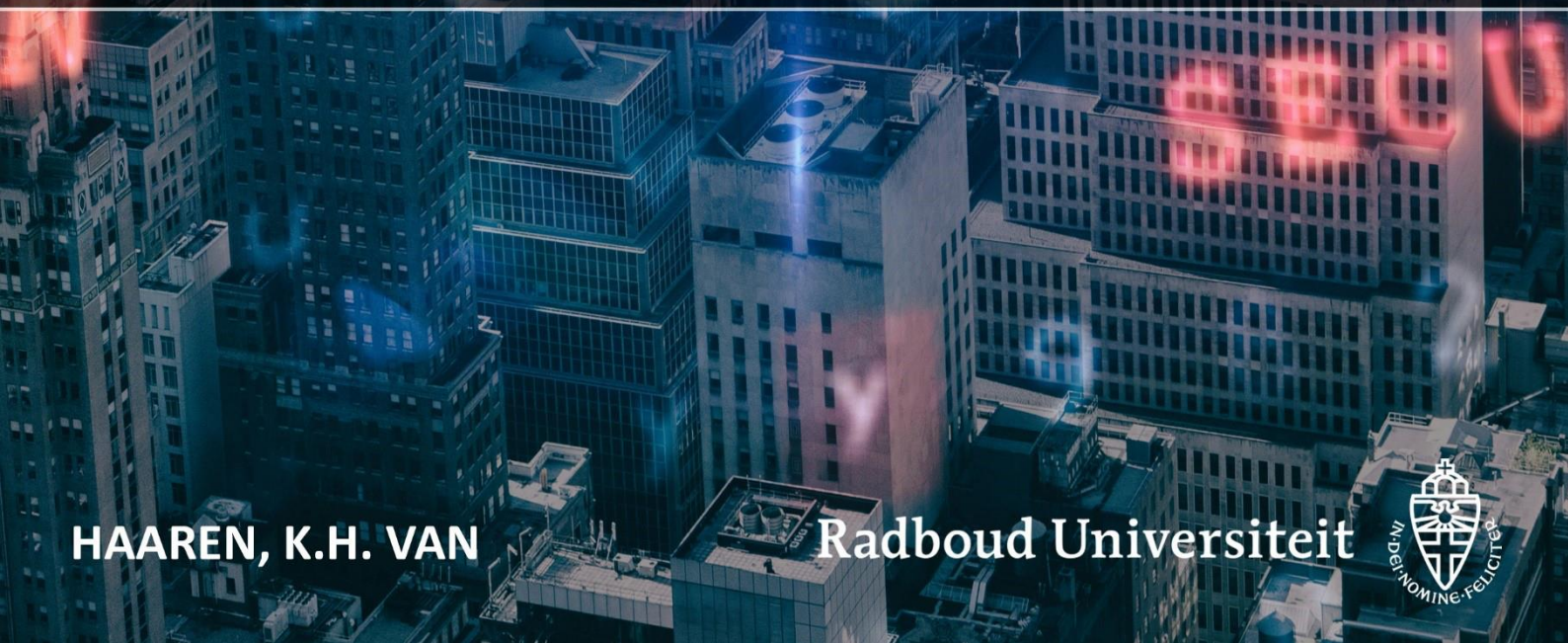
ADAPTATIE IN EEN STEDELIJKE OMGEVING:
AANPASSEN AAN DE ONTZICHTBARE DREIGING

BACHELORSCRIPTIE GEOGRAFIE, PLANOLOGIE EN MILIEU



HAAREN, K.H. VAN

Radboud Universiteit

Adaptatie in een stedelijke omgeving: aanpassen aan de onzichtbare dreiging

Een empirisch onderzoek naar de ontwikkelingen in adaptatie van smart cities aan de bedreiging van cyberaanvallen en –oorlogsvoering.

Bachelorscriptie Geografie, Planologie en Milieu

Auteur: Haaren, K.H. van (Kevin)
Studentnummer: s4318145
Datum: 17 augustus 2018
Aantal woorden hoofdtekst: 18.987
Begeleider: dr. ir. Smith, L. (Lothar)
Tweede corrector: prof. dr. Houtum, H.J. van (Henk)
Onderwijsinstelling: Radboud Universiteit Nijmegen

Foto omslag: vectorfusionart. (n.d.). *Virusbackground against view of cityscape.* Royalty-free stock illustration ID: 581478139. Shutterstock.

Voorwoord

De bachelorscriptie die hier nu voor u ligt is mijn laatste project binnen mijn bachelor Geografie, Planologie en Milieu aan de Radboud Universiteit in Nijmegen. Met dit onderzoek kreeg ik de mogelijkheid om de verschillende aspecten van mijn bachelor te combineren met een onderwerp dat in een zekere zin gerelateerd is aan de master die ik aankomend studiejaar wil beginnen. In een wereld waar het digitale domein een steeds grotere rol gaat spelen, is cybersecurity van groot belang. Nederland speelt een leidende rol wanneer het aankomt op cybersecurity. Afgelopen jaar nam Nederland dan ook het initiatief om een internationale conferentie te houden over het onderwerp in Den Haag, de stad die ik behandel in mijn case. Daarnaast heeft het smart city concept mij aangetrokken, omdat ik het belang ervan inzag dat ook steden met de tijd mee moeten gaan. Deze twee aspecten vonden elkaar al snel en vormde zo het onderwerp voor mijn scriptie.

Ik wil graag mijn begeleider, Lothar Smith, graag bedanken voor de steun gegeven bij dit project en voor het vertrouwen in mijn kunnen. Ook wil ik graag een hulde brengen aan alle mensen die me hebben geholpen een beter inzicht te krijgen in de cybersecurity van smart cities, met speciale aandacht voor de geïnterviewden die mij de kans hebben gegeven om mijn onderzoek uit te voeren. Den Haag als stad was een interessant case om te bestuderen en de stad heeft zichzelf bij mij op de kaart gezet als een stad die klaar is voor de toekomst en deze met open armen verwelkomt. Tot slot wil ik mijn familie, vriendin en vrienden bedanken voor hun steun tijdens het schrijven van deze scriptie en in speciaal ook Sander van der Goes voor het doornemen van mijn volledige scriptie en het geven van feedback.

Ik hoop dat u deze scriptie interessant vindt en dat het helpt uw horizon te verbreden op het gebied van smart city cybersecurity.

Kevin van Haaren

Nijmegen, augustus 2018

Inhoudsopgave

Samenvatting

De cyberaanvallen op de Estse regering in 2007 begonnen als kleine aanvallen waarvan het doel was de digitale infrastructuur te verstoren. Echter, vond er op 9 mei 2007 een grote aanval plaats waarmee het hele Estse internetsysteem werd platgelegd (Ashmore, 2009). Drie weken lang lag de digitale infrastructuur van Estland plat, met als gevolg dat de Estse bevolking geen gebruik meer kon maken van verschillende overheidsdiensten. Deze cyberaanvallen illustreren de kwetsbaarheid van smart cities met een kritieke infrastructuur die aangesloten is op het digitale netwerk. De opkomst van smart cities zorgt ervoor dat steden steeds vaker in aanraking komen met ICT. De ontwikkelingen die zich voordoen uit de innovatie op het gebied van ICT worden geïmplementeerd bij verschillende kritieke systemen in de stad (Ernst & Young, 2016). Maar deze digitalisering van de stad brengt ook de nodige cyberdreigingen met zich mee. De kwetsbaarheid van steden wordt op dit moment vergroot door de complexiteit van de systemen en de wereldwijd verbonden sociaaleconomische en politieke subsystemen van de stad (Kanter & Litow, 2009). Dit gebeurt omdat smart cities nog niet voldoende hebben geïnvesteerd in cybersecurity. Met het oog op deze dreiging, zou cybersecurity een hoge plek moeten krijgen op de agenda van elke smart city.

Daarom heeft dit onderzoek als doel om meer inzicht en kennis te verwerven in de preventie- en adaptatie mogelijkheden van cybersecurity omtrent smart cities. De hoofdvraag van dit onderzoek luidt dan ook als volgt:

Welke ex ante en ex post mogelijkheden zijn er voor een smart city om zich aan te passen aan cyberdreigingen en daarmee hun cybersecurity te waarborgen?

Om de hoofdvraag zo goed mogelijk te kunnen beantwoorden, zullen de volgende deelvragen worden gesteld:

- *Hoe vormen cyberaanvallen een dreiging voor smart cities?*
- *Wat zijn de zwakke punten in het smart netwerk die bij kunnen dragen aan de kwetsbaarheid van smart cities?*
- *Welke maatregelen zijn er te treffen om smart cities weerbaarder te maken?*
- *Hoe kunnen de verschillende manieren van cybersecurity geïmplementeerd worden in huidig (stedelijk) beleid?*
- *Wat is de gepercipieerde urgentie van cybersecurity verbetering ten behoeve van een smart city en wat zijn de kosten die hierbij komen kijken?*

De smart city is, naast cyberdreigingen en –security, de hoofdfocus van deze scriptie. Het concept smart city werd begin deze eeuw leven ingeblazen en beschreef een stad waarbij een gedigitaliseerde infrastructuur om economische en politieke situaties te verbeteren, een van de kernwaarden is. Naast deze kernwaarde staat de smart city ook in het teken van het verbeteren en digitalisering van de dienstverlening aan haar inwoners (Caragliu et al, 2011). Deze inwoners leven in een maatschappij waarin een netwerk gedreven door ICT centraal staat en iedereen zijn eigen functie heeft binnen dit netwerk (Castells, 2004). De ICT toegepast in een smart city is fundamenteel voor de organisatie van de stad en haar activiteiten. De stromen van informatie en (menselijk) kapitaal worden verzorgd door deze ICT en het daarbij behorende netwerk (Castells, 2004). Echter, is deze stroom van informatie en kapitaal niet altijd veilig. Verschillende cyberdreigingen verstoren het dagelijkse proces dat plaatsvindt in smart cities en zijn erop uit om gevoelige informatie te bemachtigen of de kritieke infrastructuur

van een stad te manipuleren of saboteren. De aanvallen op deze kritieke sectoren kunnen dan ook ernstige gevolgen teweegbrengen, zowel op korte als lange termijn (Choo, 2011). Om dit tegen te gaan moeten smart cities de nadruk leggen op het beveiligen en weerbaar maken van hun netwerk en systemen (Van der Meulen & Lodder, 2014). Ook moeten zij het cybersecuritybeleid dat ze voeren aanscherpen, aangezien het beleidskader vandaag de dag niet toereikend genoeg is om de problemen rondom deze cyberdreigingen systematisch op te lossen. Tenslotte moeten zij de parameters te specificeren om deze ontwikkelingen tegen te gaan (Harknett & Stever, 2011).

Om goed antwoord te kunnen geven op de hoofd- en deelvragen van dit onderzoek, wordt er gebruikt gemaakt van een case study. De case van dit onderzoek is de gemeente Den Haag, omdat zij zich al een aantal jaar profileert als smart city door het toepassen van ICT in haar stedelijk gebied en ze zich in Nederland voornamelijk bezighouden met het safety en security aspect van smart cities. Dit onderzoek bestaat voornamelijk uit literatuuronderzoek en er zijn drie interviews afgenomen met experts van verschillende instanties om zoveel mogelijk invalshoeken op het onderwerp te kunnen benaderen.

De uitkomsten van dit onderzoek komen grotendeels overeen met de verwachtingen. Cyberdreigingen kunnen van verschillende actoren komen, ieder met hun eigen motieven (Lin et al, 2017). Daarnaast verschilt ook elke cyberaanval in omvang en gevolgen. De ene cyberaanval wordt gebruikt om persoonsgegevens en gevoelige informatie mee te stelen, terwijl de andere aanval hele systemen kan platleggen voor meerdere uren (Li et al, 2012). Natuurlijk zijn smart cities niet machteloos tegen deze aanvallen. Zo hebben ze de keuze uit meerdere vormen van maatregelen om zich weerbaar te maken tegen cyberdreigingen. Deze vormen omvatten het technologische, procedurele en menselijk aspect van cybersecuritymaatregelen. Technologische maatregelen omvatten onder andere firewalls, virusscanners en een goede monitoring van het netwerk (Ernst & Young, 2016). Procedurele maatregelen omvat onder andere het opstellen van een cybersecuritykader om zo goed mogelijk in te kunnen spelen op cyberdreigingen (Jackson et al, 2017). En menselijke maatregelen omvatten onder andere cyberawareness campagnes en *fear appeals* om inwoners van smart cities bewust te maken van cyberdreigingen en –security (Johnston & Warkentin, 2010). Verder moeten smart cities zich bezighouden met het opstellen of aanpassen van beleid dat goed aansluit op de technologische ontwikkelingen en een ondergrond kan bieden voor toekomstige veranderingen in cybersecuritybeleid (Eger & Maggipinto, 2010). Bij deze besluitvorming is het van groot belang dat overheden een samenwerking met zowel private partijen als hun burgers aangaan, om zo een beleid te vormen dat van toepassing is op alle betrokken partijen (Rashman & Hartley, 2002). De kosten voor deze aanpassingen in beleid en het opzetten van een sterke verdedigingslinie zijn vaak al terug te vinden in een gemeente breed inkoopbeleid (Van Engelshoven, 2015).

Al met al hebben smart cities genoeg mogelijkheden om zich te verdedigen tegen cyberdreigingen. Zowel ex ante als ex post zijn er meerdere opties die smart cities kunnen toepassen om hun veiligheid te waarborgen. Van firewalls en end-to-end encryptie tot aan cyberawareness campagnes en trainingen. Er zijn derhalve genoeg maatregelen om cybercriminelen buiten de deur te houden. De kwaliteit van cybersecurity waarmee smart cities hun netwerk beveiligingen is van cruciaal belang, want de ketting is net zo sterk als zijn zwakste schakel.

1. Het probleem van de onzichtbare dreiging

1.1. Projectkader

In 2007 zorgde het weghalen van een oorlogsmonument voor de nodige onrust in Estland, met name in Tallinn. Tijdens deze periode van onrust werden computers van de Estse regering en Estse nationale media gehackt. De aanvallen begonnen klein, maar dat veranderde al snel toen op 9 mei 2007 een grote cyberaanval werd uitgevoerd met als doel het platleggen van het Estse internetsysteem (Ashmore, 2009). Voor deze aanval werden er wereldwijd ongeveer een miljoen computers gebruikt (Germain, 2008). Drie wekenlang lag Estlands cyberinfrastructuur eruit, met alle gevolgen van dien. De Estse overheid gaf de schuld aan een groep Russische hackers, maar de Russische overheid ontkende hierbij betrokken te zijn. Veiligheidsexperts speculeerde dat dit een van de manieren was waarop een bepaalde groepering protesteerden tegen het besluit van de Estse overheid om het oorlogsmonument te verplaatsen (Gandhi et al, 2011). De Esten waren in staat om op tijd te reageren en zo permanente schade aan hun ICT-infrastructuur te voorkomen. Echter, konden de Esten er niet achter komen vanuit waar deze aanvallen waren ingezet, omdat de hackers gebruik maakten van nep IP-adressen (Ashmore, 2009). Deze cyberaanvallen op Estland illustreren de kwetsbaarheid van elke stad waarbij kritieke systemen afhankelijk zijn van het internet. De implementatie van de ontwikkelingen op het gebied van ICT kunnen de interactie tussen groepen en individuen verbeteren, maar is nog steeds kwetsbaar voor aanvallen en onderbrekingen.

Deze cyberoorlog en andere kleinschaligere conflicten houden de mensheid al jarenlang bezig. Vanaf het begin der tijden heeft men te maken met technologische ontwikkelingen. Hiermee verandert ook de manier waarop conflicten benaderd worden. Vandaag de dag vindt er een revolutie plaats op het gebied van oorlogsvoering en wordt de angst voor de onzichtbare dreiging steeds groter (Janczewski & Colarik, 2008). Onbemande voertuigen maken steeds vaker hun entree op het slagveld, terwijl hackers het slagveld controleren vanaf een computer (Van Bever, 2012). Deze dreigingen functioneren niet op de manier waarop conventioneel wapentuig wordt ingezet om te strijden voor de vrijheid van anderen. Van een afstand zijn zij heer en meester over het gevechtsterrein en dat baat mensen zorgen. Conventioneel wapentuig kan worden bestreden met ander conventioneel wapentuig, maar wanneer men tegen over de onzichtbare dreiging staat, is men vaak machteloos en lijkt het net of God vanuit de hemel neerslaat (Gregory, 2012). Naast de controle over het slagveld, krijgen hackers ook steeds vaker toegang tot systemen die cruciaal zijn voor het onderhouden van de infrastructuur. Hiermee wordt de kwetsbaarheid van onze hedendaagse infrastructuur blootgelegd. Volgens William Church (2000), oud-directeur van het *Center for Infrastructural Warfare Studies*, zal de volgende grens van infrastructurele oorlogsvoering door de staat de ontwikkeling van capaciteiten om gecoördineerde cyberaanvallen uit te voeren zijn. Het zou een uitdaging zijn om in te breken in de computersystemen waarmee infrastructuur van een land wordt gecontroleerd, om daarmee dan een land gegijzeld te kunnen houden (Church, 2000).

Door de opkomst van smart cities komen steden vaker in aanraking met ICT. Deze innovaties worden dan toegepast op verschillende systemen binnen een stad, zoals de infrastructuur, het energienetwerk en hulpdiensten (Ernst & Young, 2016). Deze digitalisering van steden brengt natuurlijk ook de nodige cyberaanvallen met zich mee, omdat deze steden zich kwetsbaarder opstellen door zich aan te sluiten op het internet. Deze cyberaanvallen worden gezien als een dreiging die catastrofale gevolgen kan hebben (Jin et al, 2014). De innovaties in de informatietechnologie die geleid hebben tot de opkomst

van smart cities brengen, naast nieuwe sociaaleconomische kansen, ook weer nieuwe uitdagingen omtrent cybersecurity met zich mee. Veel van de systemen verbinden de stad en zijn inwoners onderling met elkaar. Door het gebruik van deze systemen nemen de standaarden van onze kwaliteit van leven toe (Ernst & Young, 2016). Om hieraan te voldoen moet ook de stedelijke infrastructuur en bijbehorende diensten worden aangepast (Elmaghraby & Losavio, 2014). Een juist getimede cyberaanval kan binnen een korte tijd het digitale netwerk van een stad plat leggen en daarmee fysieke verstoringen creëren in de infrastructuur en de beschikbaarheid van (hulp)diensten. Het is van groot belang om te kijken hoe steden zich kunnen weren door toepassingen vanuit de cybersecurity om dit te voorkomen en hiermee hun kwetsbaarheid te verminderen. Hierbij moet er worden gehouden met het persoonlijke leven van mensen, educatie, gezondheidszorg, ondernemers en handel, de fysieke infrastructuur en ook de nationale veiligheid.

