondenten genoemd. Echter betekent dit niet dat omdat de schade niet gemeten wordt de schade er niet is. De dragers van de schade blijven in dit geval ook ‘onzichtbaar’. Uiteindelijk is het de overheidsorganisatie en dus indirect de maatschappij die de schade draagt.

Wat wel overduidelijk financiële schade oplevert is wanneer systemen niet *failproof* zijn ingericht en een medewerker per ongeluk een verkeerd bedrag invult en overmaakt naar bijvoorbeeld een inwoner, een situatie die bij 3 gemeenten is voorgekomen. Het is de gemeenten niet gelukt om die bedragen volledig terug te krijgen. Ook het verkeerd invullen van emailadressen kan een hele simpele manier zijn waardoor het fout kan gaan. Hoewel deze voorbeelden geen echte vormen zijn van cybercriminaliteit hebben ze wel te maken met cyber- en informatieveiligheid.

Indirecte schade

Uit de interviews blijkt dat respondenten zich zorgen maken over de bescherming van persoonsgegevens. Er zijn 5 respondenten die daarbij meldden dat het niet zozeer de gemeente zelf is die hieronder lijdt, maar vooral de persoon van wie de gegevens zijn gelekt. Zo kan er identiteitsfraude gepleegd worden met identiteitsdocumenten waarmee bijvoorbeeld leningen kunnen worden afgesloten en iemand op zwarte lijsten kan komen. Dit heeft grote gevolgen voor de persoon in kwestie en is lastig op te sporen door de autoriteiten. Het verzuimen te melden van datalekken bij de autoriteiten en/of het niet naleven van wet- en regelgeving kan wel een boete opleveren:

> "Als overheid zeker aan de regels moeten [vol]doen die ons als overheid en worden opgelegd." (Respondent NL6)

De dragers van de schade zijn in dit geval de individuen van wie de gegevens zijn gelekt. Indirect leiden dit soort lekken tot imagoschade waarbij de overheid niet meer betrouwbaar overkomt. Deze vorm van schade wordt genoemd door 12 respondenten en is een hele duidelijke vorm van schade voor gemeenten. Bestuurders zijn daar "allergisch voor, want dat kan stemmen kosten" (Respondent NL8). Wel benoemen 3 respondenten dat imagoschade relatief is omdat inwoners niet de keus hebben zoals bij bedrijven en nergens anders terecht kunnen voor bepaalde overheidsdiensten.

De eerdergenoemde verstoring van de ICT-systemen, door bijvoorbeeld een DDoS aanval, waardoor medewerkers hun werk niet meer kunnen uitvoeren kan naast (onbekende) financiële schade ook tot indirecte schade leiden. Het kan bijvoorbeeld zijn dat loketten daardoor dicht moeten wat weer imagoschade kan opleveren. In het weekend of in de vakantieperiode is de impact kleiner, omdat er dan minder mensen aan het werk zijn en er minder burgers zijn die gebruik maken van de dienstverlening. In het Audit-rapport Vlaanderen worden imagoschade, extra kosten, technische werkloosheid en ontevreden burgers genoemd als mogelijke gevolgen van onderbrekingen van werkzaamheden door incidenten (Audit Vlaanderen, 2018, p. 26). Tijdsverlies wordt ook genoemd door een van de respondenten, zo kunnen mails die worden verstuurd niet aankomen:

> "Dat er van een van uw email *domains* (…) enorm veel *spam* en *phishing* afkomstig is dan vliegt ge op hun *black list* en daar hebben we toch een aantal weken last van gehad dat onze mails niet altijd bij de bestemming toekwamen. (…) En ze zullen wel

denken oké het is bezorgd en dan een week later, ik heb nog niet antwoord op mijn mailke en dan welk mailke? En dan zit het ergens in de wachtrij." (Respondent BE2)

Toch lijkt de schade bij de gemeenten in België en Nederland mee te vallen, 2 respondenten noemden de aanval die plaatsvond in Atlanta in de VS dat daardoor 3 weken niet kon functioneren:

> "Valt eigenlijk wel mee wat er bij ons binnenkomt want we hebben we nemen ook monitoring af en dan komt er eigenlijk niet eens zo heel veel uit. Dus dat dat geeft aan dat er dat defensie tot nu toe eigenlijk redelijk succesvol is." (Respondent NL1)

Onopgemerkte schade

Tot slot is een deel van de schade niet bekend:

> "We hebben daar nog niet echt specifiek naar ons gerichte *attacks* gemerkt maar ja je kan maar antwoorden op hetgeen dat je dat je weet en misschien zijn wij ook al jaren het slachtoffer van zoals Belgacom geweest is dat weet ge uiteindelijk niet. We hebben op dit moment niet echt het idee dat we een gericht slachtoffer zijn maar dit kan een fout idee zijn (…)." (Respondent BE1)

Ook in het Audit-rapport Vlaanderen komt dit sterk naar voren:

> "Informatiebeveiligingsincidenten blijven onder de radar. Doordat de geauditeerde besturen hun personeelsleden nauwelijks houvast bieden voor het identificeren van informatiebeveiligingsincidenten, is het niet voor iedereen binnen die besturen duidelijk wat ze als dusdanig moeten beschouwen. Daardoor worden sommige (niet-IT) incidenten niet of onvoldoende gesignaleerd. (…) Om te leren uit incidenten is het belangrijk om die incidenten te registreren. Meer dan de helft van de geauditeerde besturen heeft geen register van informatiebeveiligingsincidenten. Zelfs waar er wel een register is, worden maar weinig van de incidenten geregistreerd." (Audit Vlaanderen, 2018, p. 27)

6.1.3 Overeenkomsten en verschillen cybercriminaliteit

Opvallend is dat wanneer de respondenten gevraagd wordt naar verschillen en overeenkomsten zij hier zelf geen goed zicht op lijken te hebben. Ze doen hierbij vaak aannames en geven ook weleens tegengestelde antwoorden. Zo zeggen 7 respondenten dat grote gemeenten waarschijnlijk dingen beter voor elkaar krijgen dan kleine gemeenten en dus minder last heeft van de vormen en schade van cybercriminaliteit. Hier lijkt consensus over te zijn. Ook noemen ze soms hun eigen gemeente als koploper en noemen ze andere gemeenten die het slechter doen, of andersom terwijl een andere respondent het omgekeerde beweerd. Die laatste situatie kwam alleen voor bij de Nederlandse respondent. Verder zijn er voornamelijk overeenkomsten tussen de gemeenten en zo goed als geen verschillen omdat ze allemaal te maken hebben met cybercriminaliteit en de schade ervan. Omdat er geen rapportages beschikbaar zijn, is het niet vast te stellen welke gemeente daadwerkelijk meer of minder last heeft van de vormen en schade van cybercriminaliteit.

Overeenkomsten

De ondervonden vormen en schade van cybercriminaliteit van gemeenten lijkt vooral met elkaar overeen te komen. Alle gemeenten hebben last van de 5 typen zoals genoemd door Paoli et al. (2017, p. 31). Meest voorkomende vormen van cybercriminaliteit zijn *phishing* en *spam*, andere vormen komen in wisselende mate voor. Echter zijn de gemeenten niet goed op de hoogte van de daadwerkelijke omvang van de ondervonden vormen omdat ze dit niet voldoende bijhouden of meldingen maken bij de overkoepelende instanties. Ook wat schade betreft zijn de gemeenten niet in staat die te duiden in monetaire waarden. Indirecte schade in de vorm van imagoschade is de vorm waar de gemeenten het meest last van hebben.

Verschillen

De gevonden verschillen zijn te duiden in de omvang van de organisatie en de grootte van de schade. Hoe groter de gemeente hoe meer deze kans heeft om getroffen te worden door cybercriminaliteit vanwege de aanwezigheid van meer mensen, meer data en dus meer digitale systemen. Dit betekent niet per definitie dat de aanwezige schade ook groter is. Een kleine gemeente kan immers minder goed beveiligd zijn en dus meer schade oplopen aan systemen. Daarentegen zijn grotere gemeenten in het bezit van gevoeligere of grotere hoeveelheden data of geld die ze kunnen verliezen. Hier vallen dus geen eenduidige verschillen te benoemen die per definitie gelden.

6.2 Maatregelen voor cyberveiligheid in het beleid

De bespreking van cyberveiligheidsbeleid bij gemeenten valt uiteen in verschillende onderdelen. In het eerste deel komen de beschikbare middelen aan bod. Dan volgen eerst de proactieve maatregelen en vervolgens de reactieve maatregelen. Het vierde punt gaat in op de doeltreffendheid van de maatregelen. Daarna volgt er een bespreking van de genoemde verbeteringen die te realiseren zijn in het beleid. Tot slot is er gekeken naar overeenkomsten en verschillen tussen de cases.

6.2.1 Middelen ter beschikking

De maatregelen die de gemeenten treffen en de middelen die daarvoor beschikbaar worden gesteld zijn uiteengezet in het veiligheidsbeleid en zijn gebaseerd op een afweging van risico's (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 8; Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 4).

In beide landen is door de landelijke overheid een gids/leidraad opgesteld die de gemeenten kunnen gebruiken om hun eigen cyberveiligheidsbeleid op te baseren. Hierin zijn de basismaatregelen die gemeenten zouden moeten treffen opgenomen. In België is dit de BSG en in Nederland de BIG (vanaf 2020 de BIO) die op hun beurt weer zijn gebaseerd op de ISO-normen (CCB, 2018, p. 2; IBD, 2016, p. 6). De BSG en de BIG zijn vormen van zelfregulering en geen wetgeving. Het zijn richtlijnen die iedere gemeente op eigen wijze meeneemt in het beleid waardoor er grote verschillen kunnen ontstaan tussen de gemeenten. Gemeenten zijn daarbij ook niet verplicht gebruik te maken van deze gidsen (CCB, 2018, p. 2; IBD, 2016, p. 3). Er rust geen controle op en de meeste gemeenten zijn niet ISO-gecertificeerd.

Cyberveiligheid hangt bij de gemeenten sterk samen met informatieveiligheid. Dit wordt genoemd door 12 respondenten. Dit heeft te maken met internationale normen, wetgeving en *best practices*. Het informatieveiligheidsbeleid wordt vastgesteld door het College van Burgemeesters en Schepenen/Wethouders (en de Gemeenteraad) (IBD, 2016, p. 8; Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 1). Het beleid "omvat alle bestuurlijke processen, onderliggende informatiesystemen en gegevens (…), het gebruik daarvan door medewerkers en (keten)partners, ongeacht locatie, tijdstip en gebruikte

apparatuur" (Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 5; Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 7). Bij gemeenten 'Y' zijn waar nodig ook aanvullende, specifiekere regels beschikbaar die niet in het algemene beleidsdocument zijn opgenomen. Het beleidsdocument van de gemeente 'Y' is uit 2018 en dus recenter dan het Rapport Informatiebeveiliging uit 2017. In het beleidsdocument wordt het rapport ook genoemd als aanleiding.

De implementatie informatieveiligheidsbeheer kan worden uitgevoerd middels een *Plan, Do, Check, Act* (PDCA)-cyclus. Hierbij worden 4 basisprincipes in gedachten gehouden. Ten eerste de beveiligingsstrategie en ondersteuning, ten tweede een inventaris van activa en risicoanalyse, ten derde de uitvoering van veiligheidsmaatregelen en tot slot de evaluatie en controle van de beveiligingsmaatregelen (CCB, 2018, pp. 5-6; IBD, 2016, p. 10).

Om het beleid tot uitvoering te brengen hebben alle gemeenten zelf mensen in dienst, variërend van een persoon tot enkele tientallen in de grotere gemeenten. Zo kan het zijn dat elke afdeling zijn eigen ICT-beheerder heeft maar het komt ook voor dat de ICT voor de gehele organisatie centraal geregeld wordt. Het gaat dan niet alleen om cyberveiligheid of incidentenbeheer, maar ook om zaken als uitgifte van *hard-* of *software.* In Antwerpen is de ICT-afdeling zelfs volledig verzelfstandigd in de vorm van het bedrijf Digipolis. Ook maken alle onderzochte gemeenten gebruik van serviceproviders of externe experts die bijvoorbeeld software leveren of specifieke taken uitvoeren. Vaak hebben zij meer specialistische kennis in huis dan de mensen die werkzaam bij de gemeenten zelf. Over de exacte aantallen van het (interne of extern ingehuurde) personeel of het beschikbare budget voor cyber- en informatieveiligheid van de gemeenten is voor dit onderzoek geen data beschikbaar gesteld.

Echter is het niet volledig vast te stellen of de maatregelen voldoende gerealiseerd worden. Daarvoor zijn audits nodig en die zijn in zeer beperkte mate beschikbaar, namelijk voor Vlaamse gemeenten in het algemeen in de vorm van het Audit-rapport Vlaanderen en voor gemeenten 'Y' het Rapport Informatiebeveiliging.

6.2.2 Proactieve maatregelen

Proactieve maatregelen bestaan uit preventieve en detective maatregelen. In dit deel wordt in gegaan op proactieve maatregelen die organisatie breed worden meegenomen, fysieke veiligheid (en daarbij behorende noodplan), technische maatregelen en de menselijke factor.