De kwetsbaarheid van steden wordt op dit moment vergroot door de complexiteit van de systemen van de stad en de wereldwijd verbonden sociaaleconomische en politieke subsystemen (Kanter & Litow, 2009). Dit gebeurt omdat steden nog niet voldoende zijn beveiligd tegen cyberaanvallen, welke globaal kunnen worden opgezet en uitgevoerd. Een dreiging van een cyberaanval wordt steeds groter omdat er een oneindige hoeveelheid gegevens steeds meer binnen het handbereik komt. Met het oog op deze dreigingen, zou cybersecurity een hoge plek moeten krijgen op de agenda van elke smart city.

1.1.1. Maatschappelijke relevantie

Door het hedendaags gebruik van het internet is de kans op cyberaanvallen aanzienlijk toegenomen. Sociaaleconomische en politieke subsystemen, maar ook private partijen zijn dagelijks het doelwit voor cyberaanvallen volgens het Nationaal Cyber Security Centrum (2014). In het verslag van Ernst & Young (2016) over de cybersecurity van smart cities staat dat wanneer men het risico op cyberaanvallen effectief wil managen, het belangrijk is om eerst vast te leggen wat de grenzen zijn van dat ecosysteem. Smart city-modellen moeten voor een boost zorgen bij het tot stand komen van smart cities, maar indien niet goed uitgevoerd kunnen de grenzen van dit ecosysteem overschrijden worden en wordt de dataprivacy en beveiliging gecompromitteerd (Ernst & Young, 2016). Daarnaast is het ook belangrijk om te weten in welke categorieën men deze risico's kan vinden.

Figuur 1. Categorieën met risico op cyberaanvallen binnen een smart city. Bron: Ernst & Young

De categorieën aangegeven in het zogenoemde *risks landscape* brengen allen grote veranderingen mee in het dagelijks leven van mensen wanneer deze onder aanval zijn van een cyberdreiging. Een cyberaanval op de infrastructuur alleen al kan leiden tot onvoorziene schade met de daarbij behorende kosten (Elmaghraby & Losavio, 2014). Zo was in 2016 een waterzuiveringsinstallatie in de Verenigde Staten het doelwit van een cyberaanval. De aanvallers veranderden het niveau van chemicaliën gebruikt om het water te zuiveren en de gegevens van 2,5 miljoen huishoudens waren aangetast (Cerrudo, 2018). Het is relevant om uit te zoeken hoe deze dreiging zich tot uiting brengt en hoe een stad zich op deze dreiging dient aan te passen. In heel de wereld nemen cyberaanvallen toe, zo ook in Nederland. Het is dan ook belangrijk om in de toekomst een oplossing te hebben voor deze bedreiging en om te weten hoe we onszelf en onze steden kunnen aanpassen om deze aanvallen voor te zijn.

1.1.2. Wetenschappelijke relevantie

In de wetenschap is er al veel onderzoek gedaan naar cyberdreigingen en de bijbehorende veiligheidsmaatregelen. Over de hele wereld is er sprake van deze bedreiging en daarvoor zoekt men oplossingen (Cerrudo, 2015). Echter, voor de adaptatie van smart cities aan deze tegenwoordig meer en meer voorkomende bedreiging bestaat er nog steeds een hiaat in de wetenschappelijke literatuur Dit komt doordat andere onderzoeken voornamelijk de diepte ingaan omtrent nationaal beleid of hun focus leggen op de interne processen binnen een smart city, zoals de stedelijke economie of burgerparticipatie. In de geschreven literatuur wordt vaak alleen gesproken over de dreigingen die zich voor doen, hoe deze dreigingen resulteren in bepaalde gevolgen en hoe er gereageerd wordt op deze gevolgen. Weinigen spreken over hoe een stad zich kan aanpassen op deze dreigingen om voorbereid te zijn en daarmee te gevolgen niet hoeven te dragen.

In dit onderzoek zal ook worden ingegaan op de anterieure en posterieure effecten van cybersecurity. Door het onderzoeken van beide momenten in het proces van cybersecurity interventies, kan er kennis worden opgedaan om tot een efficiëntere vorm van cybersecurity te komen. De maatregelen die ontstaan uit deze kennis kunnen dan zowel preventief worden toegepast als repressief.

Meerdere onderzoeksinstanties, zoals het *Institute for Housing and Urban Development Studies Erasmus* in Rotterdam en het *African Center for Cities* in Kaapstad, houden zich beide bezig met de ontwikkeling van smart cities op zowel nationaal als internationaal gebied, maar bieden nog geen inzicht in de bedreigingen op het gebied van cyberaanvallen. Deze instanties houden zich voornamelijk bezig met het onderzoeken van het opzetten en verbeteren van smart cities en het beschermen van deze steden tegen klimaatsverandering en criminaliteit.

1.2. Doelstelling

Vandaag de dag neemt het aantal cyberdreigingen toe en daarmee dus ook de kwetsbaarheid van kritieke (sub)systemen in de stad, zoals *smart traffic control, smart energy management* en stedelijke beveiliging (Cerrudo, 2015). De al eerdergenoemde categorieën uit het *risk landscape* komen bloot te liggen voor aanvallen, omdat de snelle technologische ontwikkelingen op het gebied van ICT niet kunnen worden bijgehouden door de implementatie van toereikende cybersecurity (Ernst & Young, 2016). Hiermee wordt de leefbaarheid inclusief de veiligheid van de stad in gevaar gebracht. Dit valt ook terug te zien op economisch gebied. Bedrijven en inwoners van een stad ondervinden negatieve gevolgen als uitkomst van het openbaar maken van aanvallen op informatie en cybersecuritygebied (Campbell et al, 2003). Om het economisch welzijn van de stad te waarborgen, is het essentieel dat

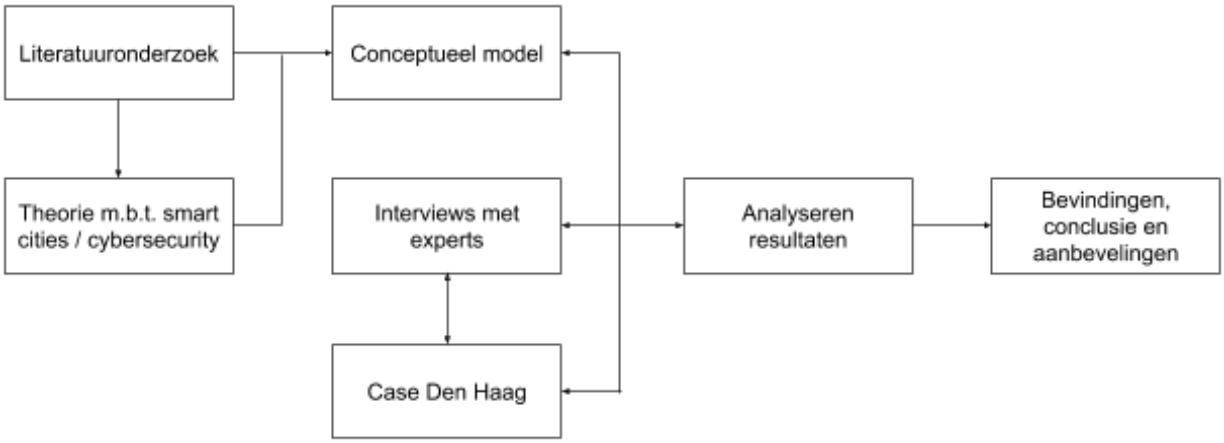
het vertrouwen in diensten op het gebied van cybersecurity behouden blijft (Borrett et al, 2013). Er moet worden afgevraagd of deze dergelijke aanvallen te voorkomen zijn en op welke manier dit kan gebeuren. Al eerder heeft de Nederlandse overheid een beleid opgesteld in samenwerking met publieke en private partijen omtrent het cybersecuritybeeld van Nederland. Het doel van dit beleid is het bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. Echter, is er op dit moment nog geen antwoord op de vraag welke preventiemaatregelen er genomen moeten worden op deze dreigingen te voorkomen. Met dit onderzoek zal er dan ook naar meer inzicht worden gezocht voor dit maatschappelijke vraagstuk.

Het doel van dit onderzoek is meer inzicht en kennis verwerven in de adaptatie- en preventiemogelijkheden van cybersecurity. Hiermee zal het hiaat in de literatuur omtrent de mogelijkheden van cybersecurity en de implementatie hiervan in stedelijk beleid worden aangevuld. Cyberdreigingen met de veiligheidsmaatregelen die daarbij komen kijken zijn een groeiend fenomeen en staat nog in zijn kinderschoenen. Zowel publieke als private partijen zijn nog steeds bezig met onderzoek naar de mogelijkheden en gevaren die het cyberlandschap met zich mee brengt. Op deze manier kan er een helder beeld worden geschetst over de mogelijkheden die de adaptatie van smart cities aan cyberdreigingen te bieden heeft.

Dit onderzoek richt zich voornamelijk op de theorie en een case waarin (het beleid over) de cybersecurity van Den Haag zal worden uitgelicht. Er wordt gekeken naar het huidige beleid over cybersecurity dat gevoerd wordt door overheden en er wordt gebruik gemaakt van verschillende theorieën, waaronder '*Network Societies*' van Manuel Castells en de 'Netwerkmaatschappij' van Jan van Dijk. Naast het gebruik van theorieën, wordt er ook objectieve en subjectieve kennis verhaalt uit verschillende experts. Deze experts voorzien het onderzoek van concrete kennis en hun eigen meningen. De doelstelling van dit onderzoek is bereikt in de periode van mei tot en met augustus 2018.

1.3. Onderzoeksmodel

Het onderzoek betreffende deze scriptie verloopt via de fases weergegeven in figuur 2. Dit onderzoeksmodel komt grotendeels overeen met het al eerder ontworpen onderzoeksmodel van Verschuren en Doorewaard (2015).



Figuur 2. Onderzoeksmodel betreffende deze scriptie.

In het begin wordt er gebruik gemaakt van literatuur en theoriegericht onderzoek om zo het nodige vooronderzoek te doen. Uit dit vooronderzoek is een conceptueel model voortgekomen. Op basis van dit conceptuele model zijn er interviews afgenomen en is de case Den Haag bestudeerd. De interviews met experts hebben tevens een bijdrage aan het onderzoek naar de case Den Haag geleverd. De interviews waren hier dan ook deels op toegespitst. Samen met de afgenomen interviews en de case, worden de resultaten geanalyseerd. Met de resultaten wordt er een conclusie opgezet waarmee de hoofdvraag en de deelvragen beantwoord zijn. Met behulp van deze conclusie is er een aanbeveling gedaan voor verder onderzoek.

1.4. Vraagstelling

Om een conclusie te kunnen trekken uit dit onderzoek moet er eerst een hoofdvraag worden opgesteld. Naast de hoofdvraag zullen er ook een aantal deelvragen worden opgesteld om dieper in te gaan op de stof en deze nader te kunnen toelichten. Het beantwoorden van deze vragen heeft als doel om te achterhalen hoe steden zich kunnen aanpassen aan de opkomende onzichtbare dreiging. De hoofdvraag van het onderzoek luidt:

Welke ex ante en ex post mogelijkheden zijn er voor een smart city om zich aan te passen aan cyberdreigingen en daarmee hun cybersecurity te waarborgen?

De volgende deelvragen kunnen gesteld worden bij de hoofdvraag:

- *Hoe vormen cyberaanvallen een dreiging voor smart cities?*

Met deze deelvraag wordt er gekeken naar hoe cyberaanvallen een dreiging vormen voor smart cities. Hiermee wordt blootgelegd welke kritieke (sub)systemen binnen een stad kwetsbaar zijn voor cyberaanvallen en wat voor een effect zij hebben op de leefbaarheid van de stad.

- *Wat zijn de zwakke punten in het smart netwerk die bij kunnen dragen aan de kwetsbaarheid van smart cities?*

Met deze deelvraag is er gekeken naar de zwakke punten van smart cities. Dit is van belang omdat deze ontwikkelingen kunnen bijdragen aan de kwetsbaarheid van de (sub)systemen van de stad. Door het opsporen van deze kwetsbaarheden zou een stad zich beter kunnen verdedigen.

- *Welke maatregelen zijn er te treffen voor smart cities om weerbaarder te zijn?*
    - *Welke vormen van cybersecurity zijn er en hoe verminderen zij de kwetsbaarheid van (sub)systemen?*

Met deze deelvraag en de bijbehorende sub-deelvraag wordt er gekeken welke maatregelen smart cities kunnen treffen om cyberaanvallen tegen te gaan. Hierbij wordt er gekeken naar de mogelijkheden ex ante en de mogelijkheden ex post. Binnen deze mogelijkheden wordt er gekeken welke vorm van cybersecurity smart cities kunnen toepassen om de veiligheid van kritieke (sub)systemen te kunnen waarborgen.

- *Hoe kunnen de verschillende manieren van cybersecurity geïmplementeerd worden in huidig (stedelijk) beleid?*

Met deze deelvraag wordt er gekeken naar hoe de mogelijke maatregelen, die genomen worden om de cybersecurity te kunnen waarborgen, opgenomen kunnen worden in het huidig (stedelijk) beleid. Door het opnemen van deze maatregelen in het beleid kunnen steden makkelijker worden aangepast aan de komende dreigingen.

- *Wat is de gepercipieerde urgentie van cybersecurity verbetering ten behoeve van een smart city en wat zijn de kosten die hierbij komen kijken?*

Met deze deelvraag wordt er gekeken naar hoe dringend de verbetering van cybersecurity in een smart city is ten opzichte van andere investeringen die een stad maakt. Er wordt gekeken hoe groot het aandeel is binnen de begroting dat naar cybersecurity gaat en wat voor een invloed dit heeft op mogelijkheid smart cities beter te beveiligen.

Het vraagstuk dat in dit onderzoek wordt behandeld is complex van aard. In het onderzoek moet niet alleen rekening gehouden worden met de interne beslissingen van het stedelijk bestuur, maar ook met beleid van de nationale overheid. Daarnaast krijgt dit vraagstuk ook te maken met externen actoren die hun invloed uitoefenen op het stedelijk bestuur en controle hebben over de kritieke subsystemen en cybersecurity van een smart city. Naast de kwestie van governance, wordt er ook gekeken naar zowel ex ante als ex post maatregelen tegen de verschillende cyberdreigingen die zich voordoen verspreid over de verschillende kritieke subsystemen. Ook dit draagt bij aan de complexiteit van het vraagstuk.

Met behulp van deze vragen en de bijbehorende resultaten kan er voor de overheden op zowel nationaal als lokaal niveau een advies worden gegeven over welke manieren van fysieke en digitale beveiliging het beste helpen bij de aanpassing aan cyberaanvallen en de implementatie van deze mogelijkheden in stedelijk beleid.

2. Conceptualisering van cybersecurity in een smart city context

In hun paper over de sterke onderlinge verbintenis binnen smart cities, openen Kanter en Litow (2009) met het volgende statement:

> "Someday soon, leaders will combine technological capabilities and social innovation to help produce a smarter world. That world will be seen on the ground in smarter cities composed of smarter communities that support the well-being of all citizens."

Om deze zogenaamde *smarter world* beter te kunnen begrijpen komen er in dit hoofdstuk verschillende theorieën en begrippen aan bod die van belang zijn voor het beantwoorden van de hoofd- en deelvragen. De eerste paragraaf gaat voornamelijk over een aantal belangrijke theorieën en begrippen die betrekkingen hebben tot smart cities, cyberdreigingen en –security en beleidsimplementatie. In de tweede paragraaf zullen de theorie en begrippen in verband worden gebracht door middel van een conceptueel model. Hiermee wordt aangetoond welke verbanden er tussen de theorie en begrippen verwacht wordt.

2.1. Theoretisch kader

Om een uitgebreidere kennis te krijgen over de theorieën en begrippen die van belang zijn voor dit onderzoek, worden zij in deze paragraaf aan het licht worden gebracht. Als eerste zal het begrip smart city worden belicht. Smart cities spelen een grote rol in dit onderzoek, aangezien er wordt gekeken naar wat voor een impact cyberaanvallen hebben op de kritieke (sub)systemen binnen smart cities. Onder het begrip smart city zal ook de theorie van netwerkmaatschappijen worden uitgewerkt. Hierna zal het begrip cyberdreiging volgen, aangezien het betrekking heeft op de kwetsbaarheid van de smart city. Daarna zal het begrip cybersecurity behandeld worden. De mogelijkheden op het gebied van cybersecurity zijn van groot belang voor de adaptatie van smart cities aan mogelijke toekomstige dreigingen. Als laatste zal de beleidsimplementatie voor cybersecurity in smart cities worden uitgewerkt.

2.1.1. Smart city

Wat is het dat een stad een smart city maakt? Sinds het concept smart city aangenomen is tijdens het tekenen van het Kyoto Protocol, heeft het meerdere betekenissen gekregen. Tijdens de jaren '90 begon het concept van *smart growth* zich te verspreiden. Men probeerde een oplossing te vinden voor de problemen die zich ontwikkelde vanuit twee belangrijke fenomenen: urbanisatie en de ontwikkeling van informatie- en communicatietechnologieën. De problemen waren onder andere verkeersopstoppingen, overvolle scholen, luchtvervuiling, het verlies van openbare ruimtes en de stijgende prijzen van publieke faciliteiten (Pardo & Taewoo, 2011). In 2005 begonnen een aantal technologiebedrijven de term smart city te gebruiken voor steden waar het toepassen van complexe informatiesystemen op stedelijke infrastructuur en diensten, zoals gebouwen, openbaar vervoer, elektriciteit- en waterdistributie en de openbare veiligheid centraal stond. Vandaag de dag staat het voor bijna elke vorm van innovatie binnen stedelijke planning en ontwikkeling die te maken heeft met technologische ontwikkelingen (Harrison & Abbott, 2011). Het technologiebedrijf IBM (2010) definieert een smart city als een stad waarin gebruik wordt gemaakt van informatie- en communicatietechnologieën om de belangrijkste informatie van de (sub)systemen te detecteren, te analyseren en te integreren. Naast het investeren in deze technologieën moet er in een smart city ook geïnvesteerd worden in zowel menselijk als sociaal kapitaal om een duurzame economische groei en

een hoge levenskwaliteit, die hand in hand gaat met het verstandig beheer van natuurlijke hulpbronnen, te bevorderen (Caragliu et al, 2011). De verschillende betekenissen van een smart city worden vaak aan elkaar gekoppeld door aan de ene kant innovatie in de informatie- en communicatietechnologie en aan de andere kant de veranderingen op economisch, politiek en socioculturee gebied. Al deze betekenissen zijn moeilijk van elkaar te onderscheiden aangezien ze vaak het een en ander van elkaar lenen in uitleg.

Het gebruik van een aangepaste infrastructuur om zo de economie en politieke situatie te verbeteren is een van de kernwaarden van een smart city. Echter, moeten deze veranderingen ergens vandaan komen. De ICT is de sector die al deze veranderingen onderling aan elkaar verbindt en dus eigenlijk de kern is van het smart city idee. Mobiele telefoons, satellieten, computernetwerken en het internet zijn de drijvende economische krachten binnen steden en zorgen voor talloze sociale en ruimtelijke effecten (Hollands, 2008). Voorbeelden van enkele van deze sociale en ruimtelijke effecten op steden zijn Singapore en Silicon Valley. In deze steden gaan stadsvernieuwing en ICT hand in hand.

Naast een aangepaste infrastructuur worden smart cities ook gekarakteriseerd door hun nadruk op een stedelijke ontwikkeling die gestuurd wordt door het bedrijfsleven. Brenner en Theodore (2002) stellen dat er een wereldwijde erkenning is van de overheersing van neoliberale stedelijke ruimtes. Deze neoliberale stedelijke ruimtes kunnen worden verklaar door het neoliberaal stedelijk beleid wat sommige steden voeren. Dit wordt onder andere veroorzaakt door de concurrentie tussen steden en publiek ondernemerschap (Sager, 2011). Steden zijn door de tijd heen ook een doelwit geworden voor een toenemende schaal aan neoliberale experimenten, institutionele innovaties en politiek-ideologische projecten vanuit de overheid (Brenner & Theodore, 2002a). Echter, worden deze ideeën betwist door een verscheidenheid aan sociale bewegingen die de reconstructie van neoliberale strategieën aan de kaak stellen. Ondanks deze bewegingen hebben steden tegenwoordig nog steeds te maken met een meer competitieve (globale) omgeving (Mayer, 2007). Het stedelijk bestuur staat tegenwoordig in het teken van ondernemerschap, met een nadruk op economische efficiëntie en individuele verantwoordelijkheden. Het mobiliseren van stedelijke ruimte als een arena voor marktgerichte economische groei is het belangrijkste doel geworden van stedelijk beleid (Mayer, 2007).

Natuurlijk zitten er ook nadelen aan het ontwikkelingen van een smart city. Door de snelle veranderingen in het gebruik van ICT binnen een stad, kan er een verschil ontstaan tussen geschoolde inwoners die zich snel kunnen aanpassen en de ongeschoolde inwoners die geen kansen hebben in het ICT-gebied. Hierdoor kan er sociale en culturele segregatie optreden binnen de stad (Hollands, 2008). Deze stedelijke gentrificatie zal zich niet alleen toepassen op huizen en wijken, maar ook op de levensstijl van de inwoners van de stad. Daarnaast wordt een stad ook veel kwetsbaarder voor cyberdreigingen naarmate het meer ICT integreert in zijn infrastructuur, waardoor kritieke (sub)systemen makkelijker kunnen worden platgelegd en zo het onderhoudsvermogen aantast waar een groot deel van de stad afhankelijk van is (Elmaghraby & Losavio, 2014).

2.1.2. Network societies

Een netwerkmaatschappij is een vorm van samenleving waarin een netwerk gedreven door ICT centraal staat. Dit netwerk bestaat uit verschillende knooppunten, die ieder hun eigen functie uitvoeren. De knooppunten zijn van verschillende waarden voor het netwerk, welke kan stijgen door

het verwerken van meer relevante informatie op een efficiëntere manier (Castells, 2004). De relevantie van een knooppunt wordt bepaald door zijn bijdrage aan het netwerk. De specifieke functie die het knooppunt uitvoert, heeft hier geen betrekking op. Ondanks dat zijn alle knooppunten van belang voor het netwerk. Wanneer een knooppunt overbodig raakt, wordt deze verwijderd of vervangen door een nieuw knooppunt (Castells, 2004).

Netwerken gebruiken hun knooppunten om informatiestromen te verwerken. Om de uitkomst van een informatiestroom, en daarmee het gehele netwerk, te veranderen moet er een nieuwe set knooppunten worden toegevoegd (Castells, 2004). Netwerken halen hun kracht uit flexibiliteit en aanpassingsvermogen, maar kunnen naarmate er meer knooppunten worden toegevoegd aan het netwerk hun efficiëntie niet meer waarborgen. De gave om nieuwe actoren te introduceren in het sociale proces werd steeds groter door middel van technologische doorbraken, met name de komst van ICT (Castells, 2004). De innovatie binnen de technologie en de implementatie van technologie is een fundamentele dimensie voor menselijke activiteit en organisatie. Het kan zich samen met andere dimensies binnen de maatschappij zeer makkelijk aanpassen (Fischer, 1992).

De manier waarop Castells (2004) de netwerkmaatschappij definieert, is ook terug te vinden in het concept van smart cities. Het netwerk van (sub)systemen binnen een smart city werkt nauw samen met elkaar en heeft alle knooppunten nodig om te kunnen functioneren naar behoren. De toegepaste ICT in een smart city is fundamenteel voor de organisatie van de stad en de activiteiten die daarin plaatsvinden. De stromen van informatie, maar ook van (menselijk) kapitaal worden verzorgd door de ICT en het daarbij behorende netwerk (Castells, 2004).

Van Dijk kijkt op een andere manier aan tegen de netwerkmaatschappij. Volgens hem is het een informatiesamenleving waarin de belangrijkste organisatiewijzen vormgegeven worden door een zenuwstelsel. Groepen en individuen zijn essentieel voor de samenleving, hoewel de nadruk steeds meer terug te vinden is bij de netwerken die hen onderling verbinden (van Dijk, 2001a). Door de aanwezigheid van groepen en individuen zal de publieke sfeer complexer worden. Om tot bepaalde resultaten te komen zullen deze groepen en individuen voortdurend verbinding zoeken met anderen. Hierdoor ontstaan netwerken die deels met elkaar overlappen, maar ook netwerken die elkaar uitsluiten of voortdurend veranderen (Aarts, 2013). Hoewel er veel individualisering plaatsvindt in de moderne samenleving, wordt de nadruk toch op de sociale netwerken gelegd, die ontstaan door de verwevenheid van samenleving en technologie (Van Dijk, 2001). Echter, stelt hij dat er binnen een netwerkmaatschappij ook een hoge graad van sociale ongelijkheid aanwezig is, zoals bij smart cities. De beheersing van informatievaardigheden (zoeken, analyseren en verwerken van informatie) en strategische vaardigheden (toepassen van deze informatie om de eigen positie te verbeteren) lijken een cruciale rol te spelen in de netwerksamenleving (Van Dijk, 2001). Hoe groter het aantal netwerken dat je bezit, hoe groter de voorsprong die je hebt in de netwerkmaatschappij.

Door het vergelijken van de netwerkmaatschappij met smart cities worden er veel overeenkomende kenmerken zichtbaar. Beide draaien om een netwerk aan systemen die onderling verbonden zijn, maar waarin een verkeerde schakel alles plat kan leggen. De mensen binnen deze maatschappij en de inwoners van smart cities moeten beide beschikken over een sterk aanpassingsvermogen om mee te kunnen draaien in de nieuwe samenleving die voortbouwt op technologische ontwikkelingen binnen de ICT.

2.1.3. Cyberdreiging

In onze onderling steeds meer verbonden steden kunnen bedreigingen afkomstig zijn vanuit onverwachte bronnen en richtingen. Niemand ziet de onzichtbare dreiging toeslaan tot dat het te laat is. Deze cyberaanvallen kunnen een grote negatieve impact hebben op het functioneren van smart cities. De beveiliging van het netwerk die daarbij komt kijken vormt complexe problemen voor onder andere smart cities, omdat zijn nog niet volledig voorbereid zijn op cyberaanvallen (Lewis, 2002). De onderling verbonden (sub)systemen in een smart city zullen voor cybercriminelen en –terroristen aantrekkelijk zijn om data en geld te stelen van inwoners en lokale ondernemingen, of om de stedelijke infrastructuur plat te leggen (Lin et al., 2017).

In het jaarverslag van de Militaire Inlichtingen- en Veiligheidsdienst (2017), valt te lezen dat het afgelopen jaar meer aanvallen dan ooit zijn uitgevoerd op doelwitten in Nederland. Deze doelwitten betroffen zowel het Ministerie van Defensie, de Defensie-industrie, overheidsinstellingen, niet-gouvernementele organisaties, kritieke sectoren en individuen. Het uitgangspunt van cyberaanvallen en –terrorisme is dan ook om zich te richten op landen en kritieke infrastructuur die meer en meer afhankelijk worden van ICT. Hiermee wordt alwaar een elektronische Achillespees gecreëerd (Lewis, 2002). Door middel van deze zwakke plek in het netwerk, kunnen cybercriminelen en –terroristen makkelijk binnendringen en het netwerk verstoren of zelfs kritieke sectoren compleet uitschakelen. Elke vorm van inbraak en sabotage zal een grote impact hebben op smart cities. Vandaag de dag zijn steden namelijk verantwoordelijke voor ongeveer 70% van de wereldwijde energiegebruik en verzorgen ze ook 70% van het bruto binnenlands product (Lin et al., 2017). In tabel 1 valt te zien welke kritieke sectoren welke effecten hebben bij een mogelijke cyberaanval.

Tabel 1. Mogelijke cyberaanvallen op kritieke sectoren en kosten die hierbij komen kijken. Bronnen: Lin et al. (2017), Reuters (2015), Via Satellite (2017), CSO (2017) en Daly (2018)

Critical Sector	Mogelijke Aanvallen				
	Veiligheid	**Financiën**	**Activiteiten**	**Privacy**	**Kosten**
Energie	**Veroorzaakt instabiliteit in de toevoer van stroom van de stad en heeft invloed op kritieke functies**	Lanceren van ransomware-aanvallen op energiebedrijven of het stelen van energie	Verstoren van de communicatie binnen energie-bedrijven	**Opsporen van *smart meter* gegevens en stelen van persoonlijke informatie**	€858 miljard (gebaseerd op het Amerikaanse energienet)
Transport	Veroorzaken van ongevallen met voertuigen	Exploiteren van kwetsbaarheden om gratis te reizen of voertuigen gegijzeld houden	**Onderbreken en manipuleren van transport- en veiligheids-diensten**	Compromitteren van gebruikersdata	€6,9 miljard (gebaseerd op de Amerikaanse transport sector)
Omgeving	Hacken van *smart valves* om (afval)water overlast te veroorzaken	Systemen en apparaten gegijzeld houden	Manipuleren van commando's en schaden van systeem reacties	Gebruik maken van sensoren om activiteiten te volgens	Afhankelijk van het risico gebonden aan de ramp
Connectiviteit		Systemen en apparaten gegijzeld houden	Verstoren van netwerk-communicatie waardoor downtime voor aangesloten systemen wordt veroorzaakt	Onderscheppen van communicatie om informatie en bewijs op te sporen	€1.12 miljoen (gebaseerd op bedrijven in Amerika)
Governance		**Systemen en apparaten gegijzeld houden**	Systemen en apparaten gegijzeld houden en aangesloten apparaten in bots veranderen	Informatie verzamelen over doelwitten via bewakings-beelden en open data	€7 miljoen (gebaseerd op publieke sector van Amerika)

De aanvallen op kritieke sectoren gaan niet zonder (fysieke) slachtoffers en kunnen ernstige vormen aannemen. De hierboven genoemde gevolgen kunnen de infrastructuur van een stad platleggen, waarmee de weg kan vrij worden gemaakt voor een eventuele fysieke aanval. Deze aanvallen hebben volgens Choo (2011) dan ook zowel korte termijn-gevolgen als lange termijn-gevolgen:

- Korte termijn gevolgen uiten zich in dat inwoners van een stad belemmerd worden in hun dagelijks activiteiten. Ze kunnen, bijvoorbeeld, geen informatie meer ontvangen over hun financiële transacties en kunnen deze ook niet meer uitvoeren. Daarnaast worden de dagelijkse activiteiten van overheden en bedrijven ook belemmerd. Bedrijven kunnen een significant deel van hun omzet mislopen en daarnaast ook nog aangeklaagd worden.

- Lange termijn gevolgen uiten zich in dat de nationale veiligheid niet meer gewaarborgd kan worden. Dit was het geval in 2010, waar vertrouwelijke overheidsinformatie werd vrijgegeven via *WikiLeaks*. Ook kan het zorgen voor sociale ontevredenheid en onrust wanneer het publiek het vertrouwen in de overheid om adequaat te kunnen functioneren verliest. Daarnaast neemt ook de kwetsbaarheid van intellectueel eigendom toe. Bedrijven en overheden kunnen hierdoor hun concurrentievermogen verliezen door middel van industriële en militaire spionage gerelateerde incidenten.

2.1.4. Cybersecurity

Eveneens als bij smart cities, zijn er ook veel definities voor cybersecurity. Dit komt doordat er verschillende actoren zijn die ieder vanuit hun eigen invalshoek de term en de daarbij behorende problematiek benaderen. In de Nationale Cybersecurity Strategie 2, een rapport van het Ministerie van Justitie en Veiligheid over de beveiliging van het Nederlandse cyberdomein, wordt de term cybersecurity als volgt definieert:

> ”Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De schade aan ICT kan bestaan uit aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van ICT opgeslagen informatie.”

Deze definitie zal doorgaande gehanteerd worden om cybersecurity te voorzien van een specifieke betekenis. Het is noodzakelijk om inzicht te hebben in potentiële kwetsbaarheden en dreigingen. Daarom ligt bij cybersecurity de nadruk op het beveiligen en weerbaarder maken van systemen en netwerken (Van der Meulen & Lodder, 2014). Na het verzamelen van informatie kan er een risicoanalyse worden gemaakt. Deze risicoanalyse wordt gebruikt bij het creëren van nieuwe maatregelen. Cybercriminelen onderscheiden zich van terroristen op het gebied van diversiteit. Hoewel beide groeperingen gebruik maken van hetzelfde materiaal en dezelfde tactieken is voor beide hun drijfveer uniek (Van der Meulen & Lodder, 2014).

Om de risico’s van een cyberdreiging tegen te gaan, moeten actoren uit verschillende sectoren de handen in een slaan (Choo, 2011). Door elk een andere rol aan te nemen binnen cybersecurity kan het risico op een cyberaanval worden gemitigeerd. De onontdekte kans om cyberdreigingen te mitigeren ligt in een effectieve samenwerking tussen publieke en private sectoren. Het delen van informatie op een veilige en betrouwbare manier is een cruciaal onderdeel voor het tijdig in kunnen grijpen bij een cyberaanval (Choo, 2011). De kwetsbaarheden in de ICT kunnen worden opgelost door preventief beveiligingsmaatregelen (ex ante) te implementeren, bestaande uit zowel technische als niet-technische maatregelen, en beveiligingsmaatregelen achteraf (ex post) die zich bezighouden met het oplossen van cyberaanvallen en de schade die hierbij is veroorzaakt (Rowe et al., 2011). Daarnaast moeten niet alleen de actoren uit een bepaalde stad of regio met elkaar samenwerken, maar moet dit ook gebeuren op internationaal niveau zonder dat één groep, land of instelling het eigendomsrecht claimt (Rowe et al., 2011). Binnen Nederland werkt de MIVD al samen met de Algemene Inlichtingen- en Veiligheidsdienst en andere instanties om de Nederlandse overheid en inwoners minder kwetsbaar te maken voor cyberincidenten of –dreigingen (MIVD, 2017). Ook voor een relatief kleine dienst als de MIVD is (internationale) samenwerking van groot belang. Zo wordt er op internationaal niveau op een optimale en verantwoorde manier informatie uitgewisseld met partners van de MIVD.

2.1.5. Smart city- en cybersecuritybeleid

Cybersecurity is een drukkende zaak geworden in de afgelopen paar jaar. Slachtoffers van vermeende cyberaanvallen van buitenaf schreeuwen om een beleid van overheden om dit te voorkomen. Er is vraag naar een uitgebreid (inter)nationaal cybersecuritybeleid. Cybersecuritybeleid kan de spanning aanpakken tussen de vraag naar cyberfunctionaliteit en de vereisten voor cybersecurity (Bayuk et al, 2012). Het blijkt echter een ontmoedigende taak om een coherent cybersecuritybeleid te ontwikkelen. Het huidige beleidskader is niet toereikeind genoeg om de problemen systematisch op te lossen en de parameters te specificeren om deze ontwikkelingen te beperken en wellicht tegen te gaan (Harknett & Stever, 2011). Het huidige beleid dat de meeste landen hanteren is niet uitgebreid genoeg in zijn focus, terwijl de implementatie van dit beleid door blijft gaan. De OESO geeft in haar rapport aan dat het noodzakelijk is om de coördinatie binnen overheden op zowel beleids- als operationeel niveau te bevorderen (OESO, 2012). De verantwoordelijkheid van het opstellen en implementeren van zo een soort beleid ligt bij de overheid. In de periode van 2009 tot 2011, hebben een aantal overheden een eigen cybersecuritystrategie geschreven. Het snelle tempo waarop deze strategieën zijn herzien en vernieuwt wijst op de bereidheid van overheden om bedacht te zijn op de opkomende dreigingen en het snel aanpasbare karakter van een mogelijke cyberdreiging (OESO, 2012).

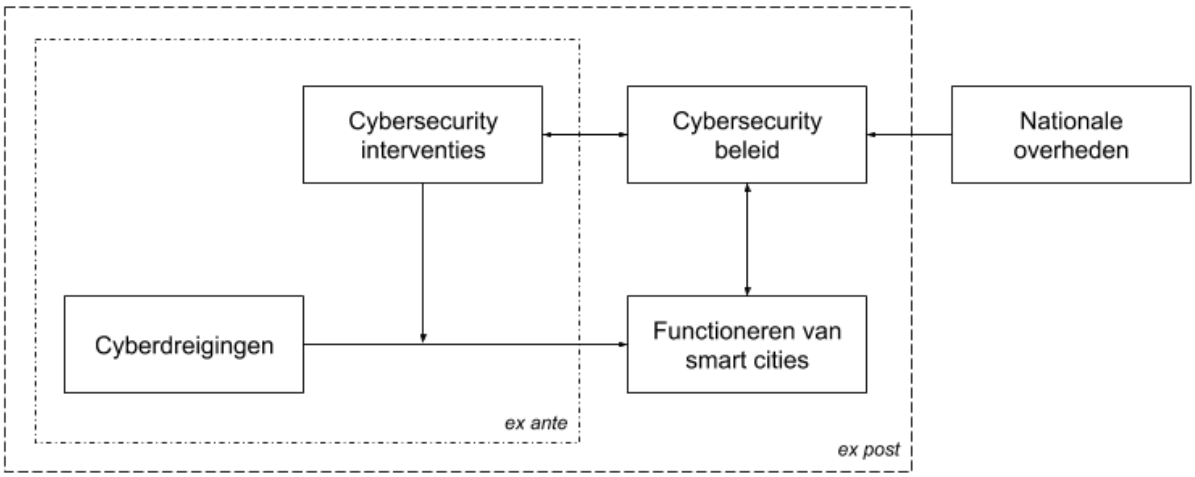
Het is van noodzaak dat steden, met name smart cities, ook hun eigen beleid opstellen om zo hun eigen veiligheid op de best mogelijke manier kunnen waarborgen. In dit beleid moet onder andere worden opgenomen hoe de stad cyberaanvallen preventief uitsluit, hoe de stad in geval van een cyberaanval de continuïteit van diensten kan waarborgen en hoe de stad omgaat met alle data die zij verzamelt (Lin et al, 2017).