Het is van belang dat cyberveiligheidsmaatregelen organisatie breed vanaf het begin worden meegenomen in de bedrijfsvoering anders wordt het moeilijk en is het eigenlijk al te laat. Door dit wel te doen wordt de effectiviteit van de maatregelen verhoogd:

> "Altijd zul je zien informatieveiligheid is niet niks aparts hè dat hoort net zo bij je bedrijfsvoering als mensen, geld, computers. Maar ook je financiële risico's managen je functiescheiding toepassen et cetera dat hoort allemaal gewoon in je bedrijfsvoering en daar hoort dit ook bij. Daar is dus degene verantwoordelijk voor degenen die het management van dat betreffende tak van sport." (Respondent NL3)

Uit de data-analyse blijkt dat een aantal (grote) gemeenten, cyber heel breed nemen. Voor die respondenten staan cybercriminaliteit en cyberveiligheid binnen de gemeentelijke bedrijfsvoering niet op zichzelf. Zo nemen ze het niet alleen mee in alle lagen en in de volledige breedte van de organisatie, maar ook in de gehele stad, inclusief verschillende partijen als bedrijven, burgers, en/of kritische infrastructuren. Zeker de grote gemeenten maken een grote digitalisering door waarbij publiek en privaat door elkaar heen loopt. Voorbeelden hiervan zijn beveiligingscamera's die niet alleen door de gemeenten worden opgehangen. Dat levert een hoop data op wat daardoor ook een hoop risico's met zich meebrengt. Sommige gemeenten hebben hier speciale beleidsmedewerkers voor die dat specifiek als taak hebben. Dit resulteert ook in de functies van de respondenten bij de gemeenten die een bredere (adviserende) beleidsrol hebben:

> "Hoe je bestuurskundig tegen veiligheid aankijkt (…) als je het niet regelt en gaat fout wordt het uiteindelijk onveilig. Daarmee moet je waken dat je dus niet alles vanuit veiligheid, wij denken dus ook alleen maar vanuit risico's, vanuit de onveiligheid. Maar je moet er dus niet aan de achterkant gaan organiseren, niet primair, want dan begin je… je eindigt bij het einde en je begint niet bij het begin. En dat wat je aan de voorkant kan voorkomen door goed dingen in te regelen voorkom je dat het juist aan die achterkant juist onveilig wordt. Alleen omdat wij zo gefocust zijn op dat risico denken en het veiligheidsdenken, kijk heel veel andere clusters, sociaal, wonen, zorg, economie, zitten helemaal niet zo in dat risico en veiligheid, onveiligheidsdenken en daardoor hebben ze wel te weinig oog over dit

soort aspecten dat kan een onbewuste keuze zijn, nogmaals als het dan fout gaat komt het alsnog bij ons terecht, of kun je als een bewuste keuze zijn want dan hoef je er ook niet van te zijn en als het dan fout gaat lossen ze het toch wel op aan de achterkant. Daarmee hebben wij een soort mandaat he, veiligheid is iets waarmee je alles bestuurlijk mee gedaan krijgt." (Respondent NL5)

Er zijn 8 respondenten die benoemen dat cyberveiligheid niet alleen digitale veiligheid behelst, maar ook samenhangt met fysieke veiligheid. De bescherming vindt plaats op verschillende niveaus. Een veelvoorkomende maatregel is dat medewerkers niet meer toegang krijgen tot informatie dan dat ze nodig hebben voor hun functie. In principe wordt dit in elke gemeente toegepast. De toegangsrechten voor digitale systemen zijn beperkt waardoor misbruik van medewerkers zoveel mogelijk wordt voorkomen. Daarnaast moeten medewerkers soms bij de start van een functie een verklaring van goed gedrag leveren of een vertrouwelijkheidsverklaring ondertekenen. Alle gemeenten hebben dus beperkte toegang tot het gebouw en systemen voor zowel buitenstaanders als medewerkers (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 9). Er zijn 2 respondenten die hierbij benadrukken dat een gemeente desondanks ook klantvriendelijk, toegankelijk en transparant wil blijven naar de burger. Opvallend is dat de bevindingen uit het Audit-rapport Vlaanderen daar niet geheel mee overeenkomen:

> "Het is echter niet omdat iedereen welkom is, dat diensten geen beschermingsmaatregelen moeten nemen voor het afschermen van sommige informatie. Bezoekers kunnen vaak het hele bestuursgebouw rondzwerven. Omdat gevoelige papieren dossiers meestal niet standaard in afgesloten kasten opgeborgen worden, is het relatief gemakkelijk om ze in te kijken. Sommige besturen nemen echter beheersmaatregelen om dit te voorkomen, zoals het gebouw in verschillende afgeschermde zones indelen of het archief en de technische ruimtes afschermen." (Audit Vlaanderen, 2018, p. 31)

Uit het Rapport Informatiebeveiliging (gemeente 'Y') blijkt volgens het informatieveiligheidsbeleid dat "dankzij investeringen in het verleden de belangrijkste bedreigingen, namelijk de bedreigingen van buitenaf, zeer beperkt zijn, maar dat de bedreigen op locatie (lees: in de gebouwen van de gemeente) aandacht behoeven" (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 4).

Andere fysieke maatregelen uiten zich bij zeker 5 gemeenten in het hebben van meerdere datacenters die in sommige gevallen voorzien zijn van noodstroom. Ook zijn er interne netwerken en/of *back-ups* die niet verbonden zijn aan het internet om infecties te voorkomen. Zo zijn ze beter beschermd tegen aanvallen van buitenaf en worden kritieke processen minder kwetsbaar. Die *back-ups* moeten dan wel regelmatig gemaakt worden zodat men niet met verouderde data blijft zitten. Echter heeft niet elke gemeente dat soort maatregelen geïmplementeerd en/of is niet voorzien in een noodplan. Dit is een kostbare maatregel die niet voor iedere gemeente haalbaar is, vooral voor de kleinere gemeenten. Het belang van het hebben van een noodplan blijkt uit EU-wetgeving:

> "(…) de nieuwe NIS-richtlijnen, nieuwe Europese wetgeving. Die aanbieders van essentiële diensten zoals dat in de wet staat. In principe organisaties die een kritische rol vervullen in de samenleving en gebaseerd is op IT. Dat die voldoende veiligheidsmaatregelen moeten nemen om die kritische dienst eigenlijk ten alle tijde te kunnen aanbieden daar komt het in essentie op neer. En nu die wetgeving, ik weet niet hoe dat in Nederland, maar in België is die vorige week omgezet van een Europese directieven naar Belgische wetgeving. De volgende fase zal zijn identificatie van die bedrijven maar in de Europese richtlijn staat [organisatie] er letterlijk in." (Respondent BE2)

Om te voorkomen dat incidenten zich voordoen worden er bepaalde technische maatregelen genomen. Zo is het belangrijk om een technische 'schil' te hebben die zo gesloten als mogelijk is. Het maakt niet uit waar het vandaan komt of wat de motieven zijn, als het maar wordt tegengehouden door bijvoorbeeld *firewalls* en virusscanners. Gemeenten kunnen de risico's voor incidenten die veel voorkomen (op die manier) met behulp van enkele essentiële basismaatregelen zo veel mogelijk indekken. Cybercriminelen hebben vaak genoeg aan een niet bijgewerkt stukje software of een klik op een *phishing* mail om toegang te krijgen tot systemen. Zorgen dat de software up-to-date blijft is echter niet altijd even makkelijk:

> "(…) *vulnerability management*, wat in essentie op neerkomt dat ge een *tool* installeert die al uw servers en andere assets, laptops en whatever afscant en kijkt van hoe kwetsbaar is die voor bepaalde types *malware*. Ook omdat dat in kaart te brengen en om te kijken van ja we moeten wij bepaalde maatregelen nemen om de servers en laptops te beschermen moeten wij onmiddellijk *patchen* of kunnen wij dat uitstellen?

(…) En in een grote organisatie is dat niet mogelijk om continu met alles mee te zijn dat gaat gewoon niet (…).” (Respondent BE2)

Detective maatregelen zijn er in de vorm van virusscanners, programma’s of *tools* zoals ENSIA, die kijken naar afwijkingen in gedrag van een medewerker om te bepalen of die persoon gehackt is. Er zijn 6 respondenten die aangeven dit wel te doen. Niet elke gemeente kan zich daar heel actief mee bezighouden vanwege de kosten, daarnaast ontbreekt de benodigde technische kennis die nodig is om te reageren binnen de eigen organisatie:

> “Wat we niet doen is echt actief op zoek gaan naar inbreuken. Daar heb je ook heel gespecialiseerde *tools* voor, maar ja. Om dat in eigen beheer te doen… Ik ken ook niet echt gemeentes die dat gebruiken (…). ” (Respondent BE4)

Alle gemeenten maken verder gebruik van *loggen*, een technische maatregel voor het bijhouden van overzicht in de ICT-huishouding en van de wijzigingen hierin. Dit gebeurt in sommige gemeenten vrij uitgebreid en in andere slechts in beperkte mate. Wat precies de valt onder uitgebreid of beperk is niet helemaal duidelijk. In totaal geven 4 respondenten aan dat er *logs* worden bijgehouden. *Loggen* is een preventieve maatregel die achteraf helpt vaststellen waar en wanneer een incident zich heeft voorgedaan.

Wanneer er toch een lek ontstaat doet de organisatie er goed aan om een *responsible disclosure* beleid te voeren waarbij het lek gemeld kan worden aan de organisatie die er dan mee aan de slag gaat en een terugkoppeling geeft aan de melder. Dit is een technische maatregel met een menselijk aspect. Slechts 1 gemeente geeft aan dat expliciet te vermelden op de website. Een respondent van een andere gemeente geeft daarover aan dat ze eerst zelf willen controleren hoe de organisatie ervoor staat voor ze communiceren naar de buitenwereld dat er bepaalde zwakheden zouden kunnen zijn. Pas nadat ze zelf tests hebben uitgevoerd zal er in de toekomst naar de buitenwereld gecommuniceerd worden dat ze open staan voor feedback in de vorm van *responsible disclosure.*

Omdat technische maatregelen nooit volledige veiligheid kunnen bieden is het ook van belang dat alle medewerkers zich bewust zijn van de risico’s, zodat het menselijke aspect zo min mogelijk aanleidingen geeft voor incidenten. Dit bewustzijn wordt door alle gemeenten in meer of mindere mate verhoogd door *awareness* campagnes. Die campagnes verschillen in mate/duur en intensiteit. Zo meldt een gemeente dat er van tevoren een campagneplan wordt opgesteld met daarin de verschillende onderdelen en wanneer ze worden uitgevoerd. Voor kleinere gemeenten zijn dit soort maatregelen vaak sporadischer en vormt de directe

aanleiding een cyberaanval. Voorbeelden zijn berichten op het intranet, posters, trainingen, directe mails etc. waarin wordt benadrukt waar de gevaren liggen. Dit soort maatregelen moeten regelmatig herhaald worden en vormen een cyclisch proces, omdat na verloop van tijd de aandacht van mensen verslapt:

> "En soms ja, als mensen mij zien dan worden er heel veel schermen geblokkeerd. Dus op zich vind ik dat wel goed. Op hoe meer plaatsen ik zit, hoe meer bewustzijn dat er is." (Respondent BE5)

6.2.3 Reactieve maatregelen

Reactieve maatregelen vinden plaats achteraf, dus nadat een incident zich heeft voorgedaan. Als eerste komt het noodplan aan bod, dan volgen herstelwerkzaamheden, vervolgens technische maatregelen die genomen kunnen worden nadat incidenten bekend zijn geworden, dan leren van het incident, het melden ervan en tot slot *awareness* creëren bij de medewerkers.

Zoals eerder benoemd draait informatiebeveiliging om risicomanagement. Risicomanagement verdwijnt in de praktijk echter naar de achtergrond, omdat medewerkers vooral bezig zijn met het oplossen van incidenten. Volgens een respondent merken medewerkers van bedrijven een incident snel op, omdat ze direct lijden onder de schade. Daardoor komen ze snel in actie. Overheden zijn loggere organisaties dan bedrijven en veel gemeenten reageren pas als het moet. Een andere respondent meent dat een reactie snel volgen kan wanneer er een 'incident respons plan' is opgesteld waarin staat opgenomen wie waarvoor verantwoordelijk is in bepaalde situaties. Het hebben van een noodplan is een preventieve maatregel met daarin een beschrijving van de reactieve maatregelen die genomen moeten worden bij incidenten. Het kan dan gaan om noodsituaties en kritische processen, maar het kan ook minder ernstige incidenten bevatten.