2.1.6. Verwachtingen

Er wordt verwacht dat smart cities de keuze hebben uit meerdere oplossingen voor het probleem dat cyberdreigingen met zich meebrengen. Deze oplossingen zijn zowel preventief, actief als passief van aard. Naast het versterken van de cybersecurity kan ook het ‘smarter’ maken van kritieke subsystemen, zodat zij uit zichzelf al beveiligd zijn tegen cyberaanvallen, ertoe leiden dat aanvallen al worden afgeweerd voordat zij plaatsvinden. Hier zou de focus van de steden dan ook moeten liggen. Ook kan er actief gestreden worden tegen cyberaanvallen door op het moment van plegen de aanval terug te kunnen leiden naar de cybercriminelen of –terroristen. Daarnaast wordt er verwacht dat zowel nationale als stedelijke overheden zich bezighouden met het opstellen dan wel aanscherpen van beleid omtrent cybersecurity. Voor de implementatie van deze vorm van beleid moet er een nieuw beleidskader worden opgebouwd, die voldoende ondersteuning biedt om deze problemen systematisch op te kunnen lossen. Door het aangaan van samenwerkingen met private partijen is het mogelijk dat smart cities zo hun regie uit handen geven. Doordat deze private partijen een expertise bezitten die overheden niet zouden bezitten, hebben deze private partijen een machtspositie over de publieke sector en zouden zijn hun invloed kunnen gebruiken om bepaalde regelgeving door te kunnen drukken binnen het cybersecuritybeleid van smart cities. Dit zou nadelig kunnen uitpakken voor overheden. Kosten zouden kunnen oplopen en ze zouden de regie kunnen verliezen over hun eigen netwerk.

2.2. Conceptueel model

Cyberdreigingen hebben in dit onderzoek een invloed op smart cities, omdat cyberaanvallen de kritieke (sub)systemen van een smart city kunnen ontregelen en/of beschadigen. Het functioneren van smart cities wordt in dit conceptueel model gezien als een entiteit en niet als *governance approach*. De nationale overheden stellen een beleid op en creëren een beleidskader die zowel stedelijke als nationale overheden kan voorzien van een ongecompliceerde implementatie van cybersecuritybeleid. De nationale overheden hebben dus indirect een verantwoordelijkheid voor de gevolgen van cyberaanvallen. Cybersecurity en de implementatie van cybersecurity beïnvloeden elkaar. Door een goede implementatie van cybersecuritybeleid, kan de cybersecurity versterkt worden. Wanneer de cybersecurity niet adequaat genoeg is om bepaalde cyberaanvallen te weren, kan de implementatie van beleid hierop worden aangepast. Smart cities en de implementatie van cybersecuritybeleid hebben ook invloed op elkaar. De innovatie in ICT en daarmee de aanpassingen in smart cities, vragen voor een constante verandering van het beleid om nieuwe kwetsbaarheden uit te kunnen sluiten. Daarnaast zorgt de implementatie van cybersecuritybeleid ervoor dat smart cities zich makkelijker kunnen ontwikkelen en minder kwetsbaar zijn voor cyberaanvallen. Dan blijft nog de vraag welke mogelijkheden van cybersecurity kunnen worden toepast om cyberdreigingen te voorkomen of tegen te gaan. Cybersecurity heeft namelijk een direct effect op de relatie tussen cyberdreigingen en smart cities. De mate van cybersecurity bepaalt in welke mate de cyberdreigingen invloed hebben op smart cities.



Figuur 3. Conceptueel model betreffende deze scriptie.

3. Methoden van onderzoek naar cybersecurity adaptatie smart cities

3.1. Onderzoeksstrategie

Dit onderzoek richt zich op het fenomeen van cyberdreigingen voor smart cities en de cybersecurity die daarbij komt kijken. Aangezien cyberdreigingen een probleem zijn van internationale omvang, is dit een in diepteonderzoek over een onderwerp dat betrekking heeft tot de gehele internationale gemeenschap. Dit onderzoek zal voornamelijk kwalitatief van aard zijn. Het kwalitatieve karakter van dit onderzoek wordt gekenmerkt door het afnemen van interviews met verschillende experts op het gebied van dit onderwerp. Deze experts zijn voornamelijk in dienst zijn van onderzoeksinstituten, gemeenten en adviesbureaus. Ook is er een relatief klein kwantitatief karakter aanwezig dat gekenmerkt wordt door het gebruik van cijfers over het aantal dreigingen, vormen van dreiging en de kosten die komen kijken bij de cybersecuritymaatregelen.

In dit onderzoek is er gekozen voor een case study. Bij een case study wordt er namelijk gekeken naar de kennis van meerdere personen en worden er verschillende bronnen gebruikt voor het onderzoek. Deze bronnen zijn interviews, theorieën en documenten van eerdere onderzoeken omtrent dit onderwerp. Er wordt gebruik gemaakt van een enkelvoudige case study. Voor de case is het van belang dat de stad zich kan definiëren als smart city of op weg is naar deze definitie. De stad moet een strategie klaar hebben liggen, waarin de ontwikkelingen tot een smart city uitvoerig worden besproken. Dit geldt onder andere voor de stad Den Haag. Den Haag profileert zich al sinds een paar jaar als smart city in wording en heeft steun gevraagd bij het kabinet voor hun smart city-strategie (Oosterveld, 2017). Daarnaast is het de politieke hoofdstad, wat betekent dat ze een mogelijk doelwit is voor cyberdreigingen. Bij de gemeente Den Haag is er een interview gehouden om te kijken hoe de gemeente zich aanpast aan cyberdreigingen en hoe zij omgaan met de implementatie van cybersecuritybeleid. De uitkomst van dit onderzoek leidt tot een aanbeveling voor zowel de gemeente Den Haag en andere gemeenten over de huidige situatie van hun cybersecurity(beleid).

De gemeente Den Haag wil inspelen op de kansen die innovaties en maatschappelijke veranderingen op het gebied van ICT te bieden hebben. Hiermee wilt de gemeente werken aan een dynamische economie waarbij er geïnvesteerd wordt in kennis en talent door onder andere bedrijven, instellingen, onderwijs en overheden. Dit alles met als doel om samen met partners in de stad en regio te komen tot een economische transitie van Den Haag en de Metropoolregio Rotterdam-Den Haag (Van Engelshoven, 2015).

Er is een interview gehouden met een afgevaardigde van het bedrijfsadviesbureau Ernst & Young, omdat deze adviseurs en onderzoekers in dienst heeft op het gebied van Cybersecurity. Ook is er een interview gehouden met de *Chief Information Officer* van gemeente Den Haag. Deze persoon is een expert op het gebied van ICT en staat aan het hoofd van de transformatie van Den Haag naar een smart city. Tenslotte is er een interview gehouden met de algemeen directeur van SIM-CI. SIM-CI houdt zich voornamelijk bezig met de gevolgen van eventuele cyberaanvallen op de kritieke infrastructuur.

3.2. Onderzoeksmateriaal

Dit onderzoek beschikt over de volgende onderzoeksobjecten: smart cities, cyberdreigingen, cybersecurity en implementatie van cybersecuritybeleid. De hoofdvraag van dit onderzoek is beantwoord aan de hand van vier deelvragen.

- *Hoe vormen cyberaanvallen een dreiging voor smart cities?*

De onderzoeksobjecten hier zijn cyberdreigingen en smart cities. Aan de hand van interviews en bestaande literatuur is er gekeken naar de dreigingen die cyberaanvallen met zich meebrengen voor smart cities. Het inzicht in deze informatie is belangrijk om erachter te komen wat een cyberaanval nou precies inhoudt en wat het doel is van een cyberaanval. Ook kan er inzicht ontstaan in welke kritieke (sub)systemen een doelwit zijn voor deze cyberaanvallen. De interviews zijn uitgewerkt in ATLAS.ti, waarna er met een codeboek is gekeken naar de belangrijkste en meest relevante aspecten die uit het interview gekomen zijn.

- *Wat zijn de zwakke punten in het smart netwerk die bij kunnen dragen aan de kwetsbaarheid van smart cities?*

Het onderzoeksobject is hier cybersecurity. Aan de hand van interviews en bestaande literatuur is er gekeken naar mogelijke kwetsbaarheden in het *smart grid* en de cybersecurity die daarbij komt kijken. De interviews zijn uitgewerkt in ATLAS.ti, waarna er met een codeboek is gekeken naar de belangrijkste en meest relevante aspecten die uit het interview gekomen zijn.

- *Welke maatregelen zijn er te treffen voor smart cities om weerbaarder te zijn?*

Het onderzoeksobject is de groep van de maatregelen die een smart city kan treffen om zichzelf te verweren tegen cyberaanvallen. Aan de hand van interviews en bestaande literatuur is er gekeken naar de mogelijkheden die een smart city heeft om cyberaanvallen tegen te gaan. Daarnaast wordt er in de subvraag ook gekeken naar hoe cybersecurity de veiligheid van kritieke (sub)systemen kan waarborgen en daarmee de kans op een verstoring of beschadiging van de infrastructuur voorkomen kan worden.

- *Hoe kunnen de verschillende manieren van cybersecurity geïmplementeerd worden in huidig (stedelijk) beleid?*

De onderzoeksobjecten zijn hier cybersecurity en de implementatie van cybersecuritybeleid. Aan de hand van interviews en bestaande literatuur is er gekeken naar hoe overheden hun beleidskader kunnen aanpassen om zo de implementatie van cybersecuritybeleid te kunnen bespoedigen. Ook is er gekeken naar welke manieren van cybersecurity het best bij welke vorm van beleid passen en of cybersecurity al opgenomen is in het huidig (stedelijk) beleid. De interviews zijn uitgewerkt in ATLAS.ti, waarna er met een codeboek is gekeken naar de belangrijkste en meest relevante aspecten die uit het interview gekomen zijn.

- *Wat is de gepercipieerde urgentie van cybersecurity verbetering ten behoeve van een smart city en wat zijn de kosten die hierbij komen kijken?*

De onderzoeksobjecten zijn hier de verbetering van cybersecurity en de urgentie en kosten die hierbij komen kijken. Aan de hand van interviews en bestaande literatuur is er gekeken naar hoe hoog cybersecurity voor overheden op de agenda staat. Ook wordt er gekeken naar kosten die komen kijken bij het verbeteren van cybersecuritymaatregelen. De interviews zijn uitgewerkt in

ATLAS.ti, waarna er met een codeboek is gekeken naar de belangrijkste en meest relevante aspecten die uit het interview gekomen zijn.

De resultaten die uit de interviews komen zijn ook verklaard aan de hand van de netwerkmaatschappij theorieën van Castells en Van Dijk. Met behulp van een analyse van de onderzoeksresultaten is er een conclusie getrokken, waarmee een antwoord is gegeven op de hoofd- en deelvragen van dit onderzoek. Daarnaast is er nog een aanbeveling voor een eventueel vervolgonderzoek gedaan op basis van de resultaten en de conclusie.

3.3. Reflectie op de methodologie

Bij het uitvoeren van het onderzoek hebben zich verschillende complicaties voorgedaan. De literatuur was op sommige vlakken niet toereikend genoeg. Er was een marginale hoeveelheid literatuur te vinden over cyberaanvallen die specifiek gericht zijn op smart cities en over de implementatie van cybersecurity in smart cities. Verder sloten academische artikelen op andere gebieden goed aan bij het onderwerp, waarmee het literatuuronderzoek voldoende werd bespoedigd.

Daarnaast was het lastig om in de periode van schrijven voldoende interviews te regelen. Er is contact gelegd met meerdere mogelijkheden, maar uiteindelijk is het maar gelukt met drie hiervan een interview af te nemen. Er is contact geweest met verschillende experts, zowel binnen Nederland als op internationaal terrein. De meeste van hen gaven aan geen tijd te hebben om een interview af te nemen, omdat ze het te druk hadden of omdat zij op vakantie waren. Ook is er een antwoord teruggekomen van een expert met de boodschap dat er eerst meer verdieping moest worden gezocht in het onderwerp voor een beter begrip van bepaalde aspecten. Echter, was dat niet meer in te passen in de planning van deze scriptie.

Er is contact geweest met de onderzoeksinstellingen The Clingendael Institute en het Haags Centrum voor Strategische Studies. Ook hier had men geen tijd of was hun kennis omtrent het onderwerp niet toereikend genoeg. Hetzelfde is gebeurd bij de bedrijven Alliander en Platform31. Zij hadden graag hun steentje bijgedragen, maar gaven aan dat ze niet de kennis hadden om waardevolle informatie in te brengen. Andere instanties, zoals HeelHelder en het Nationaal Cyber Security Centrum, hadden simpelweg geen tijd. Ook is er daarnaast nog contact geweest met het TNO en The Hague Security Delta, maar deze hebben uiteindelijk niets meer van zich laten horen.

Als laatste, is er contact geweest met een andere medewerker van gemeente Den Haag. Deze gaf echter aan dat hij niet meer zou kunnen bijdragen dan de al eerder geïnterviewde Chief Information Officer van de gemeente Den Haag en verbrak daarna ook het contact.

Al met al zijn de interviews die zijn uitgevoerd geslaagd en hebben deze een goede bijdrage kunnen leveren aan het schrijven van deze scriptie.

4. Resultaten en analyse

4.1. Analyse van Den Haag als smart city

In 2014 sloot de gemeente Den Haag een coalitieakkoord 'Vertrouwen op Haagse Kracht '2014-2018'' met daarin de ambitie invulling te geven aan Smart City Den Haag. Door middel van innovatieve technologieën pakt de gemeente Den Haag maatschappelijke vraagstukken aan. Dit doen zij door projecten en pilots te realiseren in samenwerking met bedrijven, kennisinstellingen en hun burgers (Van Engelshoven, 2015). Hierdoor krijgt Den Haag een stevige impuls meegegeven op het gebied van levenskwaliteit en duurzaamheid en verbetert het de concurrentiepositie van de stad op zowel nationaal als internationaal niveau (Van Engelshoven, 2015). In het kader van de nationale smart city strategie zijn er vijf hoofdthema's benoemd: mobiliteit, circulaire economie, *sustainability, e-health* en *safety & security*. Volgens Marijn Fraanje (bijlage I), Chief Information Officer van de gemeente Den Haag, heeft de G5 van Nederlandse steden onderling de thema's verdeeld en is *safety & security* terecht gekomen bij de gemeente Den Haag. Dit heeft onder andere te maken met het karakter van de stad, legt Marijn Fraanje (bijlage I) uit. Den Haag is het regeringscentrum van Nederland. Derhalve zitten er veel internationale instituten en ambassades in de stad, wat het een potentieel en interessant doelwit maakt voor staten en cybercriminelen. Den Haag kiest dan ook niet voor niets aansluiting bij zijn eigen profiel 'Smart The Hague', waarin de Stad van Vrede en Recht, de positie als regeringscentrum en haar elf kilometer lange strand centraal staan (Van Beurden & Wamelink, 2017).

Door het grootstedelijke karakter van de stad, krijgt Den Haag dagelijks te maken met specifieke kansen en opgaven. De concurrentie waarmee de stad moet kampen is groot, doordat veel economische stromen hier samen komen (Gemeente Den Haag, 2014). Om een grote rol te kunnen spelen op het internationale toneel, is het belangrijk dat Den Haag samenwerkt met andere steden. De Metropoolregio Rotterdam-Den Haag is één van de richtinggevende stedelijke gebieden in de Roadmap Next Economy (Gemeente Den Haag, 2014). Vanuit de International Data Responsibility Group, een globaal netwerk van experts en organisaties op het gebied van data revolutie, komen er veel spin-offs die via het kader van de Roadmap Next Economy ondersteuning hebben gekregen en zo een bijdrage leveren aan de ontwikkelingen van de Smart Digital Delta in de Metropoolregio Rotterdam-Den Haag (Van Beurden & Wamelink, 2017). Om een voortrekkersrol op zowel nationaal als internationaal gebied te kunnen vervullen, zal de komende jaren de focus van Den Haag liggen op het uitbouwen van deze positionering (Van Beurden & Wamelink, 2017).

Op het gebied van het smart netwerk is Den Haag bezig met het ontwikkelen van een programma om nieuwe technologieën toe te passen op maatschappelijke terreinen als zorg, veiligheid en duurzaamheid (Gemeente Den Haag, 2014). Door middel van verschillende projecten rondom en in de stad zelf, probeert Den Haag het vestigen van startups en buitenlandse ICT-bedrijven te stimuleren. Eén van die projecten is het verkennen van de wenselijkheid en haalbaarheid van een telecom-campus en de samenwerking met onderwijsinstellingen (Gemeente Den Haag, 2014). Daarnaast is de gemeente Den Haag ook bezig met een op sensor gebaseerde parkeeroplossing voor blauwe parkeerzones. Winkeliers kunnen hun klanten tegemoetkomen door een parkeerplek aan te bieden en (deels) de kosten te vergoeden. Hiermee wordt er een directe connectie gelegd tussen blauwe parkeerzones en een economische activiteit (Van Engelshoven, 2015). Een ander projecten waarmee de gemeente zich bezighoudt is de vervanging van DigiD door de eID, het plannen van

gebiedsontwikkeling in 3D en het implementeren van *smart lightning*. Het laatste project is tevens onderdeel van Living Lab Scheveningen.

Living Lab Scheveningen is een project dat onderdeel is van de herstructurering van de boulevard van Scheveningen. Hiermee probeert de gemeente Den Haag de openbare ruimte te digitaliseren. Hiervoor worden onder meer *smart lightning*, afvalsensoren en parkeersensoren ingezet (Van Engelshoven, 2015). Deze combinatie van ICT met straatverlichting zorgt er voor dat lantaarnpalen worden uitgerust met andere functies als wifi, verkeerscamera's, laadpunten en sensoren om lucht- en geluidsvervuiling te meten (Gemeente Den Haag, 2017). De insteek van Living Lab Scheveningen is dat het dient als ontwikkelomgeving voor het creëren van een smart netwerk binnen de openbare ruimtes in Den Haag. Het is een testcase voor de financierbaarheid en schaalbaarheid van deze soort van infrastructuur (Van Beurden & Wamelink, 2017). Volgens Marijn Fraanje (bijlage I) wordt er door de gemeente Den Haag een afweging gemaakt om op meerdere plekken aan soortgelijke projecten te beginnen, maar moet er eerst worden gekeken of er intern genoeg kennis en expertise is om dit te bewerkstelligen. Scheveningen zal binnen een aantal jaren behoren tot een van de slimste stranden van de wereld en zal dienen als een blauwdruk voor de uitrol van deze vorm van digitale infrastructuur op essentieel schaalniveau over andere smart cities binnen Nederland (Van Beurden & Wamelink, 2017).