Nadat een incident zich heeft voorgedaan wordt er gekeken naar wat er mis is gegaan en hoe de schade het beste hersteld kan worden. Een veel voorkomende reactieve maatregel is het isoleren van het incident en het onschadelijk te maken door het bijvoorbeeld te wissen en vervolgens een *back-up* terug te zetten:

> “Mocht er iets misgegaan wordt er in ieder geval gekeken waar het misgelopen is als het gaat om een veiligheidslek dan wordt dat wel onmiddellijk afgesloten tot we weten waarom dat dan toch bestaat dat het lek in ieder geval een gedicht is. En dan wordt er nagekeken dus wordt bekeken in de veiligheidscel of dat te verwijderen is dat dat in de toekomst gebeurt moet altijd afwegen of uw maatregelen haalbaar zijn. (…) op een bepaald moment moet je zeggen van ja we houden rekening met een bepaald risico waar we niet op gaan reageren. Dus als het zich voordoet gaan we wel reageren en zorgen dat het... Maar dat ga je die op grote risico’s doen natuurlijk dat gaat eerder. Dan moet je kijken kosten baten. Wat kost het om dat lek helemaal te dichten. En hoe groot is het risico dat het gaat gebeuren? (…) dat gaat nooit voorkomen, dan zorg je dat je dat oplost op het moment dat het er is.” (Respondent BE3)

Wanneer de eigen accounts weer zijn hersteld moeten er weer inspanningen verricht worden om van bepaalde *blacklist* af te komen. Ook kan imagoschade zoveel mogelijk hersteld worden door geld proberen terug te halen dat verkeerd was overgemaakt door een medewerker. In alle 3 de gevallen was dat grotendeels ook gelukt. Om verdere misbruik te voorkomen noemen 2 gemeente ook een ‘rode knop functie’ waarbij een medewerker onmiddellijk alle toegang kan worden ontzegd. Dit kan ook worden ingezet bij verlies of diefstal van gegevens.

Andere technische maatregelen zijn het blokkeren van aanvallen op de interne *firewall* en wachtwoord *resets* uitvoeren. Verder worden ook bekende gevaarlijke links, bijvoorbeeld naar niet legitieme login pagina’s, technisch geblokkeerd. Wanneer een DDoS aanval plaatsvindt zit er echter vaak niets anders op dan te wachten tot het voorbij is. Vaak duren de aanvallen niet zo lang en heeft het op korte termijn geen zin om de internetprovider te vragen om nog meer bandbreedte om de toegang tot de systemen te herstellen.

Wat de respondenten ook aangeven is dat ze die incidenten wel proberen mee te nemen in het verbeteren van de maatregelen:

> “Maatregelen achteraf ben je sowieso te laat. Ik heb wel de gewoonte, ik had die *cryptolocker* virus dat we binnengekregen hebben, een keer dat ik wist op welk toestel dat ‘t was dat die infectie verholpen is ben ik weleens gaan kijken hoe dat het binnengeraakt is. En heb ik daar dan de les uit geleerd, dat wel natuurlijk. Herstellen

van de schade en proberen in te schatten hoe dat je het in het vervolg kan voorkomen." (Respondent BE4)

Gegevenslekken worden bij Vlaamse gemeenten intern gemeld bij de DPO van de organisatie. Er worden zowel in België als in Nederland meldingen gedaan bij de Politie, maar daar gebeurt "9 van de 10 keer niets mee" (Respondent BE2). Verder hebben de gemeenten vrijwel niets te maken met wetgeving die cybercriminaliteit strafbaar stelt, zoals politie of andere handhavende instanties. Ook worden incidenten gemeld bij het CERT of NCSC die dat dan meenemen in hun waarschuwingen en analyses.

Tot slot is het van belang om, wanneer een incident zich heeft voorgedaan, *awareness* te creëren binnen de organisatie zodat medewerkers op de hoogte zijn van de laatste ontwikkelingen (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 10).

6.2.4 Doeltreffendheid maatregelen

De doeltreffendheid van de maatregelen wordt besproken aan de hand van het bestuur van de gemeenten, de aanwezigheid van ICT-professionals, het meten van de volwassenheidsniveaus en het uitvoeren van audits, samenwerking tussen de gemeenten, de basis set van maatregelen en tot slot het volgen van de opgestelde beleidscyclus.

De mate van uitwerking en dus de doeltreffendheid van dat beleid hangt (onder andere) af van hoe hoog informatieveiligheid op de politieke agenda van bestuurders staat:

"(…) audit dienst die ook aangeeft van dat zij een interne audit hadden gedaan op de *awareness* van medewerkers met betrekking tot privacy security een daaruit viel het op dat de top managementlagen eigenlijk niet zo bewust waren van security en privacy daar hebben we nu een inhaalslag gemaakt, met een *tabletop session* (…). Het is hartstikke essentieel. En dat bewustzijn dat dat moet groeien. Het is een proces." (Respondent NL7)

Daarbij geven de respondenten advies aan beleidsmakers en bestuurders. Het beleid wordt op die manier deels opgesteld door bestuur en deel door ICT- verantwoordelijke:

> "Bij de gemeente is er intern strategisch beleid welke door de CISO in samenwerking met de business wordt opgesteld, hierin is de visie van de gemeente verwerkt. Deze is voor 3 jaar vastgesteld." (Respondent NLx1)

Uit het IBD-rapport komt het volgende bovenstaande naar voren:

> "[Uit de analyse van 331 recente coalitieakkoorden blijkt] dat beveiliging van informatie niet op de politieke agenda's staat. Alles wat direct en zichtbaar bijdraagt aan de dienstverlening aan inwoners en ondernemers kan rekenen op veel belangstelling vanuit de politiek, bestuur en management. Maar informatiebeveiliging heeft niet het imago direct bij te dragen aan dienstverlening. Het wordt gezien als bijzaak, en soms zelf als drempel of last." (IBD & VNG, 2018, p. 10)

Een van de problemen met de praktische omzetting van het beleid naar de IT-werking is dat er enerzijds te weinig mensen binnen de gemeenten werkzaam zijn die zich bezighouden met dit domein en anderzijds dat de mensen die er werkzaam zijn vaak niet genoeg specialistische kennis hebben (Audit Vlaanderen, 2018, p. 17). Er is te veel werk dat moet worden gedaan door een te kleine groep mensen (IBD & VNG, 2018, p. 11). De bestuurders bepalen hierbij hoeveel budget ervoor wordt vrijgemaakt zodat er genoeg mensen kunnen worden aangenomen. Vaak is dit budget onvoldoende toereikend of zelfs afwezig (IBD & VNG, 2018, p. 10).

Het lastige is ook dat het bedrijfsleven dezelfde groep aanspreekt en daarbij veel hogere salarissen kan bieden. Er zijn 11 respondenten die aangeven dat het lastig is om alle werkzaamheden naar behoren uit te kunnen voeren met beperkte middelen. Zo moet er soms externe expertise ingeschakeld worden voor hele specifieke ICT-vragen omdat die kennis intern niet beschikbaar is. Er zijn 2 respondenten die aangeven dat overheden vaak tragere organisaties zijn die in vergelijking met het bedrijfsleven vaak achterlopen. Zo ook op het gebied van ICT en cyberveiligheid. Er zijn minder middelen beschikbaar. En dat terwijl de privacygevoelige gegevens die gemeenten bezitten zeer belangrijk zijn om goed te beveiligen.

De meerderheid van de gemeenten, op 1 na, meet het volwassenheidsniveau van de organisatie niet. Uit het informatiebeveiligingsbeleid van de gemeente 'Y' blijkt dat de gemeente ernaar streeft om op volwassenheidsniveau 3 te zitten. Dat niveau staat voor:

> "[een] gedocumenteerde beheersing, geformaliseerde en gestructureerde uitvoering waarbij de beheersing aantoonbaar is. Dit geeft invulling aan het op professionele wijze afleggen van verantwoording. Dit draagt ertoe bij dat gemeentelijke processen beter beschermd zijn. Dit zal regelmatig worden getoetst door middel van audits (…)." (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 6)

Wel hebben ze een algemeen idee over hoe ze ervoor staan op basis van analyses. In het Informatieveiligheidsbeleid van de Belgische gemeente 'X' (2018, p. 4) staat hier over dat de eerdere genomen maatregelen regelmatig moeten worden geanalyseerd en geëvalueerd op basis van effectiviteit en efficiëntie. Een drietal respondenten, waarvan 2 van dezelfde gemeente, geeft aan dat de gemeente zichzelf heeft laten testen. Zo heeft een van de gemeenten in 2017 een *spear phishing* test laten uitvoeren waaruit bleek dat veel mensen op dingen klikten waar ze niet op hoorden te klikken. De medewerkers zijn dus niet voldoende bewust van de risico's waardoor ze *phishing* niet herkennen en melden. Op basis van die test concludeerde de respondent dat de organisatie niet boven de 1 uit is gekomen wat betreft volwassenheidsniveau. Diezelfde organisatie heeft recenter een ander soort test laten uitvoeren, namelijk een technische hack op afstand (via internet), en daaruit bleek wel dat ze bovengemiddeld goed scoorden. Ook uit het Informatiebeveiligingsbeleid van gemeente 'Y' (2018, p. 21) blijkt dat die gemeente de weerbaarheid test. De grotere gemeenten doen daarbij vaker aan monitoring. Een respondent geeft aan dat de gemeente aan monitoring doet en dat daaruit blijkt de defensie effectief is. Tegen bepaalde vormen maak je echter geen kans, hoeveel je er ook bereid bent in te stoppen, aldus enkele respondenten. Desondanks schatten de meesten (vooral van de grote gemeenten) hun maatregelen in als voldoende doeltreffend:

> "In de praktijk is het behoorlijk doeltreffend. Alleen… Waar je rekening mee moet houden is dat als iemand echt wil, hij toch gewoon binnenkomt." (Respondent NL1)

Slechts 2 respondenten geven aan dat de huidige maatregelen onvoldoende zijn. De respondenten zijn het erover eens dat 100% veiligheid niet bestaat. Dit wordt expliciet genoemd door 7 respondenten en is ook te vinden in de informatieveiligheidsbeleidsdocumenten. In termen van volwassenheidsniveau's zouden volledig afgedekte risico's op niveau 5 zitten. Afhankelijk van hoeveel risico aanvaardbaar is worden verschillende maatregelen genomen:

> "[De BIG] beschrijft de basis set te nemen maatregelen die gelden voor alle processen binnen een gemeente. Zoals gezegd betreft het een basis set van maatregelen, waarbij je kunt stellen dat deze een ruime mate van doeltreffendheid hebben (zowel preventief als reactief). Dat wil niet zeggen dat ze dekkend zijn voor alle situaties. Dit is afhankelijk van het risico van het proces en de risicobereidheid van de gemeente. Hoe hoger het risico (of hoe lager de risicobereidheid) van een proces, hoe meer aanvullingen op de BIG nodig zijn. Daar komen dan eigen inzichten bij kijken en eventuele producten uit de markt teneinde het risico zo veel mogelijk te mitigeren. Het verbeterpunt van de BIG wordt op dit moment ingevuld door de BIO. Dit is een meer pragmatischer baseline, die meer leunt op risicoanalyse." (Respondent NLx1)

Ondanks de redelijk positieve uitspraken van de respondenten blijk uit de rapporten dat eigenlijk in bijna alle gevallen de cyberveiligheid onvoldoende gewaarborgd wordt bij gemeenten. "Lokale besturen lopen aanzienlijke veiligheidsrisico's" (Audit Vlaanderen, 2018, p. 21). Elk bestuur is individueel verantwoordelijk waardoor een structurele aanpak in het informatiebeveiligingsbeleid ontbreekt. Omdat bepaalde aspecten rondom informatiebeveiliging zo groot en complex zijn is samenwerking essentieel. Dit gaat dan zowel om samenwerking tussen besturen, alsmede tussen bestuursniveaus en ook ondersteunende organisaties zoals leveranciers. Zo kan expertise gedeeld worden en problemen efficiënter worden aangepakt.

Verder zijn de basismaatregelen alleen al, zoals het omgaan met incidenten, het bijwerken van de *hard*- en *software*, en het bijhouden van overzichten en wijzigingen, niet voldoende op orde. Pas wanneer alle basismaatregelen op orde zijn kan een kosten-batenanalyse worden gemaakt van informatiebeveiliging (IBD & VNG, 2018, p. 16). Andere risico's zijn dat de informatiebeveiliging onvoldoende op de politieke agenda staat, niet integraal in beeld is gebracht, er te weinig gekwalificeerde mensen in dienst zijn en tot slot dat de complexiteit toeneemt (IBD & VNG, 2018, pp. 4-5). Gemeenten zijn kwetsbaar voor incidenten en maken zich het meest zorgen om de bescherming van persoonsgegevens, verstoring van de ICT-systemen en processen die die kwetsbaar zijn voor verstoringen van buitenaf zoals verkiezingen. Er is geen uniforme werkwijze rondom informatieveiligheid en privacy. Onvoldoende zicht op de risico's zorgt er ook voor dat de risico's die wel in beeld zijn bovenmatig veel aandacht krijgen (IBD & VNG, 2018, p. 11).

Uit het Rapport Informatiebeveiliging blijkt dat de PDCA-cyclus niet gevolgd werd bij de gemeente (Rapport Informatiebeveiliging NL gemeente 'Y', 2017, p. 11). De tussentijdse resultaten werden onvoldoende gemonitord en er werd niet naar gehandeld. Ook ontbraken passende maatregelen die volgden uit systematische en actuele risicoanalyses, die daarbij ook niet volledig werden uitgevoerd. Uit de penetratietesten blijkt zelfs dat er 700 kritieke technische kwetsbaarheiden bij specifieke systemen of applicaties zijn geconstateerd bij de gemeente. Tot slot is het moeilijk percentages te geven over de doeltreffendheid van de maatregelen omdat er geen cijfers beschikbaar zijn.