4.1.1. Bedreigingen voor Den Haag

Door het profiel van de stad Den Haag als regeringscentrum van Nederland en het huizen van meerdere internationale organisaties, maakt Den Haag zichzelf een doelwit voor cybercriminelen en staten. Marijn Fraanje (bijlage I) vertelt dat er dagelijks meerdere pogingen worden gedaan om de systemen van de gemeente binnen te dringen, maar dat de gemeente zelf nog geen grote incidenten heeft gehad. Echter, is geen enkele stad 100% veilig voor cyberaanvallen en dat geldt ook voor Den Haag. Volgens een rapport van het Nationaal Cyber Security Centrum (2014) is een stad als Den Haag kwetsbaar voor meerdere vormen van cyberdreigingen. Cybercriminelen kunnen het smart netwerk van Den Haag gebruiken voor de diefstal en publicatie of verkoop van gevoelige informatie en persoonsgegevens (NCSC, 2014). Daarnaast kunnen zij ook informatie manipuleren en het netwerk verstoren, waardoor inwoners van de stad geen gebruik meer kunnen maken van de digitale diensten die de gemeente aanbiedt (NCSC, 2014).

Een andere dreiging die zich voordoet bij de gemeente Den Haag is het monitoren van publieke ruimtes. Volgens Marijn Fraanje (bijlage I) heeft de gemeente nog geen slimme manier gevonden om te achterhalen waar bepaalde sensoren zich bevinden in de publieke ruimte. Zonder deze informatie kan de gemeente Den Haag niet volgen wat deze sensoren voor een informatie binnenhalen en doorspelen naar externe actoren (Cerrudo, 2015). Wanneer deze informatie terecht komt bij een kwaadwillige actor zou dit er eventueel voor kunnen zorgen dat cybercriminelen een toegangspoort hebben tot het netwerk van de stad en zo de digitale infrastructuur kunnen verstoren of zelfs kunnen overnemen (NCSC, 2014). Wessel Sluis van SIM-CI (bijlage II) is van mening dat Den Haag hierdoor te maken kan krijgen met een grootschalige cyberaanval waarbij veel schade kan worden aangericht aan de kritieke infrastructuur. Deze schade aan de kritieke infrastructuur kan zorgen voor een groot economisch en financieel verlies voor Den Haag en leidt ook tot een afname in onderhoudend vermogen van de inwoners van de stad (Elmaghraby & Losavio, 2014).

Echter, is Den Haag niet alleen kwetsbaar voor technologische dreigingen van buitenaf. De inwoners van de stad vormen een menselijke dreiging voor zichzelf. Wanneer mensen niet goed bewust zijn van de cyberdreigingen en cybersecurity, kunnen ook zij een toegangspoort vormen voor cybercriminelen en staten (Amoroso, 2012).

4.1.2. Cybersecuritymaatregelen genomen door de gemeente Den Haag

Binnen de gemeente Den Haag zijn er veel initiatieven die zich bezighouden met de cybersecurity van de stad. Om een zeker impact te kunnen realiseren is het belangrijk dat deze initiatieven kunnen worden opgeschaald wanneer zij een significante bijdrage leveren aan de digitale veiligheid (Van Engelshoven, 2015). Een flexibel innovatiekader waarborgt de interoperabiliteit en schaalbaarheid van deze initiatieven en zijn dus belangrijk voor het realiseren van de al eerdergenoemde impact (Van Engelshoven, 2015). Dit is de reden dat cybersecurity en het daaraan gerelateerde cyberbeleid van de gemeente Den Haag een belangrijke pilaar zijn van de 'Smart The Hague'-agenda (Van Beurden & Wamelink, 2017). De specialisatie van Den Haag op het gebied van *safety & security* heeft gezorgd voor de oprichting van het cybersecuritycluster *The Hague Security Delta* (Gemeente Den Haag, 2014). *The Hague Security Delta* levert een aanzienlijke bijdrage aan de cybersecurity van Den Haag en heeft het potentieel om zich te ontwikkelen tot de grootste cybersecurityhub van Europa en volgens Marijn Fraanje (bijlage I) ook een hotspot voor start-up's op het gebied van ICT en cybersecurity.

In het interview met Marijn Fraanje (bijlage I) is naar voren gekomen dat de gemeente Den Haag zich zowel ex ante als ex post ontwikkelt op het gebied van cybersecurity. Zo heeft de gemeente zijn eigen interne ICT-dienst die de zaken over het digitale netwerk van Den Haag in de gaten houden vanuit een daarvoor speciaal ingerichte controlekamer. Vanuit deze controlekamer worden onder andere de eigen websites van de gemeente gemonitord, maar ook veiligheid van websites gelieerd aan de gemeente, vertelt Marijn Fraanje (bijlage I). Ook wordt deze monitoring deels uitbesteed aan de private partijen waarmee de gemeente Den Haag samenwerkt. Daarnaast heeft de gemeente Den Haag tijdens de Cyber Security Week een ethische hacksessie gehouden op het binnenplein van het gemeentehuis. Hiervoor hebben zij een groep jongeren uitgenodigd die de opdracht krijgen om de cybersecurity van de gemeente Den Haag te omzeilen in een live omgeving. Dit is volgens Marijn Fraanje (bijlage I) een manier om te testen of de huidige cybersecurity van de gemeente voldoet aan de cyberdreigingen van vandaag de dag. Daarnaast wordt de ex ante cybersecurity, die onder andere bestaat uit een strenge monitoring, firewalls en procedurele maatregelen ook structureel getest door professionele private partijen.

Echter, levert de ethische hacksessie ook een ander gewenst effect op dat bij de gemeente Den Haag hoog op de agenda staat. Doordat deze activiteit plaatsvond in een publieke ruimte, trok het de aandacht van veel inwoners. Marijn Fraanje stelt in het interview (bijlage I) dat het creëren van *cyberawareness* cruciaal is voor de cybersecurity van een smart city als Den Haag. Zo organiseert de gemeente spreekuren omtrent privacy- en informatiebeveiliging. Ook heeft de gemeente een mobiele applicatie ontwikkelt om *cyberawareness* promoten. Deze applicatie zag behoorlijk veel animo en werd goed ontvangen door de inwoners van de stad zegt Marijn Fraanje (bijlage I).

Naast al deze preventieve maatregelen heeft de gemeente volgens Marijn Fraanje (bijlage I) ook een back-up plan mocht de beveiliging omzeilt worden. Deze plannen zijn echter niet voor specifieke

gevallen, maar hanteren een stadsbreed plan voor het oplossen en herstellen van de schade veroorzaakt door cyberaanvallen.

4.1.3. Implementatie cybersecurity in beleid van de gemeente Den Haag

Het beleid van de gemeente Den Haag hanteert verschillende punten omtrent cybersecurity en de bescherming van gevoelige informatie en persoonsgegevens van hun inwoners. De Nederlandse gemeenten hebben zich allemaal moeten committeren aan de Baseline Informatiebeveiliging Gemeenten, ook wel de BIG. Hieruit volgt dat elke gemeente een informatiebeveiligingsbeleid moet hebben dat zij in afstemming kunnen adopteren van de informatiebeveiligingsdienst voor gemeenten (Van Beurden & Wamelink, 2017). De gemeente gaat uiterst zorgvuldig om met vertrouwelijke persoonsgegevens om zo het individuele recht op privacy te kunnen waarborgen (Van Engelshoven, 2015). De persoonsgegevens worden verwerkt volgens verschillende privacywet- en regelgevingen, indien zij van direct belang zijn voor de inwoners en bezoekers van de stad (Van Engelshoven, 2015). Vanwege Den Haag haar imago als Stad van Vrede en Recht moet de gemeente zorgvuldig opgaan met data en wordt er een beroep gedaan op het vertrouwen van de burger. Dit is dan ook de reden dat privacy als een van de belangrijkste punten is opgenomen in het ontwikkelen van Den Haag als smart city (Gemeente Den Haag, 2014).

Naast de richtlijnen voor informatiebeveiliging is er volgens Marijn Fraanje (bijlage I) ook een beleidslijn voor de kritieke infrastructuur, omdat daar een aantal sectoren in zitten die aan bepaalde eisen moeten voldoen. In het beleid van de gemeente Den Haag is dan ook opgenomen om zich actief te laten testen op deze gebieden.

4.1.4. Urgentie en kosten van cybersecurity voor de gemeente Den Haag

Cybersecurity is een van de drukkende kwesties die hoog op de agenda staat bij de gemeente Den Haag. De urgentie van cybersecurity neemt toe door de snelle ontwikkelingen op het gebied van ICT en de implementatie van deze technologieën in Nederlandse steden (Caruson et al, 2012). In het interview met Marijn Fraanje (bijlage I) laat hij weten waarom cybersecurity zo hoog in het vaandel staat bij de gemeente Den Haag. Zo probeert de gemeente het huidige niveau van hun cybersecurity te waarborgen en waar mogelijk te verbeteren. Daarnaast zijn de economische ontwikkelingen in de cybersecuritysector van de stad ook van groot belang.

Naast economisch gewin brengt cybersecurity ook kosten mee voor de gemeente Den Haag. Volgens Wessel Sluis (bijlage II) kunnen deze kosten het meest beïnvloed worden hoe eerder je in de keten van planning naar uitvoering ingrijpt. Echter, maakt dit voor de gemeente Den Haag niet uit. De kosten die komen kijken van de ontwikkeling van cybersecurity in Den Haag zijn vaak al opgenomen in een gemeente breed inkoopbeleid en worden niet gezien als een separaat onderwerp op het gebied van cybersecurity volgens Marijn Fraanje (bijlage I). Het huidige smart city programma van de gemeente Den Haag sluit dan ook aan op het vernieuwde gemeente breed inkoopbeleid. Nieuwe projecten worden ingericht binnen de bestaande mogelijkheden. Dit gebeurt in nauw overleg met gemeentelijke specialisten (Van Engelshoven, 2015). Binnen het vernieuwde gemeente brede inkoopbeleid wordt er gestuurd op innovatie als een van de nieuwe beleidsdoelen naast duurzaamheid en MKB-vriendelijkheid. Dit schept de mogelijkheden om buiten het geijkte pad te treden voor het smart city programma van de gemeente Den Haag (Van Engelshoven, 2015).

4.2. Bedreigingen voor een smart city

In de afgelopen jaren is het aantal actoren dat cyberaanvallen uitvoert sterk toegenomen (Coats, 2018). Door de steeds bredere toegankelijkheid van gereedschappen om cyberaanvallen uit te voeren, is het voor actoren, die een aantal jaar geleden nog geen significante rol speelden, eenvoudiger geworden om hun competentie in te zetten tegen smart cities (AIVD, 2018). Ondanks dat de activiteiten van deze cybercriminelen een grote impact hebben, ligt de grootste cyberdreiging echter niet bij deze actoren. Het zijn namelijk statelijke actoren met als doel spionage, beïnvloeding, verstoring en sabotage die de grootste cyberdreiging vormen (Nationaal Coördinator Terrorisme Bestrijding en Veiligheid, 2018). Deze staten voeren hun cyberaanvallen meestal uit vanuit geopolitieke motieven. Wanneer deze aanvallen zich richten op smart cities, hebben zij als doel om kritieke subsystemen te verstoren of vernietigen en om strategische informatie te verwerven (NCTV, 2018). Cyberaanvallen vormen vandaag de dag een vast onderdeel van het arsenaal dat staten en criminelen inzetten om zo hun belangen in te willigen. De statelijke actoren maken, ondanks eigen expertise, vaak gebruik van derde partijen zodat zij zelf niet hoeven te investeren in de ontwikkelingen van dit arsenaal (Coats, 2018).

Er zijn meerdere redenen waarom staten en cybercriminelen hun zinnen zouden zetten op smart cities. Voor persoonlijke voldoeningen kunnen smart cities dienen als speeltuinen waarop ze hun hackvaardigheden kunnen testen en waar ze kunnen spelen met de technologie die daar beschikbaar is. De aaneenschakeling van ICT binnen smart cities kan voor cybercriminelen een manier zijn om kapitaal en individuele informatie te stelen van burgers en private partijen gevestigd in deze stad (Lin et al, 2017). Andere staten kunnen door middel van het misbruiken van de doordringendheid van smart city technologie hun eigen spionage- of hacktivistische campagnes starten en in zeer extreme gevallen zelfs gebruiken voor terreurdaden (Lin et al, 2017).

Om te weten hoe een smart city het best kan worden beveiligd tegen cyberaanvallen, is het noodzakelijk om te weten welke bedreigingen er zijn en op welke kwetsbaarheden deze kunnen inspelen. Li et al (2012) deelt verschillende cyberaanvallen in vier soorten: *device attack, data attack, privacy attack* en *network availability attack*. Iedere aanval heeft zijn eigen doel en zijn daarmee vaak de bouwstenen voor een geavanceerdere aanval. Via deze aanvallen kan er worden ingebroken in de kritieke subsystemen van een smart city, waardoor indringers de mogelijkheid krijgen om een cascade effect teweeg te brengen, zo bleek uit een interview met Wessel Sluis (bijlage II). Ook kunnen deze aanvallen de vorm aannemen van een DDoS-aanval, ook wel *distibuted denial of service*. Het doel van deze vorm van aanval is om elke vorm van communicatiebron binnen een systeem op te gebruiken of te overbelasten. De gevolgen hiervan zijn dat systemen worden vertraagd of geheel worden afgesloten van elke vorm van communicatie (Li et al, 2012).

Zo kreeg Nederland begin 2018 te maken met DDoS-aanvallen op verschillende overheidsinstanties. Het gevolg hiervan was dat zij een lange tijd slecht bereikbaar waren voor de bevolking. Onder andere de Belastingdienst, DigiD en Rijkswaterstaat waren slachtoffer van deze aanvallen (NOS, 2018). Naast deze overheidsinstanties is het ook duidelijk dat de gemeenten van smart cities in de toekomst ook niet bespaard zullen blijven. Ook zij zullen slachtoffers worden van DDoS-aanvallen of misschien wel erger. Naast DDoS-aanvallen heeft er in 2017 een geavanceerde sabotage-aanval plaatsgevonden, waarbij de Rotterdamse haven getroffen is door de neveneffecten hiervan. Deze neveneffecten hebben tot aanzienlijke economische schade geleid (AIVD, 2018). De cybercriminelen lijken de

nevenschade te accepteren of zijn zich niet bewust van deze nevenschade (Coats, 2018). Deze vorm van cyberaanvallen heeft met name een grote impact op smart cities wanneer kritieke infrastructuur wordt platgelegd, zoals de communicatie-, mobiliteits- en energievoorzieningen, en kan daarnaast ongecontroleerde verspreiding met zich meebrengen (NCTV, 2018). Net als bij de Rotterdamse haven kan dit zorgen voor grote economische schade aan een smart city.

Een *privacy attack* probeert de persoonlijke gegevens van mensen te verzamelen door middel van het kijken naar het energieverbruik (Li et al, 2012). Een smart city maakt gebruik van een zogenaamd *smart energy grid.* Dit houdt in dat alle energie binnen de stad digitaal gemanaged wordt. Hierbij moet er worden gedacht aan een intelligent energienetwerk, intelligente energiemeters en intelligente energieopslag (Ernst & Young, 2016). Binnen dit intelligente energienetwerk wordt er meerdere keren per uur gedetailleerde data doorgestuurd over energiegebruik. Aan de hand van deze gegevens kunnen aanvallers vaak precies ziet wat de dagelijkse activiteiten van iemand aangesloten op het energienetwerk zijn (Mármol et al, 2012). Daarnaast kan het blootleggen van gevoelige gegevens van overheden en private partijen een privacy schandaal teweegbrengen. Hierdoor verliezen de burgers of klanten het vertrouwen in deze instellingen.

Het wordt steeds lastiger om effectieve cybersecurity te leveren. De bestaande maatregelen komen steeds verder onder druk te staan, doordat bedrijven en instanties steeds vaker gaan samenwerken met externe partners. Hierdoor brokkelt de organisatorische afbakening van een overheid of bedrijf langzaam af (Ernst & Young, 2016). Cybercriminelen werken aan nieuwe technieken om bestaande cybersecurity te omzeilen en zo toegang te krijgen tot allerlei gegevens, van IP-adres tot aan individuele informatie. Ze manipuleren codes en processen en infecteren systemen met spyware en malware – dit alles doen ze om intellectueel eigendom te stelen en tegelijkertijd zoveel mogelijk schade aan te richten en gevoelige gegevens te verstoren (Lin et al, 2017).

Met de dag worden de cyberaanvallen geavanceerder en moeilijker te verslaan. Ze omvatten een sterke coördinatie tussen meerdere actoren en blijven niet binnen de nationale of regionale grenzen (Kim et al, 2012). In de toekomst zullen deze bedreigingen nog gevaarlijker zijn dan die vandaag de dag. Echter, door voortdurende ontwikkelingen binnen het cyberdomein en –aanvallen kan er niet met zekerheid worden gezegd wat voor soort bedreigingen er verwacht kunnen worden (Ernst & Young, 2016). Zo is er de veronderstelling dat drones een grote rol kunnen gaan spelen op het gebied van cyberdreigingen. Met de opkomende toename van drones verwacht men dat ze een grote rol zullen spelen in de toekomst van smart cities. Bij het overvloedige gebruik van drones in deze toekomstige smart cities komen echter ook een aantal technische en maatschappelijke uitdagingen kijken op het gebied van cybersecurity, privacy en de openbare veiligheid (Wright, in Vattapparamban et al, 2016). In eerste instantie kunnen deze drones gehackt worden en, hoewel gebruikt voor de verbetering van de samenleving, tegen de gebruiker of andere actoren worden gebruikt. Daarnaast kunnen drones ook worden ingezet om cyberaanvallen uit te voeren (Vattapparamban et al, 2016). Het wordt moeilijk om potentieel schadelijke drones te identificeren naarmate het aantal toeneemt. Hierdoor wordt het ook lastig om eventuele bedreigingen die deze drones kunnen veroorzaken te voorkomen. Door een drone uit te rusten met gereedschappen gebruikt door cybercriminelen, kunnen deze drones gebruikt worden om essentiële informatie te verkrijgen van overheden en private partijen. Dit gebeurt met behulp van netwerkexploitaties en aanvallen gebaseerd op malware (Vattapparamban et al, 2016).

Een drone hoeft dus maar simpelweg naast het gebouw van een overheidsinstelling te vliegen, de nodige informatie te verzamelen en weer weg te vliegen.

Naast het technologische aspect van cyberdreigingen, zit er ook nog een menselijke kant aan dit probleem. Om cyberaanvallen al tegen te gaan voordat ze gebeuren, is het van belang dat inwoners van smart cities zich bewust zijn van de processen omtrent cyberdreigingen en –security. Volgens Marijn Fraanje van gemeente Den Haag (bijlage I) is deze *cyberawareness* cruciaal. Vaak krijgen cybercriminelen namelijk toegang tot (kritieke) subsystemen door een persoonlijke fout van iemand. Er hoeft maar op een link geklikt te worden en cybercriminelen kunnen alle in plaats gebrachte cybersecurity zo omzeilen. Dit blijkt toch elke keer weer de grootste bron van een beveiligingslek. Volgens Waltz (1998) is de informatie en kennis verkregen door analyseren en grijpen van de huidige situatie, het product dat zorgt voor deze *cyberawareness*. Het verwijst naar het collectieve begrip van de staat van veiligheidsrisico's van een groep. Een grote uitdaging voor smart cities is dat de factoren die van invloed zijn op het veiligheidsrisico vaak niet openbaar gecontroleerd worden (Amoroso, 2012). Hierdoor krijgen de burgers vaak niets mee over de situaties die spelen en krijgen zij niet de kans om *cyberawareness* te ontwikkelen.