6.2.5 Verbeteringen

De verbeteringen in de maatregelen en het beleid die mogelijk zijn worden besproken aan de hand van de punten die naar voren komen in de uitgevoerde audits, de nieuwe privacywetgeving, adviseurs van de gemeenten, de menselijke factor, externe leveranciers en tot slot samenwerkingsverbanden.

“Informatieveiligheid is een continu verbeterproces. Het informatieveiligheidsbeleid dient in lijn te zijn met veranderende omstandigheden op allerlei vlakken” (Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 2). Cyberveiligheid is dan ook geen statisch gegeven. Het beleid bevat een cyclisch proces waarbij technische tests, audits of rapportages worden uitgevoerd waarbij er wordt gekeken naar “de kwaliteit van informatie en ICT en compliance aan wet en regelgeving” (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 12). De audits worden zowel uitgevoerd door externen die zijn ingehuurd, als door internen. Die bevindingen dienen als input voor de nieuwe jaarplanning (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 12). Prioriteiten liggen in het verlengde van de risico’s, zoals het op orde brengen van de basis en het versterken van de menselijke schaal (IBD & VNG, 2018, pp. 4-5; Audit Vlaanderen, 2018, pp. 22-25). Ook kan de beheersing van risico’s verbeterd worden door simpele maatregelen, zoals het tijdig bijwerken van systemen, het goed beheren van toegangsrechten, sterke wachtwoorden afdwingen bij medewerkers en het opstellen van een incident respons plan.

In Nederland heeft het Rapport Informatiebeveiliging (gemeente ‘Y’) over de informatiebeveiliging van de Nederlandse gemeente geholpen cyberveiligheid meer op de agenda te krijgen:

> "Het directe effect is geweest dat er een groot programma is gestart. Waarbij allerlei maatregelen zijn genomen door de hele organisatie heen. Om de beveiliging te verbeteren. Ik heb bijvoorbeeld een extern bureau die ons helpt om de volwassenheid van de hele organisatie een tree omhoog te krijgen. Dat soort dingen. *Business continuity management* krijgt ook meer aandacht. Dus dat zijn zaken die wel geholpen hebben." (Respondent NL1)

In dit rapport werd geconcludeerd dat de gemeente de informatieveiligheid onvoldoende op orde had (Rapport Informatiebeveiliging NL gemeente 'Y', 2017, p. 11). Dit rapport is echter alweer deels verouderd volgens 4 Nederlandse respondenten, omdat de impact groot was en de aanbevelingen inmiddels al zoveel mogelijk zijn doorgevoerd in het nieuwe beleid. Zo is de fysieke toegang tot het gebouw bijvoorbeeld aangescherpt en is er permanente bewaking aanwezig. Het rapport zou ook bekend zijn bij andere gemeenten die niet hebben deelgenomen aan dit onderzoek. Desondanks is het rapport relevant omdat het dezelfde bevindingen toont zoals de 2 andere rapportages en het onwaarschijnlijk is dat alle aanbevelingen in korte tijd zijn doorgevoerd bij alle Nederlandse gemeenten.

De laatste jaren staat cyberveiligheid steeds meer op de agenda en er zijn recentelijk al veel verbeteringen geweest. De invoering van de *General Data Protection Regulation* (GDPR) heeft gezorgd voor meer aandacht voor de bescherming van persoonsgegevens waardoor privacy een blijvend aandachtspunt is voor gemeenten:

> "Om aan die wetten te moeten voldoen zijn er wel bepaalde dingen die ge als organisatie moeten ondernemen zoals de GDPR ook een organisatie verplicht om maatregelen te nemen is er met de NIS net hetzelfde. En die maatregelen gaan voor een groot deel gebaseerd zijn op ISO 27001 standaard." (Respondent BE2)

Een andere respondent zegt hierover:

> "Het kan altijd beter. Enerzijds, (…) ik denk dat veel besturen pas in actie komen omdat het moet. Of omdat ze er last van hebben dan spreken we over de GDPR-wetgeving die eigenlijk verplicht van bepaalde maatregelen te nemen. En langs de andere kant ziet je, met het gebeuren natuurlijk, dat de gemeenten gaan er dikkels vanuit dat het vooral imagoschade zal zijn." (Respondent BE4)

Bij deze recente ontwikkelingen plaatsten 3 respondenten kanttekeningen. Zo is soms te veel een kwestie van wat er juridisch is toegestaan en minder van wat er technisch mogelijk is.

Privacy heeft vooralsnog voorrang waardoor de efficiëntie in het geding komt. Zolang er nog geen rechtsspraak is blijft de interpretatie van de wet lastig. Daarbij noemden 2 respondenten dat de Gegevensbeschermingsautoriteit in België een tijd lang geen bestuur heeft gehad waardoor advies uitbleef. Nederland lijkt voorop te lopen, wat ook wordt benoemd door een aantal Vlaamse respondenten:

> "(…) vanuit de Vlaamse overheid is er het de Vlaamse toezicht commissie bijvoorbeeld en de privacy commissie op federaal dan die dan wel met richtsnoeren zijn gekomen eigenlijk ook maar in navolging van Nederland een aantal daar zijn ze ook al een aantal jaren mee bezig. Maar je merkt dat dat in Nederland veel meer afgedwongen wordt of meer controles op zitten ook. Terwijl in... In België is dat toch ja anders geregeld, is een is een ja gemeentebestuur is veel meer op zijn eigen aangewezen om die zaak uit te bouwen." (Respondent BE1)

Verder maken de gemeenten in België gebruik van een (externe) informatieveiligheidsconsulent die advies geeft over informatieveiligheid. Verschillende verantwoordelijkheden worden daarmee duidelijk in kaart gebracht en onafhankelijk handelen wordt benadrukt. Uit het Audit-rapport Vlaanderen (2018, p. 19) blijkt echter wel dat de dienstverlening van de informatieveiligheidsconsulent sterk verschilt bij gemeenten. Recent is de rol van veiligheidsconsulent verworden tot DPO welke zich voornamelijk focust op privacy. Die rol is formeel gescheiden van de gemeente; het gaat om een externe adviserende rol. Echter blijkt in de praktijk dat de functie van informatieveiligheidsconsulent veelal (bij 3 gemeenten) wordt vervuld door iemand die in vaste dienst is van de gemeente en ook vaak nog een andere rol heeft, zoals DPO. Hoewel de functies overlap tonen zijn ze niet geheel hetzelfde. De DPO is een rol die is ontstaan naar aanleiding van de recentelijk ingevoerde GDPR. De informatieveiligheidsconsulent kijkt breder naar informatieveiligheid binnen de organisatie. Hoewel de respondenten aangeven wel voldoende onafhankelijk te zijn in hun rol als informatieveiligheidsconsulent, is het maar de vraag of ze voldoende ruimte krijgen om objectieve bevindingen te terug te koppelen aan het stadsbestuur. Hierbij moet ook gedacht worden aan het aankaarten van negatieve bevindingen zonder gevolgen voor de positie van de persoon. In Nederland zou dit de functionaris gegevensbescherming zijn die een soortgelijke rol heeft. Deze functie wordt nu vaak niet (expliciet) vervuld (IBD, 2016, p. 11). In het beleid van gemeente 'Y' wordt deze rol wel genoemd in relatie met privacy en zou er een nauwe samenwerking moeten zijn met de CISO (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 13).

Toch blijft het belangrijk om organisatie breed bij de medewerkers het belang van cyber- en informatieveiligheid te onderstrepen. Niet alleen de CISO is verantwoordelijk voor beveiligingsvraagstukken binnen de gemeente, ook de proces-eigenaren of lijnmanagers hebben hier een verantwoordelijkheid in. Zij moeten inzien wat het belang is van processen waar zij verantwoordelijk voor zijn en de risico's van bijbehorende beveiligingsmaatregelen kennen die daaraan verbonden zijn (IBD & VNG, 2018, p. 16). Het IBD-rapport benoemt hier echter dat:

> "lijnmanagers de verantwoordelijkheid voor de beveiliging van hun dienst of product onvoldoende [voelen]. Informatiebeveiliging komt in de verantwoording over output en financiën niet aan de orde. Lijnmanagers sturen op output en financiën, niet op het managen van risico's in de informatiebeveiliging." (IBD & VNG, 2018, p. 10)

Niet alleen de lijnmanagers maar al het personeel moet zorgvuldig omgaan met informatie. Het bewustzijn bij hen moet vergroot worden. Dat is misschien nog wel het meest belangrijk omdat mensen vaak de zwakste schakel zijn (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 4): ze klikken verkeerd, voeren beschikbare updates niet uit, hebben geen sterk wachtwoord of vergeten het *locken* van de computer bij het verlaten van de werkplek. De technische maatregelen kunnen dan nog zo geavanceerd zijn, wanneer de gebruikers van de systemen simpele fouten maken hebben die maatregelen simpelweg geen zin. Iedereen heeft dus een verantwoordelijkheid en het is belangrijk dat er bewustzijn wordt gecreëerd. De proceseigenaar is verantwoordelijk voor het veilig gebruiken van informatie binnen dat proces. Hierbij is het van belang dat alle verantwoordelijkheden van iedereen zijn vastgelegd zodat er duidelijkheid over is (Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 14).

Andere verbeterpunten liggen op het vlak van externe leveranciers waarvan gemeenten afhankelijk is voor ICT-voorzieningen en de beveiliging daarvan. Hoewel het daarbij mogelijk is om bij de aanbestedingen aan derde partijen de eisen van het geleverde product te vermelden in het lastenboek is deze procedure niet geheel foutresistent. Zo is het niet voor alle leveranciers mogelijk om te voldoen aan die hoge eisen. Een voorbeeld genoemd door 3 respondenten (van 2 gemeenten) is een waterpomp die de gemeente aanschaft die verbonden onversleuteld is aan het internet en dus *gehackt* zou kunnen worden met alle gevolgen van dien. Een andere respondent meldt dat leveranciers softwarepakketten niet goed beveiligen. Een deel van de informatie wordt niet versleuteld wat de gemeente

kwetsbaar maakt voor data lekken. Dus wanneer nieuwe opdrachten worden aanbesteed moeten de eisen die de gemeente stelt aan de opdracht helder in kaart worden gebracht en zoveel mogelijk worden nageleefd. Wanneer dat niet gebeurd is het onduidelijk wat de wederzijdse verwachtingen zijn en wie waarvoor verantwoordelijk is. Het gaat dus om de invulling van rollen en verantwoordelijkheden waarbij het helder moet zijn wat er van externe software- en IT-dienstleveranciers verwacht wordt met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Anders kan dit problemen opleveren met bijvoorbeeld de opslag van gevoelige gegevens of het uitvoeren van updates. Het lastige hierbij is dat zeker bij de gemeenten met minder gespecialiseerd personeel in eigen dienst de kennis ontbreekt om de eisen goed te formuleren (Audit Vlaanderen, 2018, p. 18). Uit het Audit-rapport Vlaanderen (2018, pp. 34-35) blijkt verder dat winst te behalen valt wanneer de gemeenten samen met hun leveranciers de huidige onduidelijke taakverdeling eenduidig vaststellen.

Om niet elke keer het wiel opnieuw uit te moeten vinden werken gemeenten ook samen met elkaar en met andere partijen:

> "Ik zit… De VVSG heeft een werkgroep informatieveiligheid waar in principe elke veiligheidsconsulent naar toe kan gaan. Daar maak ik deel uit. Maandelijks komen we bij mekaar in Brussel. Daar worden ook praktische dingen uitgelegd. Op die manier heb je ook contact met de anderen." (Respondent BE3)

Zo blijven ze op de hoogte van recente ontwikkelingen en *best practices*. Een voorbeeld daarvan zijn incidenten in de haven van Rotterdam en Antwerpen die met elkaar werden gedeeld waardoor verbeteringen in het beleid konden worden doorgevoerd. Veiligheidswaarschuwingen en dreigingsbeelden worden ook afgegeven door ENISA, het CERT en het NCSC die de respondenten in de gaten houden, al zijn die verder vrijblijvend. Daarnaast volgen de meeste respondenten opleidingen en cursussen waar ze kennis kunnen uitwisselen.

Samenwerkingen met het buitenland zijn nog lastig omdat de gemeenten hun handen al vol hebben aan samenwerkingsverbanden op regionaal en nationaal niveau. Nederland heeft sterke samenwerkingsverbanden, onder andere met overkoepelende organisaties en Gemeenschappelijke Regelingen, wat het lastig maakt om een uniforme werkwijze te hanteren in informatieveiligheid. De rol voor de overkoepelende instanties kan op dit vlak zeker vergroot worden. Zo komt er een gemeenschappelijk netwerk voor gemeenten:

> "Je ziet de laatste tijd wel, ook vanuit de VNG veel meer zaken centraal opgepakt waardoor je als het ware... Een andere situatie… Waardoor je veel meer eenzelfde soort situatie over de gemeentes heen gaat krijgen. Er komt een gemeenschappelijk netwerk, er komt extra informatiebeveiliging. Er is een grote landelijke aanbesteding voor informatiebeveiliging waar geloof ik iets van 330 gemeentes aan deelnemen. Dus je ziet daar wel allemaal op ontwikkeling dat gebied." (Respondent NL3)

Gemeenten zouden samenwerking veel structureler kunnen aanpakken, omdat het voor zowel lokale besturen als voor hun software- en IT-dienstenleveranciers moeilijk blijft om alle uitdagingen rond informatiebeveiliging autonoom aan te pakken. Zo kunnen bijvoorbeeld vertalingen van juridische vereisten naar de dagelijkse praktijk worden vertaald (Audit Vlaanderen, 2018, p. 19). Verder staat hierover in het rapport:

> "Elk lokaal bestuur moet zijn informatiebeveiliging te garanderen. Voor een individueel bestuur is het vaak niet mogelijk om alle vereiste expertises zelf in huis te hebben. In de praktijk is elk bestuur sterk in sommige expertises en vormen andere expertises vaak de zwakke plekken. Bovendien moeten besturen momenteel al te vaak het warm water opnieuw uitvinden. Zo brengen veel organisaties momenteel de maatregelen in kaart in het kader van de [GDPR]. Veel besturen werken daarvoor op eigen houtje aan modellen voor de opmaak van een verwerkingsovereenkomst, een register van verwerkingsactiviteiten of een gegevensbeschermingseffectbeoordeling. Zo'n vertaalslag van regelgeving naar praktische acties is echter geen sinecure." (Audit Vlaanderen, 2018, p. 36)

6.2.6 Overeenkomsten en verschillen cyberveiligheid

Hoewel van de meeste gemeenten het beleid niet is bestudeerd geven de interviews en de selectie van beleidsdocumenten een inzicht in de overeenkomsten en verschillen in cyberveiligheid bij de gemeenten. Een deel van de overeenkomsten en verschillen is onder bovenstaande punten al naar voren gekomen. Hier volgt nog een bespreking van andere dan wel opvallende overeenkomsten en verschillen tussen de cases, zowel tussen de landen als daarbuiten.

Overeenkomsten

De overeenkomsten worden besproken aan de hand van de aanwezigheid van een veiligheidsbeleid en het ontwikkelen van vakkennis, het onvoldoende op orde zijn van de genomen maatregelen, de overeenkomsten in het beleid, de overeenkomsten in wet- en regelgeving en de samenwerkingsverbanden.

Ondanks de praktische uitwerking van het verschil in wet- en regelgeving in de landen vertonen de cases vooral veel overeenkomsten met elkaar. De gemeenten die zijn opgenomen in dit interview hebben allemaal in meer of mindere mate beleid opgesteld om de cyberveiligheid te vergroten en personeel in dienst genomen om het beleid uit te voeren. Dit lijkt vanzelfsprekend, maar er zijn ook gemeenten die bij de contactopname lieten blijken dat er geen beleid aanwezig was. Ondanks dat blijkt dat alle gemeenten structurele tekortkomingen hebben, doen ze het wel beter dan gemeenten die nog niet zo ver zijn. Tevens hebben alle respondenten de mogelijkheid om zich te blijven ontwikkelen binnen hun vakgebied. Dit kan in de vorm van cursussen of opleiding waarvan de kosten worden vergoed door de werkgever. Daar kunnen ze dan ook kennis en *best-practices* uitwisselen.

Een aantal respondenten zijn heel open over de zwakheden binnen de organisatie, terwijl anderen hierin wat voorzichtiger zijn. De respondenten zijn zich allemaal bewust van de risico's en proberen binnen de mogelijkheden van hun functie zaken zo goed mogelijk op orde te stellen. Uit de rapportages van het IBD en Audit Vlaanderen komen ook dezelfde conclusies naar voren. Gemeenten hebben de informatiebeveiliging nog onvoldoende op orde. Alle gemeenten komen structureel personeel te kort en moeten gebruik maken van externe expertise. Opvallend is dat bijna alle respondenten aangeven dat ze niet voldoende middelen hebben voor een effectief cyberveiligheidsbeleid: een te hoge werkdruk, dat ze niet alle maatregelen kunnen doorvoeren die ze graag zouden willen, dat het budget niet voldoende toereikend is en dat ze niet voldoende collega's hebben. Dit is dus tegenstrijdig met de eerdere bevinding dat de respondenten aangeven dat de gemeenten over het algemeen voldoende doeltreffend is met betrekking tot de genomen maatregelen.

Ook het beleid vertoont veel overeenkomsten. Soms zelfs letterlijk, waarbij dit stuk tekst in beide informatieveiligheidsbeleidsdocumenten is opgenomen:

> "[Het] beleid omvat alle bestuurlijke processen, onderliggende informatiesystemen en gegevens van de gemeente en externe partijen, het gebruik daarvan door medewerkers en (keten)partners, in de meest brede zin van het woord, ongeacht

> locatie, tijdstip en gebruikte apparatuur.” (Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 5; Rapport Informatiebeveiliging NL gemeente 'Y', 2017, p. 7)

Verder worden natuurlijk de meest kostbare onderdelen en kritieke processen het zwaarst bewaakt (Informatieveiligheidsbeleid BE gemeente 'X', 2018, p. 4; Informatiebeveiligingsbeleid NL gemeente 'Y', 2018, p. 10). Dit hangt samen met *business continuity management* waarbij continuïteit in de (belangrijkste) werkzaamheden zoveel mogelijk gewaarborgd wordt.

Wat betreft wet- en regelgeving lijken de overkoepelende instanties en de bevindingen bij de gemeenten van beide landen op elkaar. Het zijn parallelle structuren met veel overeenkomsten. Zo hebben beide landen overkoepelende instanties die zich bezighouden met cybercriminaliteit en cyberveiligheid en hebben zij richtlijnen opgesteld in de vorm van de BSG en de BIG. Wel zit er een verschil in dat CERT geen Vlaamse maar een federale organisatie is, wat in Nederland niet mogelijk is omdat Nederland geen federatie is. Echter zijn er wat betreft de wet- en regelgeving vooral veel overeenkomsten, omdat wetgeving zoals de GDPR en de NIS-*Directive* doorwerking hebben in de nationale rechtssystemen. Toch kan de Belgische beleidsmedewerker niet terecht bij de Nederlandse CERT of gebruik maken van ENSIA (en andersom). De gemeenten werken alleen binnen eigen land samen met andere gemeenten of overkoepelende organisaties.

Verschillen

Er zijn een aantal verschillen geconstateerd met betrekking tot de maatregelen voor cyberveiligheid, namelijk de structuur van de organisatie, de grootte van de organisatie en het omzetten van nationaal beleid naar lokaal beleid.

Het grootste verschil zit in de verschillende landen en de daarbij behorende organisatiestructuren in wet- en regelgeving. Zo maken Belgische gemeenten duidelijker gebruik van een informatieveiligheidsconsulent. Alle Nederlandse respondenten geven aan een adviserende rol te hebben waarbij ze het bestuur van de gemeente informeren en adviseren, soms ook ongevraagd. Bij hen is dit geen aparte functie, maar lijkt dit verweven te zijn in de functie van de respondent als bijvoorbeeld CISO.

Een ander verschil dat opvalt tussen de cases onafhankelijk van het land is die tussen grote en kleine gemeenten. Grote gemeenten hebben vaak een uitgebreider beleid, meer budget, meer mensen (en expertise) en een voortrekkersrol. Niet elke gemeente heeft *responsible*

disclosure, *logt* uitgebreid, maakt gebruik van detective software of houdt incidenten bij. Hoe groter de gemeente hoe meer van dit soort maatregelen zijn geïmplementeerd. Kleinere gemeenten volgen vaak het voorbeeld van grotere gemeenten..

De gemeenten werken allemaal met beleidsstukken, maar er is een verschil in hoeverre het beleid ontwikkeld en uitgewerkt is. Zo is het beleid van de Belgische gemeente ‘X’ effectief 6 pagina’s terwijl die van de Nederlandse gemeente ‘Y’ op effectief 17 pagina’s zit. Daarbij heeft de Nederlandse gemeente ‘Y’ voor verschillende specifieke gebieden nog losse beleidsstukken die niet zijn opgenomen in het algemene beleidsdocument. Grote verschillen zijn ook te vinden in hoe lang en intensief de gemeente al bezig is met cyberveiligheid. Dit blijkt onder andere uit het aantal personen dat in de organisatie op dat vlak werkzaam is. Dat varieert van één persoon die er fulltime mee bezig is tot enkele tientallen. Dit hangt samen met de grootte van de organisatie.

Alle gemeenten zijn zich bewust van de ISO-normering en de BSG of de BIG. Omdat die enkel als leidraad dienen maakt niet elke gemeente ook daadwerkelijk gebruik van deze gidsen ontstaan er grote verschillen. Zoals eerder genoemd zijn het geen harde eisen maar slechts richtlijnen en vind er ook geen controle plaats (met boetes of andere maatregelen). Elke gemeente vult het in naar eigen inzicht en stemt het voor zover mogelijk af op de behoeften van de eigen organisatie. Tot slot is een ander verschil dat Antwerpen de beveiliging (samen met Gent) volledig uitbesteedt aan Digipolis, waar andere gemeenten een eigen afdeling of medewerkers hebben binnen de eigen organisatie.

Hoofdstuk 7. Discussie, conclusie en aanbevelingen

In hoofdstuk 7 volgt er een bespreking van de onderzoeksresultaten die worden uiteengezet tegenover het literatuuronderzoek, waarbij ook conclusies worden getrokken. Daarnaast worden een aantal aanbevelingen uiteengezet.

7.1 Discussie en conclusie

De opbouw van de bespreking verloopt in lijn met de volgorde van de onderzoeksvragen waarbij relevante literatuur per onderdeel wordt besproken en daaruit conclusies worden getrokken. In het IBD-rapport staat een belangrijke opmerking die ook van toepassing is op dit onderzoek:

> "De conclusies tonen een gemiddeld beeld van het collectief van alle gemeenten. De resultaten zijn niet zonder meer te extrapoleren naar individuele gemeenten." (IBD & VNG, 2018, p. 5)

7.1.1 Mate van confrontatie met cybercriminaliteit

De eerste onderzoeksvraag focust op de vormen en schade van cybercriminaliteit de gemeenten ondervinden.

Vormen

De gemeenten hebben last van een grote verscheidenheid aan ondervonden schade van cybercriminaliteit die in lijn vallen met de bevindingen in de literatuur. Echter maken ze geen verwijzingen naar wetgeving of typologieën bij het benoemen van die vormen, zoals de 'technologie neutrale' typologie van Paoli et al. (2017, p. 31) waarin verschillende soorten van cybercriminaliteit worden genoemd, namelijk: illegale toegang tot IT-systemen, bedrijfsspionage, gegevens- of systeeminterferentie, cyber afpersing en internetfraude. Van die typen zijn *spam* en *phishing* de vormen die het meest worden genoemd door respondenten. De gemeenten hebben daar op dagelijkse basis last van. Verder komen ook andere vormen voor, zoals bijvoorbeeld DDoS aanvallen, *cyrptolockers* en *defacing.*

Uit de rapportage van het IBD komt een ander beeld naar voren. Hoewel de categorieën uit het rapport niet precies overeenkomen met de eerdergenoemde typologie toont het wel grote overeenkomsten. Uit het rapport blijken vooral ongeautoriseerde toegang en exploitatie van kwetsbaarheden veel voor te komen. Hierbij moet wel vermeld worden dat het rapport waarschijnlijk een vertekend beeld geeft, omdat een melding pas wordt gedaan bij het IBD wanneer een aanval succesvol is en negatieve gevolgen heeft voor de organisatie. Alleen de incidenten die gemeld zijn bij het IBD zijn opgenomen in het rapport.

Wat betreft de wetenschappelijke literatuur die specifiek ingaat op cybercriminaliteit bij (Amerikaanse en Belgische) gemeenten zijn er ook veel overeenkomsten te zien. Nederlandse en Belgische gemeenten worden in toenemende mate afhankelijk van technologieën en zijn daardoor extra gevoelig voor datalekken zoals omschreven door Cliff (2017, pp. 6-8). Verder blijkt zowel uit de literatuur als uit de bevindingen dat gemeenten de incidenten niet goed bijhouden, een deel blijft dus onopgemerkt, en weten niet waarom ze slachtoffer zijn van cybercriminaliteit (Norris & Mateczun, 2017, pp. 3-4). Geconcludeerd kan worden dat Belgische en Nederlandse gemeenten zeer kwetsbaar zijn voor verschillende vormen van cybercriminaliteit, maar hier slecht zicht op hebben.

Schade

De schade wordt in de literatuur onderverdeeld in directe, indirecte en onopgemerkte kosten (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 7; Leukfeldt & Weulen Kranenbarg, 2017, p. 287; Wall, 2007, p. 20). De dragers van de schade worden besproken aan de hand van Greenfield & Paoli (2013). De dragers kunnen individuen zijn, private-sector entiteiten, overheden of de omgeving.