4.3. Zwakke plekken in het smart netwerk

De kwetsbaarheid van het smart netwerk hangt af van twee factoren: de grenzen van de technologie en hoe deze geïmplementeerd worden in een smart city (Lin et al, 2017). Net als de dreigingen die smart cities ondervinden, zijn de zwakke plekken in het netwerk van een smart city onder te delen in verschillende categorieën. Ook hier speelt het menselijk aspect op het gebied van cyberawareness weer een grote rol. Het is logisch dat steden zich bezighouden met het inpassen van goede technologische en procesmatige maatregelen, maar er blijft altijd een bepaald gevaar bestaan bij hoe gebruikers gebruik maken van de toepassing (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Hiermee kan men dus stellen dat de gebruiker, indien niet goed geïnformeerd of bewust van de aanwezige dreiging, altijd een zwakke plek zal zijn in het netwerk. Met de opkomst van nieuwe *smart technologies* en vormen van beveiliging, worden inwoners van een smart city dagelijks blootgesteld aan het gebruik hiervan (Elmaghraby & Losavio, 2014). Woningen, auto's, publieke ruimtes en andere sociale systemen zullen in de nabije toekomst in zijn geheel met elkaar verbonden zijn. Dit staat ook wel bekend als 'het internet der dingen'. Voor al de systemen die onderling met elkaar verbonden zijn, worden nieuwe standaarden gevormd (Elmaghraby & Losavio, 2014). Met deze nieuwe standaarden, lijkt het of de inwoners steeds meer worden geïnstrueerd met gegevens over hun verblijfsplaats en activiteiten, waardoor privacy langzamerhand begint te verdwijnen. Indien de inwoners van smart cities steeds vaker met deze fenomenen te maken zullen krijgen, zullen overheden en private partijen zich vaker moeten gaan focussen op de enige zwakke plek die ze zelf niet volledig in de hand hebben: de menselijke gebruiker.

Maar ook de gebreken in technologie spelen een grote rol in het vormen van zwakke plekken binnen een smart netwerk. Zo blijk uit het interview met Wessel Suis (bijlage II) dat deze netwerken een bepaalde mate van complexiteit bevatten. Naar mate de systemen complexer worden door de toevoeging van meer systemen en nieuwe technologieën, neemt ook de kwetsbaarheid toe. Deze kwetsbaarheid valt te mitigeren door het installeren van sensoren, maar ook deze sensoren moeten weer voorzien worden van intelligentie. Zonder deze intelligent kunnen sensoren overheden en private partijen alleen voorzien van camerabeelden en niet van de data nodig om kwetsbaarheden op te

sporen zodat deze kunnen worden aangepakt. Deze sensoren vereisen een inzicht in het netwerk en soms ook controle over het netwerk (Morren & Slootweg, 2016).

De al eerder besproken cyberdreigingen en de technologie die door smart cities wordt gebruikt, kunnen dienen als platform voor verschillende mogelijke cyberaanvallen. Elke nieuwe technologie of systeem die toegevoegd wordt aan het smart netwerk, creëert nieuwe kansen voor cybercriminelen om binnen te komen en scharen zichzelf hierdoor dus onder de categorie van zwakke plekken in het netwerk (Cerrudo, 2015). In zijn werk behandelt Cerrudo (2015) verschillende subsystemen van het smart netwerk die kunnen dienen als toegangspoorten voor cybercriminelen met kwade intenties. De verkeerscontrolesystemen binnen een smart city kunnen eenvoudig gehackt worden en vormen hiermee dus een makkelijk doelwit (Ghena et al, 2014). De apparaten gebruikt in het verkeerscontrolesystemen zijn vaak niet voorzien van codering, waardoor cybercriminelen toegang kunnen bemachtigen tot de communicatie tussen de verkeersregelingssystemen en de verkeerlichten. Hiermee kunnen ze de verkeerslichten direct veranderen (Ghena et al, 2014). Smart cities hebben vaak niet de middelen om te detecteren dat cybercriminelen via hun achterdeur toegang krijgt tot hun systemen. Zo kunnen zij bijvoorbeeld ook toegang krijgen tot de draadloze systemen voor straatverlichting die in steden wereldwijd worden gebruikt (Philips, 2018). Deze draadloze systemen hebben dezelfde problemen met codering als de verkeerscontrolesystemen en omdat ze niet complex van aard zijn kunnen ze eenvoudig worden gehackt. Echter, kan hiermee een black-out worden veroorzaakt in grote delen van de stad (Cerrudo, 2015).

Maar ook de overheidsinstellingen zelf kunnen een zwakke plek vormen in het smart netwerk. Overheden hebben vaak de controle over een grote hoeveelheid systemen om verschillende diensten en taken te kunnen uitvoeren. Door een slechte mate van cybersecurity en onvoldoende monitoren van hun eigen systemen leggen overheden zich bloot voor verschillende cyberaanvallen. Het hacken van deze systemen geven staten en cybercriminelen de kans om veel schade te kunnen veroorzaken (Cerrudo, 2015). De documenten en persoonsgegevens in het bezit van de overheid spelen een cruciale rol in onze samenleving. Wanneer overheden hun zaken niet op orde hebben en criminelen makkelijk bij deze gegevens kunnen, ontstaat er een kans dat de burgers hun vertrouwen in de overheid verliezen. Dit verlies in vertrouwen zou niet alleen slecht zijn voor de overheid, maar ook voor de bedrijven die betrokken zijn geweest bij het beveiligen van deze kwetsbare gegevens (Conklin & White, 2006). Daarnaast is het ook aan overheden om hun systemen actief te laten testen. Sommige overheden trekken een aantal muren op en steken daarna de kop in het zand, hopend dat alles goed gaat. Deze aanpak kan een overheid juist de kop kosten volgens Marijn Fraanje (bijlage I). Door het niet actief monitoren van hun netwerken en kanalen naar de buitenwereld halen overheden cybercriminelen binnen. Het ontbreken van een interne ICT-dienst binnen een gemeente is dan ook zonder meer een zwakke plek binnen het netwerk. Smart cities moeten zich constant blijven aanpassen aan de ontwikkelingen binnen de ICT. Organisaties kunnen deze ontwikkelingen vaak niet bijbenen en dit zorgt voor gaten in hun beveiliging (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Maar zelfs met al deze technologische en procedurele maatregelen is niemand 100% veilig voor cyberaanvallen. Als een aanvaller echter binnen wilt komen, dan lukt dat hem wel.

4.4. Maatregelen om de kwetsbaarheid te verminderen

Om nieuwe en geavanceerde technologieën te kunnen ondersteunen vereist een smart city een hoge mate van netwerkconnectiviteit. Met deze hoge mate van connectiviteit wordt, zoals eerdergenoemd, ook de complexiteit van het netwerk vergroot – deze complexiteit brengt kwetsbaarheden met zich mee (Bartoli, 2011). Een van de grootste uitdagen van smart cities is dan ook de beveiliging van de stad. Het toenemende aantal cyberaanvallen op de kritieke infrastructuur van smart cities zorgt ervoor dat cybersecurity hoog op de agenda staat bij overheden en bedrijven (NCSC, 2014). De focus van cybersecurity ligt vaak op drie verschillende vlakken: technologische maatregelen, procedurele maatregelen en menselijke maatregelen (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Dit omdat cybersecurity vaak niet alleen te maken heeft met opzettelijke aanvallen, maar ook met onbedoelde verstoring in de ICT zoals gebruikersfouten en apparatuur storingen (Bartoli, 2011). Deze maatregelen moeten rekeningen houden met een select aantal problemen om smart cities om de juiste manier te beschermen: privacy, netwerkconnectiviteit, complexiteit, beveiligingsdiensten en de beschikbaarheid van deze diensten (Bartoli, 2011). Volgens Ernst & Young (2016) veronderstelt een standaardaanpak voor risicobeheer dat een vertrouwensgrens al is gedefinieerd. Nieuwe processen en een nieuw beleid zijn nodig om de risicogrens uit te breiden. Dit biedt de mogelijkheid voor smart cities om de technologische ontwikkeling op de voet te kunnen volgen (Ernst & Young, 2016).

4.4.1. Technologische maatregelen

Een van de belangrijkste technologische maatregelen, misschien zelfs de belangrijkste, is het monitoren van het netwerk en daarbij horende cybersecurity. Het goed monitoren van het netwerk stelt smart cities in staat aanvallers op te sporen voordat zij schade kunnen aanbrengen aan het netwerk (Kitchin, 2016). Ook wordt deze data gebruikt voor besluitvorming en probleemoplossing. Achteraf kan deze data zelfs gebruikt worden om bepaalde aspecten van het leven in smart cities te onderzoeken en zo voorspellende modellen op te stellen die betrekkingen hebben tot ex post maatregelen bij cyberaanvallen (Kitchin, 2016). In het interview met Wessel Sluis (bijlage II) stelt hij ook dat deze data en modellen gebruikt worden voor het creëren van simulaties die kunnen dienen als trainingsmiddelen. Door het zorgvuldig analyseren van deze simulaties kunnen overheden en bedrijven erachter komen wat de beste ex post maatregelen zijn indien een cyberaanval zich voordoet.

Het uitvoeren van kwaliteitsinspecties en penetratietesten is ook een belangrijke maatregel in de strijd tegen cybercriminelen en –terroristen. De *smart technologies* die smart cities gebruiken ten behoeve van het verbeteren van de levenskwaliteit van de inwoners in de stad, moeten worden onderworpen aan strenge controles en testen voordat deze worden geïmplementeerd in de hele stad (Lin et al, 2017). Op deze manier kunnen smart cities de ontstane problemen al verhelpen voordat deze technologie voor de inwoners beschikbaar komt. Net als de gemeente Den Haag, kunnen smart cities gebruiken maken van de expertise van externe actoren en deze inhuren om penetratietesten uit te laten voeren. Standaard productprocedures worden ook verplicht uitgevoerd, aangezien penetratietesten zich alleen richten op de kwetsbaarheden van het systeem (Lin et al, 2017).

Naast het monitoren en uitvoeren van testen is er natuurlijk ook nog een breed scala aan hardware- en softwareapplicaties die smart cities kunnen gebruiken om cyberaanvallen te voorkomen. Firewalls, end-to-end encryptie, virus- en malwarescanners en sterke wachtwoord- en toegangscontroles zijn hier een aantal voorbeelden van (Ernst & Young, 2016). Deze applicaties zorgen ervoor dat toegang tot gevoelige gegevens en kritieke subsystemen ontzegd wordt voor cybercriminelen en indien ze een

weg naar binnen vinden, deze te vertragen. Hardware- en softwareapplicaties vormen een kritieke basis van elke simpele vorm van cybersecurity (Yan et al, 2012). Omdat het niet mogelijk is om alle toekomstige dreigingen of alle verschillende aanvalsmethode te voorzien, wordt er ook wel een meerlaagse benadering gebruikt (Jennex, 2007). Het is een concept dat meerdere compenserende hardware- en softwareapplicaties in lagen gebruikt om zo een bedreiging te voorkomen of te verminderen (Bass & Robichaux, 2002). De inspanning die nodig is om het netwerk aan te vallen wordt verhoogd door het gebruik van meerdere onafhankelijk controles. Wanneer één van deze controles wordt omzeild of beschadigd raakt, bieden de andere lagen nog steeds bescherming (Bass & Robichaux, 2002). Door het gebruik van deze benadering kunnen smart cities de basis van hun cybersecurity op een simpele manier verbeteren.

4.4.2. Procedurele maatregelen

Het is onvermijdelijk dat bij het ontwikkelingen, implementeren en onderhouden van een cybersecurityprogramma veel planning en documentatie komt kijken. Meestal gebeurt dit in de vorm van beleid en procedures (Marsteller et al, 2014). Smart cities kunnen door middel van een MISPP-document (*Master Information Security Policy & Procedures*) te ontwikkelen, een handleiding creëren voor hun cybersecurityprogramma. In deze handleiding staan onder andere een overzicht van het project, een samenvatting van rollen en verantwoordelijkheden, een georganiseerde lijst van andere beleidsdocumenten met informatie over cybersecurity en de kernprocedures voor het ontwikkelen, implementeren en onderhouden van het programma (Marsteller et al, 2014).

Een andere procedurele maatregel is het opstellen van een cybersecuritykader, zoals het NIST-CSF (*National Institute of Standards and Technology Cybersecurity Framework*). Een cybersecurity kader representeert een samenwerking tussen private partijen en de overheid en bestaat uit standaarden, richtlijnen en werkwijzen voor het beheersen van cybersecuritygerelateerde risico's (Jackson et al, 2017). De flexibele en kosteneffectieve aanpak van een cybersecuritykader draagt bij aan de bescherming en veerkracht van de kritieke infrastructuur van smart cities (Jackson et al, 2017). Smart cities kunnen cyberdreigingen detecteren, beperken of erop reageren door middel van een op risico's gebaseerde aanpak van een cybersecuritykader. Een cybersecuritykader vertrouwt op een verscheidenheid aan bestaande richtlijnen en werkwijzen om cybersecurity van kritieke infrastructuren veerkrachtig te kunnen laten handelen, in plaats van het ontwikkelen van nieuwe cybersecurity normen en riskmanagementprocessen (Shackelford et al, 2015). Een cybersecuritykader biedt een "gemeenschappelijke taal" voor zijn gebruikers. Hiermee kunnen zij hun huidige cybersecurity evalueren, hun beoogde staat van cybersecurity bepalen en prioriteit geven aan mogelijkheden voor verbetering (Shackelford et al, 2015). Ook kan een cybersecuritykader helpen bij het ontwikkelen van voldoende communicatie tussen interne en externe partijen over cyberdreigingen (Shackelford et al, 2015).

Ook op het gebied van wetgeving kunnen er procedurele maatregelen worden ingevoerd. Wetgevende en regelgevende maatregelen moet helpen om een milieu te creëren waarin cybercriminelen een verhoogd gevoel van risico oplopen en de voorwaarden om een cyberaanval te plegen minder gunstig zijn (Ghernouti-Hélie, 2010). Het werken aan effectieve en operationele juridische, procedurele en organisatorische maatregelen kan bijdragen aan het verminderen van cyberdreigingen voor smart cities. Nationale overheden moeten in samenwerking met smart cities een afdwingbaar wettelijk kader opstellen. Hierbij moet de strafwetgeving worden bijgewerkt om het gebruik van ICT gelijkwaardig te

dekken (Schjolberg & Ghernouti-Hélie, 2011). Smart cities moeten via procedurele maatregelen toegang krijgen tot opgeslagen of doorgegeven gegevens, zonder de privacy, vrijheden en veiligheid van de burgers te schaden. Daarnaast moeten rechters, politie, advocaten en onderzoekers – de opkomst van de netwerkmaatschappij in acht nemende – worden opgeleid om om te gaan met het verwerven, bewaren, analyseren en interpreteren van digitale informatie (Schjolberg & Ghernouti-Hélie, 2011; Van Dijk, 2001). Smart cities moeten een adequaat grondwerk leggen met behulp van procedurele maatregelen, om zo een toegangspoort te creëren voor cybersecurity om een zo sterk mogelijke verdedigingslinie neer te kunnen zetten.

4.4.3. Menselijke maatregelen

De grootste van de maatregelen binnen het menselijk aspect van cybersecurity is *cyberawareness*. Net als de gemeente Den Haag, die veel geld steekt in *awareness* campagnes, zouden smart cities de *cyberawareness* van hun inwoners hoog in het vaandel moeten nemen. Mensen zijn interactief betrokken bij de maatschappij die zich vormt in smart cities (van Dijk, 2001a). Zo hebben de inwoners van smart cities vaak toegang tot verschillende applicaties vanuit het smart netwerk van de stad. Door deze verbintenis van de burger aan het netwerk vormt de burger een toegangspoort voor cybercriminelen om het netwerk binnen te dringen (Elmaghraby & Losavio, 2014). Door de burger te voorzien van een bewustzijn over de mogelijkheden die *smart technology* en cybersecurity bieden, kunnen zij worden ingezet om cyberaanvallen tegen te gaan. Door cybercriminelen de toegang te ontnemen om via onwetende burgers het netwerk te betreden, wordt het risico van cyberdreigingen significant vermindert (Bartoli, 2011). In het interview met Marijn Fraanje (bijlage I) kwam onder andere ook naar voren dat mensen zich aangetrokken voelen tot de blootstelling van cybersecurity. Het is belangrijk dat de inwoners van een smart city zien waar hun overheid mee bezig is om zo een betere *cyberawareness* te creëren.

Door middel van *cyberawareness* kunnen smart cities hun burgers inlichten over de gevaren van cyberdreigingen. Dit kan door grote groepen tegelijk te voor zien van deze informatie met behulp met *fear appeals*, of op een kleinere schaal door middel van gespecialiseerde trainingen (Evans et al, 2016). Deze zogenaamde *fear appeals* zijn overtuigende mededelingen die een element van angst bevatten om een door het management gewenste uitkomst te bewerkstelligen (Johnston & Warkentin, 2010). Aangezien de ontvangers van het bericht een cognitief proces ondernemen om dreiging af te wenden, zouden positieve *fear appeals* een proces van risicobeheersing bevorderen, wat kan leiden tot een succesvol resultaat (Evans et al, 2016). Deze vormen van promotie worden onder meer gebruikt in de gezondheidszorg en marketing om het sentiment tegen roken te bevorderen, maar zouden ook goed hun intrede kunnen maken in de wereld van cybersecurity. Er moet wel rekening gehouden worden met wanneer deze vorm van *cyberawareness* wordt toegepast; wanneer smart cities waarschuwingen gaan afgeven omtrent privacy (bijvoorbeeld bepaalde persoonsgegevens), dit ervoor kan zorgen dat mensen geen gebruik willen maken van bepaalde smart city applicaties, terwijl ze tal van andere applicaties gebruiken die precies hetzelfde doen (maar ze er bij deze applicaties geen weet van hebben) (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Ook kan het zo zijn dat het bericht dat smart cities proberen over te brengen genegeerd wordt, verkeerd wordt begrepen of gewoon simpel weg wordt genegeerd door de inwoners (Johnston & Warkentin, 2010). Dit is een reden waarom overheden en andere instanties nooit volledig moeten vertrouwen op de efficiëntie van deze benadering en het alleen moeten gebruiken als waarschuwingsmechanisme.

Naast de cyberawareness campagnes voor een groot publiek worden er gespecialiseerde trainingen gegeven aan mensen die werken bij bedrijven met controle over kritieke infrastructuren. Voor deze bedrijven staat de bewustwording van hun personeel hoog op de agenda (NCSC, 2014). Volgens een beschouwing van PWC (2015) zijn mensen de grootste kwetsbaarheden voor een veilige onderneming. Uit het onderzoek blijkt dat van alle factoren die hebben bijgedragen aan een toename in cyberdreigingen, 81% daarvan te wijten was aan menselijk fouten en het onbewust zijn op het gebied van deze dreigingen (PWC, 2015). Door het geven van deze trainingen worden bedrijven ervan verzekerd dat hun personeel zich beter bewust is van cyberdreigingen en de mogelijk schade die cyberaanvallen kunnen aanrichten aan de kritieke infrastructuur.

4.5. Implementatie cybersecurity in (stedelijk) beleid

Het woord 'beleid' kan worden toegepast op verschillende situaties die betrekking hebben op cybersecurity. Het wordt onder andere gebruikt om te verwijzen naar verschillende wet- en regelgevingen omtrent informatieverspreiding en doelstellingen van bedrijven die te maken krijgen met databescherming (Gallaher et al, 2008).

Tijdens de transformatie van een normale stad naar een smart city gaan de ontwikkelingen binnen de ICT gepaard met verschillende politieke en institutionele componenten (Mauher & Smokvina, 2006). De politieke elementen in deze transformatie worden gerepresenteerd door het stedelijke bestuur en de nationale overheid met de daarbij behorende politieke agenda en politiek die invloed heeft op de ontwikkelingen van ICT. Institutionele paraatheid is van groot belang voor een soepele implementatie van cybersecuritybeleid binnen smart cities. Dit houdt in: het wegnemen van wettelijke en regelgevende belemmeringen omtrent het cyberdomein (Rocheleau, 2003). Naast het stedelijk bestuur en de nationale overheid zijn er ook andere actoren die van belang zijn bij het creëren van een bruikbaar beleidskader voor cybersecuritybeleid. Externe actoren, zoals cybersecuritybedrijven, oefenen niet alleen invloed uit op het gedrag van de opdrachtgever, maar ook op anderen. Hiermee worden zij stakeholders in het beleid (Bayuk et al, 2012). Echter, worden voor deze externe actoren wel normen vastgesteld door het bestuursorgaan om te voldoen aan het beleid.

Het gebruik van ICT op de juiste manier vereist een goed begrip van het toepassen van deze ICT. Hiervoor is de beleidscontext van cruciaal belang. Een innovatieve overheid kan niet innoveren zonder een maatgevende gedrevenheid in het beleid en zal vandaar ook de veranderingen in het beleid benadrukken (Eger & Maggipinto, 2010). De beleidscontext karakteriseert zowel de institutionele als niet aan ICT gerelateerde stedelijke kwesties en schept hiermee voorwaarden die stedelijke ontwikkeling mogelijk maken. Wijzigingen in de beleidscontext zijn ingewikkeld, terwijl innovatie in de ICT makkelijk kan worden waargenomen en toepast in een smart city (Hartley, 2005).

Er komen veel uitdagingen kijken bij het wijzingen van het huidige beleidskader en de beleidsomgeving waarin de overheid opereert. Het probleem ligt niet alleen bij het feit dat het huidige beleidskader niet toereikend genoeg is voor het systematisch oplossen van de problemen omtrent cybersecurity, maar er moet ook rekening gehouden worden met normen, waarden en gedrag dat mensen als goed of vanzelfsprekend beschouwen (Scott, 2013). Het voeren van adequaat cybersecuritybeleid is op dit moment een grote uitdaging voor organisaties in de publieke sector (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Vaak zijn implementaties van cybersecuritybeleid grote en langzame (verander)trajecten die na invoering al weer achterlopen op de huidige ontwikkelingen, wat een groot

risico met zich mee brengt. De veranderingen in beleid kunnen de technologische ontwikkelingen niet bijbenen.

De verschillende opvattingen over beleid en governance die hierboven geschetst zijn, zorgen voor implicaties voor de rol van beleidsmakers bij het opstellen van cybersecuritybeleid. In deze benadering is het creëren van wetgeving en het ondersteunen van de grootschalige veranderingen die hierdoor teweeg worden gebracht een belangrijke rol van de beleidsmakers (Moore, 1995). De ontwikkelingen die plaatsvinden binnen de overheden van smart cities stellen de beleidsmakers in staat een leidende rol aan te nemen bij het vertalen van nieuwe ideeën naar vormen van actie en onderneming (Hartley, 2005). Nationale overheden blijven door middel van grootschalige wetgeving innoveren, terwijl de beleidsmakers zich bezighouden met het ondersteunen van cybersecurity innovatie en het orkestreren van de belangen van actoren die betrokken zijn bij het beveiligen van smart cities (Hartley, 2005). Volgens Moore (1995) spelen beleidsmakers een grote rol binnen het koesteren van innovatie:

> "…explorers commissioned by society to search for public value. In undertaking the search, managers are expected to use their initiative and imagination. But they are also expected to be responsive to more or less constant political guidance and feedback."

Beleidmakers spelen in op de ontwikkelingen die ontstaan als product van innovatie binnen de ICT. Volgens Wessel Sluis (bijlage II) moet er eerst een aanleiding zijn voordat bepaalde processen in beweging worden gezet. Hetzelfde geldt voor cybersecuritybeleid. Er moet zich eerst een probleem voordoen binnen de ICT, zoals een informatielek of bepaalde economische schade, voordat men hier naar gaat handelen. Zowel lokale overheden van smart cities als nationale overheden moeten zichzelf in de komende jaren aanpassen aan deze nieuwe omgeving om de aankomende uitdagingen boven het hoofd te blijven en om ervoor te zorgen dat hun inwoners hun vertrouwen niet verliezen in hun vermogen dingen voor elkaar te krijgen (Mauher & Smokvina, 2006).

4.5.1. Schaalvergroting van smart city governance

Binnen smart cities valt de drijfveer achter de innovatie binnen cybersecurity op te delen tussen verschillende actoren. Deze verspreiding van innovatie naar andere organisaties en plaatsen is van groot belang voor de publieke sector (Rashman & Hartley, 2002). Hierin verschillen overheden met private partijen. Overheden houden zich vooral bezig met innovatie gedreven door het verbeteren van governance en serviceprestaties om de publieke waarde te vergroten, terwijl de innovatie binnen bedrijven zich laat leiden door concurrentievoordelen. Er wordt ook gesproken van concurrentievoordelen wanneer bedrijven terughoudend zijn in het delen van informatie met actoren die zich niet kenmerken als (strategische) partners (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Terwijl overheden, zoals de gemeente Den Haag, juist deze informatie delen met verschillende actoren, om hier een zo groot mogelijk publieke waarde uit te kunnen halen. In het interview met Marijn Fraanje (bijlage I) laat hij dan ook weten dat overheden in een bepaalde verhouding staan ten opzichte van private partijen. Overheden gaan vaak een samenwerking aan met private partijen, omdat zij een zekere expertise bezitten die niet terug te vinden is in de publieke sector. Echter, geven de smart cities de regie niet uit handen. Dit komt omdat de private partijen waar zij mee samenwerken vaak al vaste partners zijn van overheden en daardoor ook niet de drang hebben invloed uit te oefenen over beleidsprocessen volgens Marijn Fraanje (bijlage I).

Naast deze benadering tot private partijen handelen smart cities ook naar de behoeven van hun inwoners. De betrokkenheid van burgers is dan ook een fundamentele hoeksteen van smart city governance (Castelnovo et al, 2016). De traditionele methoden waarmee het complexe samenspel tussen technologische kennis en politieke beperkingen werd onderbouwt voldoet niet langer aan de hedendaagse eisen van publieke besluitvorming en een nieuwe vorm van publieke participatie is dan ook hoognodig (Pardo & Taewoo, 2011). Smart cities moeten inwoners betrekken bij de beslissingen die genomen moeten worden, omdat het hen ook aangaat. In een samenleving waar onderlinge verbintenis met behulp van ICT centraal staat, kan het niet anders dat inwoners een integraal onderdeel zijn van de besluitvorming. Echter, wordt het stimuleren van burgerparticipatie in beleidsbeslissingen beslecht door indicaties die een typisch top-down besluitvormingsproces volgen (Castelnovo et al, 2016). De inwoners worden niet direct betrokken bij het vormen van publieke diensten en netwerkapplicaties. Deze worden eerst gevormd door de overheid, waarna de burger pas betrokken raken door middel van online en offline initiatieven waar zij hun kritiek en suggesties kunnen achterlaten (Castelnovo et al, 2016). ICT kan gebruikt worden om de participatie van burgers te verhogen. Met behulp van social media en het ontwikkelen van slimme applicaties, zoals Den Haag hun mobiele game, kan het aantal deelnemer aan het publieke debat worden uitgebreid en kan er een stem worden gegeven aan de personen die gewoonlijk niet zouden deelnemen aan deze vorm van discussie (Gupta et al, 2012). Door het toepassen van deze benaderingen betrekt een smart city zowel zijn burgers als de private partijen bij de besluitvorming en kan het optimaal handelen naar de uitkomsten van deze participatie.

4.6. Urgentie en kosten van cybersecurity

Met de snelle ontwikkelingen binnen de ICT en de implementatie van deze technologie in steden, neemt de urgentie voor cybersecurity in smart cities toe (Caruson et al, 2012). Steeds vaker verloopt de communicatie tussen en binnen actoren via het digitale netwerk. Wanneer de beveiliging van dit netwerk te kort schiet, heeft dit een direct effect op de beschikbaarheid en betrouwbaarheid van het netwerk (NCSC, 2014). Volgens het NCSC (2014) hebben cyberaanvallen een toenemende impact op het functioneren van de kritieke infrastructuur binnen smart cities, waardoor de belangen van individuen, private partijen en de maatschappij in het geheel in gevaar komen. Cybersecurity is fundamenteel voor smart cities. Het welzijn van de inwoners is een uiterst belangrijke verantwoordelijkheid die ligt bij het stadsbestuur van smart cities (Elmaghraby & Losavio, 2014). Net als bij de gemeente Den Haag, staat cybersecurity en de verbetering van zijn kwaliteit dus hoog op de agenda voor de meeste steden. In het interview met Wessel Sluis (bijlage II) wordt er benadrukt dat informatie omtrent cybersecurity van smart cities vertrouwelijkheid factor één betreft. Wanneer dit niet wordt gewaarborgd, kan belangrijke informatie over de cybersecurity van smart cities terecht komen bij cybercriminelen. Deze cybercriminelen hebben toegang tot nieuwe digitale producten en processen waarvoor nog geen maatregelen voor zijn getroffen. Doordat het potentieel voor schade van aanvallen steeds groter wordt, neemt ook het belang van cybersecurity toe (NCSC, 2014).

Bijna tien jaar geleden stond een zekere bezorgdheid over cybersecurity en begrotingstekorten centraal en is het vooral belangrijk dat overheden hun prioriteiten op orde hebben (Reddick, 2010). Dit is nog steeds zo. Er tekent zich een spanningsveld af tussen aan de ene kant cybersecurity en aan de andere kant kostenreductie (NCSC, 2014). Wanneer het aankomt op cybersecurity in smart cities gaat het in de praktijk vaak om een kostenafweging (Ernst & Young, peroonlijke communicatie, 16 juli, 2018). Er moeten worden gekeken of de baten wel opwegen tegen de kosten. Kostenreductie is vaak

een belangrijke reden voor smart cities om ondersteunde ICT-processen uit te besteden aan externe actoren (NCSC, 2014). Daartegenover staat dat het gevoel van controle vaak afneemt bij smart cities, omdat de interne expertise over de ingekochte producten en diensten ook afneemt (NCSC, 2014). Echter, is dit niet het geval volgens Marijn Fraanje (bijlage I). Overheden houden nog steeds de controle in handen. De kosten die hierbij komen kijken worden vaak, net als bij Den Haag, meegenomen in deze nieuwe ontwikkelingen en zijn een integraal onderwerp van het terrein waarop deze ontwikkelingen plaatsvinden. Hierdoor hoeft er door overheden ook niet geschoven te worden binnen de begroting.

Naast de kosten voor het opzetten van cybersecurity, krijgen de verschillende actoren betrokken bij de transformatie van steden naar smart cities ook te maken met eventuele kosten opgelopen door schade van cyberaanvallen. Private partijen kunnen te maken krijgen met inbreuken op intellectueel eigendom en lopen hier door een groot risico op financiële schade (NCSC, 2014). Ook de mondiale economie leidt schade door cyberaanvallen. Aan het begin van deze eeuw bedroeg de schade gedaan aan de economie alleen al een bedrag in de honderdeden miljarden (Cashell et al, 2004). Wereldwijd verliezen private partijen in de honderden miljarden euro's als gevolg van inkomstenderving, verlies aan concurrentiepositie en door de kosten van cybersecuritymaatregelen (NCSC, 2014). Deze kosten zullen de aankomende jaren niet afnemen, aangezien cybercriminelen nieuwe manieren zullen vinden om bestaande cybersecuritymaatregelen te omzeilen.

5. Cybersecurity: de ketting is zo sterk als zijn zwakste schakel

In dit onderzoek is getracht een bijdrage te leveren aan de theorieontwikkelingen met betrekking tot smart city cybersecurity, door te onderzoeken welke mogelijkheden van cyberdreigingen en –security er zijn, hoe deze toepassingen het best kunnen worden opgenomen in (stedelijk) beleid en hoe hoog de urgentie en kosten van cybersecurity liggen. Door middel van uitgebreid literatuuronderzoek en interview is geprobeerd een antwoord te vinden op de vraag welke ex ante en ex post mogelijkheden er zijn voor een smart city om zich aan te passen aan cyberdreigingen en daarmee hun cybersecurity te waarborgen.

Gebleken is het aantal cyberaanvallen in de afgelopen jaren sterk is toegenomen. Doordat kwaadwillende actoren een steeds bredere toegankelijkheid hebben tot gereedschappen om cyberaanvallen mee uit te voeren, lukt het ze steeds vaker om de cybersecurity van smart cities te omzeilen. Toch ligt de grootste dreigingen niet bij cybercriminelen, maar bij statelijke actoren die met de hulp van derde partijen zich richten op het beïnvloeden, verstoren en saboteren van de kritieke infrastructuur van een smart city of haar bestuurlijke organisatie. Op deze manier kunnen zij steden aanzienlijke schade toedienen op zowel economisch als bestuurlijk gebied. Door zich te richten op de economie, kunnen zij de kosten bij private partijen en overheden hoog laten oplopen. Daarnaast zullen burgers bij het verlies en manipuleren van persoonsgegevens hun vertrouwen verliezen in de overheid. Globaal worden overheden en bedrijven dagelijks getroffen door verschillende vormen van cyberaanvallen. Van het stelen van persoonlijke gegevens door middel van *privacy attacks* tot aan de welbekende DDoS-aanvallen die complete digitale systemen voor meerdere uren kunnen platleggen. Het wordt steeds lastiger om een effectieve beveiliging te leveren tegen de constant ontwikkelende vormen van cyberdreigingen. Ook omdat de dreigingen niet alleen aan de technologische kant van het verhaal liggen. Burgers die zijn onvoldoende bewust zijn van cyberdreigingen en –security spelen een grote rol bij het creëren van toegangspoorten voor kwaadwillende actoren. Doordat zij niet goed zijn ingelicht over de mogelijke dreigingen in het cyberdomein, kunnen zij via het openen van links en het onderbewust doorsturen van gevoelige informatie de deuren wagenwijd openzetten voor cybercriminelen zonder dat overheden en bedrijven hier iets aan kunnen doen.

Wanneer er wordt gekeken naar de zwakke plekken in het smart netwerk die kunnen bijdragen aan de kwetsbaarheid van smart cities, kan er worden gesteld dat deze afhangt van twee verschillende factoren. Het functioneren van cybersecurity hangt af van de grenzen die gesteld zijn aan de huidige vormen van technologie. Deze begrenzing vormt een zwakke plek in het smart netwerk, omdat de technologie toegepast in de beveiliging niet kan voldoen aan de nieuwe technologische standaarden, Hierdoor kunnen cyberaanvallen deze beveiliging met gemak passeren. Daarnaast kan ook technologie een zwak punt in het netwerk vormen wanneer deze niet goed is geïmplementeerd. Door de ontoereikende implementatie en kennis van nieuwe technologie kunnen er hiaten in het systeem ontstaan, via waar cybercriminelen hun weg kunnen vinden naar de kern van het netwerk en deze plat kunnen leggen of kunnen gebruiken voor eigen doeleinden. Deze zwakke plekken kunnen worden ingedeeld in drie aspecten: het technologische aspect (inpassing van ontoereikende of gedateerde technologische applicaties), het procedurele aspect (het gebruik maken van gedateerde procedures en processen om cyberaanvallen te voorkomen of op te lossen) en het menselijke aspect (het niet bewust zijn van de burgers over cyberdreigingen en –security).

Ook de maatregelen die smart cities kunnen treffen om zichzelf weerbaar te maken tegen cyberaanvallen kunnen ingedeeld worden in deze drie aspecten. Deze zijn op hun eigen beurt ook weer in te delen in ex ante en ex post maatregelen, waarbij ex ante maatregelen zich bezighouden met het voorkomen van cyberaanvallen en ex post maatregelen zich bezighouden met het oplossen van cyberaanvallen en de schade die erbij is ontstaan. Daarbij moeten cybersecuritymaatregelen ook de volgende aspecten in acht nemen om smart cities op een juiste manier te voorzien van een goede beveiliging: privacy, netwerkconnectiviteit, complexiteit, beveiligingsapplicaties en de beschikbaarheid van deze applicaties. Deze aspecten vormen samen de basis van elke maatregel genomen tegen cyberaanvallen.

Technologische maatregelen houden zich onder andere bezig met het monitoren van het netwerk en de daarbij horende beveiliging. Deze maatregelen zijn over het algemeen ex ante. Het monitoren is cruciaal en misschien wel de belangrijkste van alle technologische maatregelen samen met het proactief testen van de geïmplementeerde cybersecurity. Daarnaast vallen verschillende hardware- en softwareapplicaties, zoals firewalls, end-to-end encryptie, virus- en malwarescanners en wachtwoord- en toegangscontroles, ook onder technologische maatregelen. Deze applicaties weerhouden cybercriminelen ervan om toegang te krijgen tot de kritieke infrastructuur en gevoelige gegevens.

Procedurele maatregelen zijn ex post maatregelen. Hiermee kunnen overheden en private partijen de staat van hun huidige cybersecuritymaatregelen evalueren, de beoogde staat van cybersecurity bepalen en prioriteiten leggen waar er ruimte is voor verbetering. Door het opstellen van een cybersecuritykader kan een smart city cyberdreigingen detecteren, beperken en erop reageren voordat er schade wordt aangericht. Ook kan er op het gebied van wetgeving procedurele maatregelen worden genomen. Door het opstellen operationele juridische, procedurele en organisatorische maatregelen omtrent cybersecurity, stellen overheden zichzelf en private partijen in staat om een adequaat grondwerk te leggen voor een zo sterk mogelijke verdedigingslinie tegen cyberdreigingen.