De voornaamste schade die de gemeenten ondervinden van cybercriminaliteit is indirecte schade, namelijk imagoschade, wanneer datalekken of andere fouten bekend worden. Dit wordt door bijna alle respondenten genoemd en komt ook naar voren in het Audit-rapport Vlaanderen en de literatuur (Van der Meulen, 2015, pp. iv-v). De imagoschade wordt hierbij gedragen door de gemeenten zelf. De dragers van de schade van de datalekken zijn de individuen van wie de gegevens zijn gelekt. In mindere mate hebben ze ook last van directe schade, in de vorm van financieel economische schade door bijvoorbeeld tijdsverlies. Deze vorm van schade wordt echter niet bijgehouden waardoor het moeilijk is om hier echte conclusies op te trekken. Ook is er een deel van de schade niet bekend, omdat de meeste gemeenten niet aan monitoring doen (Wall, 2007, p. 20).

Zowel volgens de respondenten als volgens het IBD-rapport (2018, p. 9) is de impact van de schade beperkt, in de literatuur komt dit overeen met marginale schade (Paoli, Visschers, Verstraete, & van Hellemont, 2017, p. 9). Het gaat hier dan zowel om de direct ondervonden schade die uitgedrukt kan worden in monetaire waarden als om de imagoschade. Anders dan bij bedrijven kunnen burgers namelijk niet terecht bij een concurrent van de organisatie, omdat die er niet is. Verzekeringen om de schade af te dekken zoals genoemd door *The Cyber Security Coalition* (2016, p. 3) komen dan ook nergens terug in de resultaten. Dat de impact tot nu toe beperkt was geeft echter geen garantie dat dit in de toekomst ook zo zal blijven. Wanneer gemeenten volledig ontregeld raken door een cyberincident kunnen de gevolgen voor de samenleving erg groot zijn.

Overeenkomsten en verschillen

Opvallend is dat wat betreft de vormen en schade er vooral veel overeenkomsten zijn tussen de gemeenten. Ongeacht de grootte of het land van de gemeenten blijkt uit de resultaten dat ze te maken hebben met dezelfde problematiek. Dit komt overeen met de bevindingen in de literatuur waarin wordt gesteld dat elke organisatie, ongeacht de sector, te maken heeft met cybercriminaliteit (Tully, 2018, pp. 9-10). Voor de Belgische en Nederlandse gemeenten in dit onderzoek is dit dus niet anders.

7.1.2 Maatregelen voor cyberveiligheid in het beleid

De tweede onderzoeksvraag focust zich op de proactieve en reactieve maatregelen die gemeenten hebben opgenomen in hun cyberveiligheidsbeleid. Ook is er gekeken naar of de gemeenten die als doeltreffend ervaarden en welke verbetermogelijkheden zij zagen.

Middelen

De middelen die de gemeenten tot hun beschikking hebben staan omschreven in hun informatieveiligheidsbeleidsstukken. Hierin staan de maatregelen die de gemeenten nemen om de cyberveiligheid binnen de organisatie te vergroten. Het beleid wordt opgesteld door het bestuur van de gemeenten, waarbij een groot deel van de respondenten een adviserende rol heeft. Het beleid van de gemeenten ‘X’en ‘Y’ zijn gebaseerd op de BSG en de BIG. Die zijn op hun beurt weer gebaseerd op de ISO-normen, een van de belangrijkste richtlijnen op het gebied van cyberveiligheid (Van Houten, Spruit, & Wolters, 2015, p. 149). Het is

onduidelijk hoeveel de gemeente investeert in cyberveiligheidsmaatregelen omdat er geen modellen zijn om mee te meten, cyberveiligheid verweven is in producten, processen en projecten en cyberveiligheid voornamelijk vanuit een kwalitatief perspectief wordt benaderd (Van der Meulen, 2015, p. 51).

Alle gemeenten maken verder gebruik van externe expertise, omdat ze zelf onvoldoende kennis en personeel tot hun beschikking hebben. Uit zowel de literatuur als de geanalyseerde rapportages blijkt echter dat de kwaliteitseisen vaak onvoldoende worden gewaarborgd (Nussbaum & Park, 2018, pp. 3-5). Gemeenten doen er dus goed aan heldere afspraken te maken met hun leveranciers zodat bij beiden partijen bekend is wat de wederzijdse verwachtingen zijn.

Maatregelen

Het beleid van de gemeenten bevat een vorm van risicomanagement. Het beleid omschrijft daarbij welke maatregelen er nodig zijn om de basisveiligheid te garanderen. De resultaten laten zien dat de praktische maatregelen die de gemeenten nemen oorsprong vinden in richtlijnen en *best practices.* De gemeenten maken gebruik van fysieke en digitale/technische maatregelen. Concrete voorbeelden van de genomen maatregelen zijn een beperkt toegangsbeleid tot gebouwen, het hebben van verschillende datacenters of het maken van *back-ups*, voorbeelden die ook worden genoemd door onder andere White (2017, p. 52).

Wat betreft transparantie, dat door 2 respondenten is genoemd, is er een sterke overeenkomst te zien met de literatuur. Gemeenten bezitten grote hoeveelheden privacygevoelige data en willen dat voldoende afschermen wat conflicteert met de verwachting van een transparante (maar ook betrouwbare) overheid. De gemeenten zouden er dus goed aan doen om te focussen op duidelijke standaarden, trainingen, software, meer personeel en betere *oversight* op dit gebied (Macmanus, Caruson, & Mcphee, 2016, p. 466; Van Erp, 2017, pp. 81-82).

Ook is er een focus op de menselijke factor, die vaak een zwakke schakel is, al zijn de technische maatregelen nog zo sterk (Van Houten, Spruit, & Wolters, 2015, p. 94). Tot slot worden incidenten waar nodig gemeld bij de instanties, zoals de politie of de CERT, zodat die een beter beeld krijgen van het fenomeen, de incidenten kunnen opvolgen en waarschuwingen of andere resultaten kunnen terugkoppelen naar de gemeenten. Uit de literatuur blijkt echter dat de aangiftebereidheid bij cybercriminaliteit lager is waardoor het *dark number* hoger is en politie en justitie geen goed beeld hebben van de aard en omvang

en schade van daderschap, slachtofferschap en de gevolgen van de verschillende vormen van cybercriminaliteit (Leukfeldt & Weulen Kranenbarg, 2017, p. 287).

Doeltreffendheid en verbeteringen van maatregelen

De besturen van de gemeenten hebben een grote invloed op de mate van doeltreffendheid van de maatregelen en het beleid. Zij bepalen uiteindelijk welke middelen er beschikbaar zijn om de cyberveiligheid te vergroten, dit wordt ook benoemd door Norris & Mateczun (2017, pp. 5-6). Hoe groter het budget en hoe meer medewerkers met ICT-kennis er zijn, hoe beter de gemeente zich kan verzekeren van een goed uitgevoerd beleid.

Volgens een aantal respondenten analyseren de gemeenten de maatregelen en het beleid en kijken waar er ruimte is voor verbetering. Zo is nog niet overal de *business continuity* volledig gegarandeerd. In de praktijk blijkt dat de maatregelen die de gemeenten nemen onvoldoende zijn. Ondanks dat respondenten dit zelf niet als zodanig aangeven blijkt dit wel uit rapportages van het IBD, Audit Vlaanderen en het (verouderde) rapport van gemeente 'Y'. Ook worden volgens de rapportages audits onvoldoende uitgevoerd. De *tools* van ENSIA en V-ICT-OR worden bijvoorbeeld maar in beperkte mate gebruikt. Het volwassenheidsniveau van cyberveiligheid wordt vrijwel nergens gemeten door de gemeenten, een bevinding die overeenkomt met de bevindingen uit de literatuur over cyberveiligheid bij kritische infrastructuren (Van der Meulen, 2015, p. 51). Er zijn echter geen interne rapportages (met kwantitatieve data) beschikbaar gesteld voor dit onderzoek dus is de effectiviteit lastig te beoordelen. Het is daardoor moeilijk te zeggen op welk niveau de gemeenten daadwerkelijk zitten en hoe doeltreffend het beleid is (Papelard & Bobbert, 2018, pp. 58-60; Van Houten, Spruit, & Wolters, 2015, p. 45).

Wat betreft verbeteringen adviseren de respondenten de bestuurders, waardoor cyberveiligheid steeds hoger op de politieke agenda komt en het beleid steeds beter kan worden. De recente ontwikkelingen rondom privacywetgeving (GDPR) hebben hier sterk aan bijgedragen. Die wetgeving is echter niet opgenomen in de literatuur waardoor er geen terugkoppeling gemaakt kan worden op dat vlak. Verder moet er moet meer personeel beschikbaar komen dat beschikt over de juiste kennis en expertise (Tully, 2018, pp. 9-10). Belangrijk is vooral dat de basismaatregelen op orde worden gebracht die zijn opgenomen in het beleid van de gemeenten. De beleidscyclus wordt onvoldoende gevolgd bij gemeenten terwijl die juist zo belangrijk is (Donaldson, Siegel, Williams, & Aslam, 2015, pp. 23-25).

Overeenkomsten en verschillen

De overeenkomsten en verschillen die naar voren komen in de resultaten tussen de gemeenten zijn niet terug te herleiden naar de literatuur, omdat soortgelijk onderzoek ontbreekt. De overeenkomsten dat elke gemeente er goed aan doet een cyberveiligheidsbeleid op te stellen, uit te voeren en te toetsen komt wel terug in de literatuur (Donaldson, Siegel, Williams, & Aslam, 2015, pp. 23-25). Het is dan ook positief dat elke onderzochte gemeente een beleid heeft, zelfs als die gebrekkig is. Ook het eerdergenoemde onvoldoende op orde hebben van de maatregelen is iets wat terugkomt bij de gemeenten en in de literatuur (Norris & Mateczun, 2017, p. 3).

7.2 Aanbevelingen

Wat betreft praktische aanbevelingen op basis van de onderzoeksresultaten liggen die grotendeels in lijn met de eerdergenoemde verbeteringen in de resultaten sectie. Die aanbevelingen zijn ook te vinden in de rapportages van Audit Vlaanderen, het IBD, en die van de gemeente 'Y'. Zo is het zaak om cyberveiligheid hoger op de politieke agenda te krijgen zodat er meer middelen vrijkomen om de organisaties, en daarmee onze samenleving, beter te beschermen. Het gaat dan om een integrale aanpak waarbij gemeenten samenwerken met elkaar en andere instanties waarbij een uniforme aanpak gecreëerd kan worden om de efficiëntie te verhogen. Momenteel vindt er zeer weinig (tot geen) internationale samenwerking plaats terwijl uit dit onderzoek blijkt dat de gemeenten in beide landen meer overeenkomsten met elkaar vertonen dan verschillen. Omdat de wet- en regelgeving niet exact gelijk is zouden vooral *best practices* kunnen worden uitgewisseld. Hierbij kan dan gedacht worden aan nieuwe oplossingen of waarschuwingen, zoals eerder gebeurde tussen de havens van Antwerpen en Rotterdam.

Belangrijk is ook dat de gemeenten beter inzicht krijgen in de vormen en schade van cybercriminaliteit door betere monitoring en audits. Zo is het nu onvoldoende bekend wat de (omvang van de) schade is voor de gemeenten door de ondervonden cybercriminaliteit. Ook weten de gemeenten onvoldoende of de genomen maatregelen voldoende doeltreffend zijn. Ze baseren hun bevindingen meer op gevoel dan op daadwerkelijk gemeten resultaten. De gemeenten zouden er goed aan doen om zich regelmatig onafhankelijk te laten toetsen op kwetsbaarheden zodat goed in kaart wordt gebracht waar de maatregelen nog verbeterd

moeten worden. Daarbij moeten ze beginnen met de basismaatregelen, die nu nog onvoldoende zijn.

Ook kunnen er aanbevelingen gedaan worden voor verder onderzoek. Dit is nodig om zoveel mogelijk te weten te komen over cybercriminaliteit en effectief cyberveiligheidsbeleid om de samenleving zo goed mogelijk te beschermen. Een vervolgonderzoek zou zich kunnen richten op een uitgebreidere literatuurstudie die ook focust op andere wetsgebieden, zoals de recente GDPR. Voor de beeldvorming van de omvang en frequentie van de incidenten zouden de gegevens kunnen worden aangevuld met statistisch/cijfermatig materiaal. Wat betreft de doeltreffendheid van maatregelen geldt hier hetzelfde. Wanneer rapportages die inzicht geven hierin niet verkregen kunnen worden zou dit zou mogelijk kunnen worden gemaakt door middel van *mixed methods* waarbij kwantitatieve en kwalitatieve onderzoeksmethoden worden samengevoegd (Mortelmans, 2013, p. 371).

Daarnaast zou een betere representativiteit bereikt kunnen worden. Dit kan door middel van zowel het spreken van meerdere beleidsmedewerkers en/of bestuurders per gemeente. Ook kan het door middel van het benaderen van meer gemeenten of andere gemeentelijke organisaties voor deelname aan het onderzoek. Een andere aanbeveling richt zich op het gebruik van verdere datatriangulatie, zoals het gebruik van observaties (Baarda, et al., 2013, pp. 75-76). Hierbij kan gedacht worden aan het bijwonen van vergaderingen of het opnemen van bevindingen over de fysieke maatregelen in de bezochte gebouwen. Een ander voorbeeld is het analyseren van uitgevoerde penetratietesten of een situatie waarbij een *cyberhack* gesimuleerd wordt om te zien hoe gemeenten omgaan met daadwerkelijke noodsituaties. Tot slot zou toekomstig onderzoek zich verder kunnen richten op het verschil tussen cybercriminaliteit en cyberveiligheid in overheden en bedrijven of een vergelijking met andere landen kunnen maken om het fenomeen beter in beeld te krijgen.

Bibliografie

Sociaalwetenschappelijke bronnen

Adams, S. A., Brokx, M., Dalla Corte, L., Galič, M., Kala, K., Koops, B.-J., . . . Škorvánek, I. (2015). *The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK.* Tilburg, The Netherlands: Tilburg University.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Red.), *The Economics of Information Security and Privacy* (pp. 265-300). Dordrecht, the Netherlands: Springer.

Audit Vlaanderen. (2018). *Thema-audit Informatiebeveiliging.* Brussel, België: Vlaamse Overheid.

Baarda, B., & Van der Hulst, M. (2017). *Basisboek Interviewen.* Groningen/Houten, Nederland: Noordhoff Uitgevers.

Baarda, B., Bakker, E., Fischer, T., Julsing, M., De Goede, M., Peters, V., & Van der Velden, T. (2013). *Basisboek kwalitatief onderzoek.* Groningen/Houten, Nederland: Noordhoff Uitgevers.

Bennet, D., & Stephens, P. (2014). Preventing Digital Crime. In R. Bryant, & S. Bryant, *Policing Digital Crime* (pp. 64-82). Surrey, UK: Ashgate Publishing Limited.

Benschop, A. (2013). *Cyberoorlog - Slagveld Internet.* Tilburg, Nederland: De Wereld.

Beyens, K., & Tournel, H. (2016). Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview. In T. Decorte, & D. Zaitch (Red.), *Kwalitatieve methoden en technieken in de* (3e ed., pp. 187-220). Leuven/Den Haag, België/Nederland: Acco.

Bijleveld, C. C. (2018). *Methoden en Technieken van Onderzoek in de Criminologie.* Den Haag, Nederland: Boom Juridische Uitgevers.

Binnelands Bestuur. (2017). *BEL-gemeenten getroffen door cyberaanval*. Opgeroepen op 2 6, 2018, van Binnelands Bestuur:

http://www.binnenlandsbestuur.nl/digitaal/nieuws/bel-gemeenten-getroffen-door-cyberaanval.9560940.lynkx

Bobbert, Y., & Broersma, M. (2018). *Cybersecurity in 60 minuten.* Zaltbommel, Nederland: Haystack.

Bobbert, Y., & Mulder, H. (2018). Governance Practices and Critical Success factors suitable for Business Information Security. In T. Papelard, & Y. Bobbert, *Critical Succes Factors for Effective Business Information Security* (pp. 71-96). Zaltbommel, Nederland: Dialoog Publishing.

Bryant, R., & Bryant, S. (Red.). (2014). *Policing Digital Crime.* Surrey, UK: Ashgate Publishing Limited.

CCB. (2018). Baseline Security Guidelines (BSG). Brussel, België: Centrum voor Cybersecirity België.

CCB. (2019). *Centrum voor Cybersecurity Belgium*. Opgehaald van Government: https://www.ccb.belgium.be/nl/government

CCV. (2019). *Cybercrime*. Opgehaald van Centrum voor Criminaliteitspreventie en Veiligheid: https://hetccv.nl/onderwerpen/cybercrime/

CERT. (2019). *Over ons*. Opgehaald van Computer Emergency Response Team: https://www.cert.be/nl/over-ons

Cliff, G. (2017). Growing impact of cybercrime in local government: managers face uphill battle. *Public Management, 99*(5), 6-9.

Clough, J. (2012). The Council of Europe Convention on Cybercrime Defining ‘crime’ in a digital world. *Criminal Law Forum, 23*, 363-391.

Clough, J. (2015). *Principles of cybercrime* (2e ed.). Cambridge, UK: Cambridge University Press.

Cohen, M. A., & Bowles, R. (2010). Estimating Costs of Crime. In A. R. Piquero, & D. Weisburd (Red.), *Handbook of Quantitative Criminology* (pp. 143-162). New York, USA: Springer.

Collins, S., & McCombie, S. (2012). Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism, 7*(1), 80-91.

Commissie van de Europese Gemeenschappen. (2007). Mededeling van de Commisie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's - Naar een algemeen beleid voor de bestrijding van cybercriminaliteit. 1-12. Brussel, België.

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy. Een analyse van de Wet computercriminaliteit III. *Justitiële Verkenningen, 44*(5), 100-117.

De Morgen. (2017). *Eén op de vijf gemeentelijke websites gooit gegevens van inwoners te grabbel*. Opgeroepen op 2 6, 2018, van De Morgen: https://www.demorgen.be/technologie/een-op-de-vijf-gemeentelijke-websites-gooit-gegevens-van-inwoners-te-grabbel-b0e7951b/

Decorte, T. (2016). Kwalitatieve data-analyse. In T. Decorte, & D. Zaitch (Red.), *Kwalitaiteve Methoden en Technieken in de Criminologie* (3e ed., pp. 463-512). Leuven/Den Haag, België/Nederland: Acco.

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.* New York, USA: Springer Science.

ENISA. (2019). *About ENISA.* Opgehaald van European Union Agency for Network and Information Security: https://www.enisa.europa.eu/about-enisa

Finnerty, K., Motha, H., Shah, J., White, Y., Button, M., & Wang, V. (2018). *Cyber Security Breaches Survey 2018.* Opgehaald van https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Firth, C. M., Ayoub, R., & Nayaz, M. (2017). *Cyber resilience in the digital age.* EY. Opgehaald van https://www.ey.com/Publication/vwLUAssets/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region/$File/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region.pdf

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology, 53*(5), 864-885.

Hildebrandt, M., & Koning, M. E. (2012). Universele handhavingsjurisdictie in cyberspace? *Strafblad. het Nieuwe Tijdschrift voor Strafrecht, 3*, 195-203.

Hoogerwerf, A. (2014). Beleid, processen en effecten. In A. Hoogerwerf, & M. Herweijer (Red.), *Overheidsbeleid. Een inleiding in de beleidswetenschap* (9e ed., pp. 17-35?). Alphen aan den Rijn, Nederland: Wolters Kluwer.

IBD & VNG. (2018). *Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020.* Den Haag, Nederland: Informatie Beveiligings Dienst.

IBD. (2016). Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Den Haag, Nederland: Informatie Beveiligings Dienst.

IBD. (2019). *Baseline Informatiebeveiliging Overheid*. Opgehaald van Informatie Beveiligings Dienst: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

Informatiebeveiligingsbeleid NL gemeente 'Y'. (2018). Nederland: [Gemeente 'Y'].

Informatieveiligheidsbeleid BE gemeente 'X'. (2018). België: [BE gemeente 'X'].

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology, 4*(1&2), 26-31.

Kerkhofs, J., & Van Linthout, P. (2010). *Cybercriminaliteit doorgelicht.* Leuven, België: Kluwer.

Kerkhofs, J., & Van Linthout, P. (2013). *Cybercrime.* Brussel, België: Politeia.

Kleemans, E. R., Korf, D. J., & Staring, R. (2008). Mensen van vlees en bloed: Kwalitatief onderzoek in de criminologie. *Boom Lemma Tijdschriften, 50*(4), 323-336.

Koops, B.-J. (2010). *Cybercrime legislation in the Netherlands.* Antwerpen, België: Intersentia.

Koops, B.-J. (2012). De dynamiek van de cybercrime-wetgeving in Europa en Nederland. *Justitiële verkenningen, 38*(1), 9-24.

Koops, B.-J. (2014). Cybercriminaliteit. In S. van der Hof, A. R. Lodder, & G. J. Zwenne (Red.), *Recht en Computer* (6e ed., pp. 213-241). Deventer, Nederland: Kluwer.

Leukefeldt, E., Domenie, M., & Stol, W. (2009). *Verkenning cybercrime in Nederland 2009.* Den Haag, Nederland: Boom Juridische uitgevers.

Leukefeldt, R., Kentgens, A., Barend, F., Toutenhoofd, M., Stol, W., & Stamhuis, E. (2012). *Alledaags politiewerk in een gedigitaliseerde wereld.* Den Haag, Nederland: Boom Lemma Uitgevers.

Leukfeldt, R., & Weulen Kranenbarg, M. (2017). De menselijke factor in cybercrime. *Tijdschrift voor Criminologie, 3*(59), 282-290.

Leys, M., Zaitch, D., & Decorte, T. (2016). De gevalstudie. In T. Decorte, & D. Zaitch (Red.), *Kwalitatieve methoden en technieken in de criminologie* (3 ed., pp. 161-186). Leuven/Den Haag, België/Nederland: Acco.

Luysterborg, E. (2016). *Agreement reached on new EU Network Information Security (NIS) Directive*. Opgehaald van Deloitte: https://www2.deloitte.com/be/en/pages/risk/articles/nis-directive.html#

Macmanus, S. A., Caruson, K., & Mcphee, B. D. (2016). Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs, 35*(4), 451-470.

Maesschalck, J. (2016). Methodologische kwaliteit in het kwalitatief onderzoek. In T. Decorte, & D. Zaitch (Red.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 131-160). Leuven/Den Haag, België/Nederland: Acco.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschetschenko, E. (2013). *Comprehensive Study on Cybercrime - Draft 2013.* UNODC. New York, USA: Untited Nations.

Maynard, C., Ijzinga, N., & Van Veldhuizen, D. (2018). *Why is the NIS Directive so important?* Opgehaald van Deloitte: https://www2.deloitte.com/nl/nl/pages/risk/articles/why-do-you-need-to-know-about-the-nis-directive.html?id=nl:2sm:3tw:eng_risk_corp:nis-directive-cyber-security

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence. Research Report 75. Summary of key findings and implications.* Home Office, Londen, UK.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A methods Sourcebook.* Londen, UK: Sage Publications.

MIVD. (2018). *Jaarverslag 2017.* Militaire Inlichtingen en Veiligheidsdienst. Den Haag, Nederland: Mediacentrum Defensie.

Mortelmans, D. (2013). *Handboek Kwalitatieve Onderzoeksmethoden.* Leuven, België: Acco.

Mortelmans, D. (2016). Het kwalitaitef onderzoeksdesign. In T. Decorte, & D. Zaitch (Red.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 82-130). Leuven/Den Haag, België/Nederland: Acco.

NCTV. (2018). *Cybersecuritybeeld Nederland 2018.* Nationaal Coördinator Terroismebestrijding en Veiligheid. Den Haag, Nederland: Ministerie van Justitie en Veiligheid.

Norris, D. F., & Mateczun, L. (2017). Local Government Cybersecurity in the U.S.: Survey Tells a Cautionary Tale. *Public Management, 99*(11), 2-6.

Nussbaum, B., & Park, S. (2018). Tough Decision Made Easy? Local Government Decision: Making about Contracting for Cybersecurity. *CM International Conference Proceeding Series*, 1-9.

Oerlemans, J.-J. (2017). De Wet computercriminaliteit III: meer handhaving op internet. *Strafblad, 4*(49), 350-359.

Paoli, L., Visschers, J., & Verstraete, C. (2018). *The Impact of Cybercrime on the Belgian government.* Leuven, België: Leuven Institute for Criminology/Centre for IT & IP Law.

Paoli, L., Visschers, J., Verstraete, C., & van Hellemont, E. (2017). *The Impact of Cybercrime on Belgian Businesses.* Leuven, België: Leuven Institute for Criminology/Centre for IT & IP Law.

Papelard, T., & Bobbert, Y. (2018). *Critical Succes Factors for Effective Business Information Security.* Zaltbommel, Nederland: Dialoog Publishing.

Porche, I. R., Sollinger, J. M., & McKay, S. (2011). *A Cyberworm That Knows No Boundaries.* Santa Monica, USA: RAND Corporation.

Port of Rotterdam. (2019). *Organisatie*. Opgehaald van Port of Rotterdam: https://www.portofrotterdam. com/nl/havenbedrijf/over-hethavenbedrijf/organisatie/organisatie

Prins, R. (2013). Voorwoord. In A. Benschop, *Cyberoorlog - Slagveld Internet* (pp. 7-8). Tilburg, Nederland: De Wereld.

RAND Europe. (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* Brussels, Belgium: European Parliament .

(2017). *Rapport Informatiebeveiliging NL gemeente 'Y'.* Nederland: [Gemeente 'Y'].

Rijksoverheid. (2018). *Cybercrime*. Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/cybercrime

Rijksoverheid. (2018). *Nederlandse Cybersecurity Agenda.* Den Haag, Nederland: Rijksoverheid.

Rijksoverheid. (2019). *Nieuwe wet versterkt bestrijding computercriminaliteit*. Opgehaald van De Rijksoverheid: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit?utm_source=e-mailnieuwsbrief&utm_medium=email&utm_campaign=Veiligheid+en+Justitie+Bulletin

Schuilenburg, M., & Van Steden, R. (2016). Positieve veiligheid. Een inleiding. *Tijdschrift over Cultuur en Criminaliteit, 6*(3), 3-18.

Silverman, D. (2013). *Doing qualitative research.* Londen, UK: Sage Publications.

Stol, W. P. (2018). *Burgemeesters in cyberspace.* Opgehaald van VeiligheidsAlliantie regio Rotterdam: https://veiligheidsalliantie.nl/bibliotheek/cybercrime/cijfers-en-achtergronden

The Council of Europe. (2018). *The Council Of Europe's Relations with Observer States*. Opgehaald van Council of Europe Portal: https://www.coe.int/en/web/der/observer-states

The Cyber Security Coalition. (2016). *Cyberveiligheid Gids voor Indicentenbeheer*. Brussel, België: Christine Darville.

The New York Times. (2019). *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*. Opgehaald van The New York Times: https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Thomas, G. (2016). *How to do your case study.* Londen, UK: Sage Publications.

Tully, M. (2018). Local governments a growing target for cyberattacks. *Rochester Business Journal, 34*(9), 9-10.

UNODC. (2017). *Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime.* New York, USA: United Nations.

Van der Meulen, N. (2015). *Investing in Cybersecurity.* WODC, Ministerie van Veiligheid en Justitie. Den Haag, Nederland: Rand Europe.

Van Eecke, P., & Dumortier, J. (2003). De implementatie van het Europese verdrag cybercriminaliteit in de Belgische wetgeving. *Computerrecht: tijdschrift voor informatica en recht, 2*, 123-133.

Van Erp, J. (2017). New governance of corporate cybersecurity: a case study of the petrochemical industry in the Port of Rotterdam. *Crime Law Soc Change, 68*, 75-93.

Van Houten, P., Spruit, M., & Wolters, K. (2015). *Informatiebeveiliging onder controle.* Amsterdam, Nederland: Pearson Benelux.

V-ICT-OR. (2019). *Informatieveiligheidstool*. Opgehaald van Vlaamse ICT Organisatie: https://www.v-ict-or.be/ondersteuning/informatieveiligheidstool

V-ICT-OR. (2019). *Over ons*. Opgehaald van Vlaamse ICT Organisatie: https://www.v-ict-or.be/over-ons

VNG & CCV. (2017). *Inventarisatie Cyberveiligheid.* Den Haag, Nederland: Centrum voor Criminaliteitspreventie en Veiligheid.

VNG. (2019). *ENSIA*. Opgehaald van Vereniging Nederlandse Gemeenten: https://www.vngrealisatie.nl/ensia

VNG. (2019). *Informatieveiligheid*. Opgehaald van Vereniging Nederlandse Gemeenten: https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid

VVSG. (2019). *Over ons*. Opgehaald van Vereniging van Vlaamse Steden en Gemeente: https://www.vvsg.be/over-ons

Wall, D. S. (2007). *Cybercrime: The transformation of Crime in the Information Age.* Cambridge, UK: Polity Press.

White, S. J. (2017). Assessing Cyber Threats and Solutions for Municipalities. In R. M. Clark, & S. Hakim (Red.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 49-65). Switzerland: Springer International Publishing.

WODC. (2019). *Organisatie*. Opgehaald van Wetenschappelijk Onderzoek- en Documentatie Cenrtum: https://www.wodc.nl/organisatie/

Yar, M. (2006). *Cybercrime and society.* London, UK: Sage Publications.

Juridische bronnen

Europees

Eur-Lex. Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio's – Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, 22 mei 2007.

Kaderbesluit 2001/413/JBZ van 28 mei 2001, *betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten*, Pb.L. 2 juni 2001, L 149/1.

Kaderbesluit 2005/222/JBZ van 24 februari 2005, *over aanvallen op informatiesystemen*, Pb.L. 16 maart 2005, L 69/67.

Richtlijn 2011/92/EU van het Europese Parlement en de Raad van 13 december 2011, *ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad*, Pb.L. 17 december 2011, L 335/1.

Richtlijn van het Europese Parlement en de Commissie nr. 2016/1148 van 6 juli 2016, *concerning measures for a high common level of security of network and information systems across the Union*, Pb.L. 19 juli 2016, L 194/2.

Verdrag van Boedapest betreffende de computercriminaliteit van 23 november 2001, *Treaty Series of the Council of Europe* – No. 185, *BS* 21 november 2012, 69.093.

Belgisch

Belgisch Strafwetboek 8 juni 1867, *BS* 9 juni 1867, 3.133.

Memorie van toelichting van het wetsontwerp inzake informaticacriminaliteit, *Gedr. St.* Kamer 1999-2000, nr. 0213/001 en nr. 0214/001.

Wetboek van Strafvordering, *BS* 17 november 1808.

Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, *BS*, 8 augustus 1981. Gewijzigd op *BS* 12 april 1994, *MB* 7 mei 1999, *BS* 25 februari 2003 *MB* 10 mei 2007, *BS* 17 augustus 2013, en op *BS* 21 december 2018.

Wet van 28 november 2000 inzake informaticacriminaliteit, *BS*, 3 februari 2001, 02909.

Nederlands

Kamerstukken II, 1989/90, 21 551 (MvT), nr. 1-3.

Kamerstukken II, 2015/16, 34372 (MvT), nr. 2.

Kamerstukken II, 2015/16, 34372 (MvT), nr. 3, p. 7-15

Rechtbank Leeuwarden 21 Oktober 2008, LJN BG0939; Gerechtshof Leeuwarden 10 November 2009, LJN BK27764 en BK2773; Rechtbank Amsterdam 2 April 2009, LJN BH9789, BH9790, en BH9791.

Rijkswet van 1 juni 2006 tot goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (*Trb*. 2002, 18). *Stb.* 2006, 299.

Wet Computercriminaliteit, *Stb*. 1993, 33.

Wetboek van Strafrecht, *Stb*. 1881, 35.

Wetboek van Strafvordering, *Stb*. 1925, 343.

Bijlagen

Bijlage 1: Contactbrief gemeenten

Geachte mijnheer/mevrouw,

Als master studente *criminology* aan de Katholieke Universiteit Leuven hoop ik dit jaar in het kader van mijn meesterproef onderzoek te doen naar hoe verschillende gemeenten in Nederland en Vlaanderen omgaan met cybercriminaliteit en cyberveiligheid. Dit onder begeleiding van Cedric Verstraete en professor Letizia Paoli. Meer specifiek wil ik met dit onderzoek te weten komen hoe lokale overheden cybercriminaliteit en cyberveiligheid definiëren, met welke vormen ze ervaringen hebben in de eigen organisatie, wat voor schade dit oplevert, wat ze doen om zichzelf te beschermen en wat de verschillen zijn in het Nederlandse en Belgische beleid.

In het kader van dit afstudeeronderzoek ben ik op zoek naar experts die werkzaam zijn op dit vlak. Mijn vraag is dan ook of er binnen de organisatie ruimte is om mij van informatie te voorzien door middel van het afnemen van interviews en/of het leveren van beleidsdocumenten. Het onderzoek richt zich niet uitsluitend op beleidsmedewerkers van gemeenten, dus als er personen zijn die samenwerken met de gemeente op dit gebied verneem ik dat graag.

Bij het uitvoeren van mijn onderzoek zal ik de verzamelde gegevens met de nodige vertrouwelijkheid behandelen en deze uitsluitend voor mijn afstudeeronderzoek gebruiken.

Ik hoop van harte dat u als gemeente uw medewerking wil verlenen. Indien u meer informatie wenst of mij verder kan helpen met deze vraag, kunt u mij altijd bereiken via e-mail: reyhan.cigdem@student.kuleuven.be of telefoon: +31628209616.

Ik dank u om dit verzoek in overweging te nemen.

Met vriendelijke groet,
Reyhan Cigdem

Bijlage 2: Overzicht geanalyseerde beleidsdocumenten

Belgische overheid:

- Thema-audit Informatiebeveiliging 2018 (Audit Vlaanderen)
- BSG (CCB)

Belgische gemeente ‘X’:

- Informatieveiligheidsbeleid 2018

Nederlandse overheid:

- Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020 (IBD & VNG)
- BIG (IBD)

Nederlandse gemeente ‘Y’:

- Informatiebeveiligingsbeleid 2018
- Rapport Informatiebeveiliging 2017

Bijlage 3: Interviewschema

Inleiding

Goeiedag, ik ben Reyhan Cigdem masterstudente aan de Katholieke Universiteit Leuven. Voor dat we starten wil ik u bedanken voor uw tijd en medewerking aan mijn afstudeeronderzoek. Zoals u weet doe ik in het kader van mijn opleiding *criminology* een onderzoek naar hoe de gemeenten België en Nederland omgaan met cybercriminaliteit en cyberveiligheid. Door het afnemen van interviews kan ik de bevindingen uit de literatuur staven, een beeld krijgen van waar beleidsmedewerkers mee te maken hebben in hun werk en hoe het er in de praktijk aan toe gaat.

Indien u er geen bezwaar op heeft wil ik dit gesprek opnemen. Dit vergemakkelijkt de verwerking van het interview aanzienlijk. Ook wil ik benadrukken dat het interview volledig vertrouwelijk is. Dit wil zeggen dat niemand herkenbaar zal zijn in de rapportage en dat na het documenteren van het gesprek de opname zal worden gewist. Buiten ikzelf en mijn begeleiders om zal niemand de volledige inhoud van het gesprek te zien krijgen. Heeft u bezwaar tegen deze opname?

- *Ja, bezwaar*: aangezien het gesprek niet zal worden opgenomen, zal ik uitgebreide notities maken voor de verwerking.
- *Nee, geen bezwaar*: af en toe zal ik aantekeningen maken om het interview te structureren.

Heeft u nog vragen?

Vragen

- Wat is u rol binnen/met de gemeente?
  Alternatieve vraag: Wat houdt uw baan precies in?
    - Wat is de titel van uw functie?
    - Wat zijn uw werkzaamheden?

- Hoe lang vervult u deze rol al?
  Alternatieve vraag: Hoe lang heeft u uw baan al?

- Heeft u een opleiding genoten die te maken heeft met het cyberdomein, voor of tijdens uw baan?
  Alternatieve vraag: Wat was u voorkennis voor u deze baan kreeg en/of heeft u extra opleidingen gevolgd?

- Wat houden volgens u de begrippen ‘cybercriminaliteit’ en ‘cyberveiligheid’ in?
  Alternatieve vraag: Hoe zou u ‘‘cybercriminaliteit’ en ‘cyberveiligheid’ omschrijven?

- Met welke vormen van cybercriminaliteit heeft u te maken in uw werk?
  Alternatieve vraag: Hoe zou u de vormen van cybercriminaliteit omschrijven waarmee u te maken heeft in uw werk?

- In welke mate heeft u of de gemeente last van de schadelijke gevolgen van deze vormen?
  Alternatieve vraag: Welke schade ondervindt u of de gemeente van de verschillende vormen van cybercriminaliteit waarmee u wordt geconfronteerd?

- In welke mate denkt u dat cybercriminaliteit en cyberveiligheid een rol spelen in de samenleving?
  Alternatieve vraag: Welke rol spelen cybercriminaliteit en cyberveiligheid in het algemeen?

- Welke beleidsmaatregelen heeft uw/de organisatie in plaats om de cyberveiligheid te vergroten?
  Alternatieve vraag: Welk beleid is er omtrent cyberveiligheid binnen de gemeente?
    - Hoe zou u de preventieve maatregelen omschrijven?
    - Hoe zou u de reactieve maatregelen omschrijven?
    - Hoe zou u de doeltreffendheid van die maatregelen omschrijven
    - Ziet u verbeter punten in en/of aanvulling op het beleid?

- Hoe wordt het beleid bepaald?

- Met welke actoren werkt u samen?
  Alternatieve vraag: Wie hebben er allemaal te maken met cybercriminaliteit- en het cyberveiligheidsbeleid van de gemeente?

- Denkt u dat er een verschil is in hoe de gemeente als organisatie omgaat met cybercriminaliteit en cyberveiligheid in vergelijking met het beleid van bedrijven?
  - Zo ja: wat is dan het verschil?
  - Zo nee: wat zijn de overeenkomsten?

- Hoe denkt u zelf dat uw gemeente het doet tegenover andere gemeenten (in eigen land)?
  Alternatieve vraag: In welke mate worden verschillen opgemerkt met hoe 'cybercriminaliteit' en 'cyberveiligheid' in andere Nederlandse/Vlaamse gemeenten zal worden aangepakt?
    - Denkt u dat een van de 2 landen beter omgaat met cybercriminaliteit en cyberveiligheid?
      - Zo ja, waarom?
      - Zo nee, waarom niet?

- Heeft u in het dagelijks werk te maken met de Europese wetgeving? Denk hierbij aan het Cybercrimeverdrag/Verdrag van Boedapest of de *Network and Information Security* (NIS) *Directive.*
  - Deze wetgeving is geïmplementeerd in Nederland in de wet computercriminaliteit I & II.
  - Deze wetgeving is geïmplementeerd in België in de wet informatiecriminaliteit.

- Zijn er internationale raamwerken (richtlijnen) verwerkt in het beleid? Zo ja, welke?

- Kunt u iets zeggen over het volwassenheidsniveau (1 tot 5) van de gemeente?

- Heeft u zelf nog aspecten die u wilt bespreken of wat nog niet aan bod is gekomen?

Afronding

Dan zijn we aan het einde van dit interview gekomen. Ik wil u nogmaals bedanken voor uw tijd en medewerking. Indien u nog vragen of opmerkingen heeft over het interview of over de verwerking ervan kunt u mij contacteren via e-mail.