Menselijke maatregelen richten zich vooral op het bewust maken van de inwoners van een smart city met betrekking tot cyberdreigingen en –security. Het vergroten van *cyberawareness* onder de bevolking kan gezien worden als de belangrijkste van alle maatregelen die een smart city kan treffen. Ook al zijn smart cities voorzien van een sterke cybersecurity, kunnen kwaadwillende actoren alsnog binnendringen door menselijk falen. Het vergroten van dit bewust zijn bij de inwoners van smart cities kan worden ondernomen op twee manieren: via *cyberawareness* campagnes en trainingen of via *fear appeals*. De laatste van deze twee focust zich vooral op de negatieve kant van het gebruik van digitale applicaties, waarbij mensen door angst voor de eventuele risico's ontmoedigd worden deze te gebruiken. Bij *cyberawareness* campagnes en trainingen wordt dit gebruik gepromoot en worden mensen ingelicht over hoe zij om moeten gaan met cyberdreigingen. Deze maatregelen hebben beide als gevolg dat de menselijke bijdrage aan een beveiligingslek wordt gemitigeerd. Dit is ook het gebied waar men de meeste aspecten kan herleiden naar de netwerkmaatschappijtheorieën van Castells en Van Dijk. Beide beargumenteren zij de noodzaak dat inwoners van de huidige maatschappij moeten worden (her)opgeleid om zich zo goed mogelijk te kunnen aanpassen aan een met ICT geïntegreerde maatschappij. Dit is dan ook van groot belang indien de inwoners van smart cities willen meedraaien in de dagelijkse praktijken die zich binnen de stad afspelen.

Om de verschillende manieren van cybersecurity die hierboven zijn genoemd goed te kunnen implementeren in het huidige beleid van smart cities, moet het huidige beleidskader eerst worden aangescherpt. Het huidige beleidskader van de meeste steden in niet toereikend genoeg voor het inpassen van nieuwe technologische ontwikkelingen. Omdat institutionele paraatheid van groot belang is voor de soepele implementatie van cybersecuritybeleid, moeten wettelijke en regelgevende beperkingen worden weggenomen. Dit kan vaak alleen in samenwerking met nationale overheden, aangezien steden vaak gebonden zijn aan een nationaal beleid. Bij het wijzigen van het huidige beleidskader en de beleidsomgeving zullen veel uitdagingen komen kijken voor smart cities. Er moet onder andere rekeningen worden gehouden met normen en waarden en met het gedrag dat bepaalde inwoners als goed of vanzelfsprekend beschouwen. Zowel lokale als nationale overheden zullen in de komende jaren gedateerd beleid moeten aanpassen aan de nieuwe ontwikkelingen in de ICT. Zij moeten beleidsmakers in staat stellen een leidende rol aan te nemen bij integreren van nieuwe ideeën in oude beleidsstukken.

Overheden gaan vaak samenwerkingen aan met private partijen om zo het kennispotentieel te optimaliseren wanneer zij bezig zijn met het opstellen van nieuwe beleid. Deze private partijen zijn vaak vaste partners van overheden en oefenen geen invloed uit op de beslissingen die overheden maken bij het ondernemen van cybersecuritymaatregelen en het opstellen van beleid voor deze maatregelen. Wel proberen overheden een zo groot mogelijk publieke waarde te halen uit de verschillende samenwerkingen. De betrokkenheid van burgers is dan ook een fundamentele hoeksteen van *smart city governance*. De inwoners van smart cities moeten betrokken worden bij de besluitvorming van (lokale) overheden, omdat onder andere zij de gevolgen hiervan zullen ondervinden. Het toenadering zoeken naar zowel burgers als private partijen betekent dat smart cities optimaal kunnen handelen naar de uitkomsten van deze participatie en deze verworven kennis in acht kunnen nemen bij hun besluitvorming.

De gepercipieerde urgentie van de verbetering van cybersecurity staat volledig in zijn recht. Het behouden van de kwaliteit van de huidige cybersecurity en het verbeteren hiervan staat hoog op de agenda van de meeste smart cities. Omdat communicatie vaker via digitale kanalen verloopt, zien overheden in dat een adequate beveiliging van groot belang is. De kosten die hierbij komen kijken zijn vaak al opgenomen in deze nieuwe ontwikkelingen en zijn een integraal onderwerp van het terrein waarop deze ontwikkelingen plaatsvinden. Echter, in het kader van kostenreductie, worden ondersteunende ICT-processen door overheden uitbesteed aan externe actoren. Naast de kosten die komen kijken het opzetten van cybersecuritymaatregelen, krijgen smart cities ook te maken met kosten die veroorzaakt worden door schade van cyberaanvallen. Deze kosten kunnen vaak oplopen tot in de miljarden, omdat zij processen teweeg kunnen brengen die gevolgen hebben op zowel lokaal als globaal niveau.

Al met al lijkt het erop dat smart cities verschillende maatregelen kunnen toepassen om zichzelf goed te kunnen beveiligen tegen een wereld vol cyberdreigingen. Ook al zal cybersecurity nooit 100% bescherming bieden tegen deze dreigingen, moeten er wel concessies worden gemaakt in het belang van cybersecurity. Zowel ex ante als ex post zijn er meerdere mogelijkheden voor smart cities om zichzelf aan te passen aan cyberdreigingen en daarmee hun cybersecurity te waarborgen. Cybersecurity interventies spelen als ex ante maatregelen de belangrijkste rol in de hele opzet. Firewalls, end-to-end encryptie, virus- en malwarescanners en een sterke controle op wachtwoorden

en toegankelijkheden staan paraat om hun taak als eerste verdedigingslinie tegen cyberdreigingen uit te voeren. Door het toedoen van deze applicaties worden kwaadwillende actoren de toegang tot kritieke systemen en gevoelige informatie ontnomen. Daarachter, een netwerk wat sterk gecontroleerd wordt door monitoring en het proactief testen van eigen cybersecurity. Indien cybercriminelen de eerste lijn aan verdediging weten te omzeilen, worden ze alsnog gedetecteerd en in de gaten gehouden vanuit de controlekamer dankzij deze monitoring. Mocht de schade al zijn gedaan, kunnen er eveneens maatregelen genomen worden om dit in de toekomst te voorkomen. Ex post maatregelen, zoals het aanpassen van beleid en het simuleren van toekomstige gevaren en maatregelen, haken in op de situatie die zich voordoet na een cyberaanval. Beleid kan in samenwerking met private partijen en inwoners van smart cities worden aangepast om een grondwerk te leggen voor het soepel implementeren van applicaties die toegespitst zijn op de proberen die zich eerder hebben voorgedaan. Terwijl simulaties een basis creëren voor nieuwe ideeën en toepassingen die kunnen worden meegenomen in het beleid. Als allerlaatste, zijn er nog de menselijke maatregelen die zowel ex ante of ex post kunnen optreden, afhankelijk van de situatie waarin smart cities zich bevinden. *Cyberawareness* campagnes en –trainingen en *fear appeals* zijn maatregelen die kunnen zorgen voor een krachtig effect. Wanneer de inwoners van smart cities zich bewust zijn van complicaties rondom cyberdreigingen en –security, is het voor cybercriminelen een stuk moeilijker om toegang te verkrijgen tot het netwerk van de stad. Er kan dus worden gesteld dat een bewuste samenleving een veilige samenleving is in deze nieuwe netwerkmaatschappij.

5.1. Aanbevelingen

Naar aanleiding van dit onderzoek kan ik enkele aanbevelingen maker in het verder ontwikkelen van theorie over smart city cybersecurity. Deze scriptie heeft aangetoond dat er verder onderzoek nodig is naar de verschillende cyberdreigingen voor smart cities en de cybersecuritymogelijkheden van smart cities. Deze benadering zou het gebied van cybersecurity ten goede komen omdat de algemeen bruikbare kennis over de beveiliging van smart cities momenteel nog niet compleet is en sommige organisaties nog vaak afhankelijk zijn van onafhankelijke individuelen of private partijen voor vaardigheden en kennis op het gebied van cybersecurity. Voorgesteld wordt dat er een specifiek kader wordt ontwikkeld waarin smart cities mogelijke dreigingen boven het hoofd kan blijven en de mogelijkheden omtrent cybersecurity volledig worden verkend zonder de privacy, vrijheden en veiligheid van de burgers te schaden.

Een extra aanbeveling wordt voorgesteld met betrekking tot *cyberawareness*. Wanneer steden een hoger niveau van ICT-integratie bereiken, is het belangrijk dat inwoners zich volledig bewust zijn van de mogelijkheden en beperkingen die cyberdreigingen en cybersecurity met zich meebrengen. Een beleid waarin grootschalige campagnes rondom *cyberawareness* in zijn opgenomen, zou een vereiste moeten zijn voor iedere stad die zich bezighoudt met de transformatie naar een smart city.

Ook zou er onderzoek gedaan kunnen worden naar hoe steden en overheden op internationaal niveau samenwerken met anderen organisatie zoals de Europese Unie of de NAVO.

6. Discussie en reflectie

In dit laatste hoofdstuk komen er een aantal kanttekeningen voorbij die geplaatst kunnen worden bij dit onderzoek. Ten eerste kan men nadenken over de afbakening van dit onderzoek. In dit onderzoek is namelijk slecht alleen Den Haag geanalyseerd. Wanneer meerdere steden een intrede in dit onderzoek hadden gemaakt, zou er meer data en literatuur gevonden kunnen worden om de argumentatie uit het literatuuronderzoek kracht bij te zetten. Ondanks dat heeft Dan Haag laten zien dat het vele overeenkomsten heeft met de internationale gemeenschap van smart cities. Overal op de wereld hebben smart cities te maken met dezelfde problemen op het gebied van cybersecurity.

Wanneer er wordt gekeken naar de interviews die geanalyseerd zijn, valt er te zien dat de informatie uit de interviews een goede samenhang heeft met het literatuuronderzoek. Echter, was de informatie uit de interviews soms moeilijk in te passen in de literatuur, omdat de geïnterviewden soms in zekere zin verschillende visies hadden over bepaalde onderwerpen dan dat terugkwam in de literatuur. Hoewel hun antwoorden vaak samenhingen met wat er gezegd werd in wetenschappelijke artikelen, waren de antwoorden toegespitst op voorbeelden van eventuele situaties waardoor verbintenis tussen het transcript en de literatuur vaak lastig was te bewerkstelligen. Ook zijn deze interviews geïnterpreteerd door één persoon. Dit zou mogelijk een niet geheel objectief beeld kunnen vormen van wat de geïnterviewden hebben gezegd. Ook het aantal interviews dat is uitgevoerd voor dit onderzoek was niet groot, zoals al eerder vermeldt in de reflectie op de methodologie. Verder is er in dit onderzoek persoonlijk contact geweest met maar één expert op het gebied van de case. Ook dit geef een niet geheel objectief beeld van de daadwerkelijke situatie, ondanks dit interview is afgenomen met iemand die een hoge functie bekleed binnen de organisatie.

Het tijdsbestek waarin dit interview geschreven is heeft ook zijn rol gespeeld in de kwaliteit van dit onderzoek. Door het krappe tijdschema en de noodzaak van het volgen andere cursussen, heeft ervoor gezorgd dat er niet voldoende literatuuronderzoek gedaan kon worden en dat het aantal interviews niet groter is geworden dan drie. Desalniettemin heeft dit onderzoek mij de urgentie van kritisch kijken naar bepaalde situaties laten zien. Hiermee heb ik een poging gewaagd een holistische zo objectief mogelijke weergave van de werkelijkheid neer te zetten.

Referentiekader

Aarts, N. (2013). Communicatie in de netwerksamenleving. *APG Groep NV Jaarverslag 2013,* p. 41-65.

AIVD. (2018). *Jaarverslag 2017.* Den Haag, Nederland: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Amoroso, E. (2012). *Cyber Attacks: Protecting National Infrastructure.* Waltham, Verenigde Staten: Elsevier.

Ashmore, W. (2009). *Impact of Alleged Russian Cyber Attacks.* Leavenworth, Verenigde Staten: School of Advanced Military Studies.

Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J. & Weiss, J. (2012). *Cyber Security Policy Guidebook.* Hoboken, Verenigde Staten: John Wiley & Sons, Inc.

Bass, T. & Robichaux, R. (2002). Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. *2001 MILCOM Proceedings Communications for Netwerk-Centric Operations: Creating the Information Force.* Piscataway, Verenigde Staten: IEEE.

Beurden, H. van & Wamelink, R. (2017). *NL Smart City Strategie.* Den Haag, Nederland: Rehms Druck.

Bever, S. van. (2015). Oorlog voeren in de 21ste eeuw. *Koerier, vol. 5,* p. 2-16.

Borrett, M., Carter, R. & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider? *Journal of Business Continuity & Emergency Planning, vol. 7*(1), p. 163-171.

Brenner, N. & Theodore, N. (2002). *Spaces of Neo-liberalism.* Oxford, Verenigd Koninkrijk: Blackwell.

Brenner, N. & Theodore, N. (2002a). Cities and the Geographies of "Actually Existing Neoliberalism". *Antipode, vol. 34(*3), p. 349-379.

Bruin, H. de & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly, vol. 34*(1), p. 1-7.

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. (2003). *The economic cost of publicly announced information security breaches: empirical evidence from the stock market.* Verenigde Staten: University of Maryland.

Caragliu, A., Del Bo, C. & Nijkamp, P. (2011). Smart cities in Europe. *Journal of Urban Technology, vol. 18*(2), p. 65-82.

Caruson, K., MacManus, S. & McPhee, B. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Journal of Homeland Security and Emergency Management, vol. 9*(2), p. 1-22.

Cashell, B., Jackson, W., Jicklin, M. & Webel, B. (2004). *The Economic Impact of Cyber-Attacks.*

Castells, M. (2004). *The Network Society: A Cross-cultural Perspective*. Cornwall, Verenigd Koninkrijk: MPG Books.

Castelnovo, W., Misuraca, G. & Savoldelli, A. (2016). Smart Cities Governance: The Need for a Holistic Approach to Assessing Urban Participatory Policy Making. *Social Science Computer Review 2016, vol. 34*(6), p. 724-739.

Cerrudo, C. (2015). *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks.* Securing Smart Cities.

Cerrudo, C. (2018). *Cities Are Facing A Deluge Of Cyberattacks, And The Worst Is Yet To Come.* Forbes. Geraadpleegd op 17 juni 2018, van https://www.forbes.com/sites/forbestechcouncil/2018/04/18/cities-are-facing-a-deluge-of-cyberattacks-and-the-worst-is-yet-to-come/#21f35e362559

Coats, D. (2018). *Worldwide Threat Assessment of the US Intelligence Community*. Verenigde Staten: National Intelligence Agency.

Conklin, A. & White, G. (2006). e-Government and Cyber Security: The Role of Cyber Security Exercises. *Proceedings of the 39th Hawaii International Conference on System Sciences.* San Antonio, Verenigde Staten: Center for Infrastructure Assurance and Security.

Choo, K. (2011). The cyber threat landscape: Challengers and future research directions. *Computers & Security, vol. 30*(8), p. 719-731.

Church, W. (2000). Information Warfare. *International Review of the Red Cross, vol. 82,* p. 205-215.

CSO. (2017). *Cyber attacks cost U.S. enterprises $1.3 million on average in 2017.* Geraadpleegd op 4 juli 2018, van https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html

Daly, G. (2018). *Cutting the Cost of Public Sector Cybercrime in 2018.* Security Magazine. Geraadpleegd op 4 juli 2018, van https://www.securitymagazine.com/articles/88634-cutting-the-cost-of-public-sector-cybercrime-in-2018

Dijk, J. van. (2001). *De Netwerkmaatschappij, Sociale aspecten van nieuwe media.* Alphen a/d Rijn, Nederland: Samsom.

Dijk, J. van. (2001a). *Netwerken, het zenuwstelsel van onze maatschappij*. Rede uitgesproken bij de aanvaarding van het ambt van Hoogleraar Toegepaste Communicatiewetenschap, toegespitst op de Sociale Aspecten van de Informatiesamenleving op 1 november 2001. Enschede, Nederland: Universiteit Twente.

Eger, J. & Maggipinto, A. (2009). Technology as a Tool of Transformation: e-Cities and the Rule of Law. *Information Systems: People, Organizations, Institutions, and Technologies,* p. 23-30.

Elmaghraby, A. & Losavio, M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research, vol. 5*(4), p. 491-497.

Engelshoven, I. van. (2015). *Voortgangsrapportage Programma Smart City Den Haag.* Geraadpleegd op 10 mei 2018, van https://denhaag.raadsinformatie.nl/modules/13/overige_bestuurlijke_stukken/90973

Ernst & Young LLP. (2016). *Cyber Security: A necessary pillar of Smart Cities.* India.

Evans, M., Maglaras, L., Ying, H. & Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance. *Security and Communication Networks, vol. 9*(17), p. 4667-4679.

Fischer, C. (1992). *America Calling: A Social History of the Telephone to 1940*. Berkeley, Verenigde Staten: University of California Press.

Gallaher, M., Link, A. & Rowe, B. (2008). *Cyber Security, Economic Strategies and Public Policy Alternatives.* Cheltenham, Verenigd Koninkrijk: Edward Elgar.

Gandhi, R., Sharma, A., Mahoney, W., Zhu, Q. & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political. *IEEE Technology and Society Magazine, vol 30*(1), p. 28-38.

Gemeente Den Haag. (2014). *Coalitieakkoord 2014-2018: Vertrouwen op de Haagse Kracht.*

Gemeente Den Haag. (2017). *Living Lab Scheveningen.* Geraadpleegd op 15 augustus 2018, van https://futureproofthehague.com/projects/living-lab-scheveningen

Germain, J. (2008). *The Art of Cyber Warfare, Part 1: The Digital Battlefield.* TechNewsWorld. Geraadpleegd op 3 juli 2018, van https://www.technewsworld.com/rsstory/62779.html

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J. & Halderman, J. (2014). *Green Lights Forever: Analyzing the Security of Traffic Infrastructure.* Michigan, Verenigde Staten: University of Michigan.

Ghernouti-Hélie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture. *2010 International Conference on Availablity, Reliability and Security.* Piscataway, Verenigde Staten: IEEE.

Gregory, D. (2012). From a View to a Kill: Drones and Late Modern War. *Theory, Culture & Society, vol. 28*(7-8), p. 188-215.

Gupta, J., Bouvier, J. & Gordon, E. (2012). *Exploring new modality of public engagement. An evalution of digital gaming platforms on civic capacity and collective actions in the Boston public school district.* New York, Verenigde Staten: Public Agenda.

Harknett, R. & Stever, J. (2011). The New Policy World of Cybersecurity. *Public Administration Review, vol. 71*(3), p. 455-460.

Harrison, C. & Abbott, I. (2011). A Theory of Smart Cities. *Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences.* Verenigde Staten: IBM.

Hartley, J. (2005). Innovation in Governance and Public Services: Past and Present. *Public Money & Management, vol. 25*(1), p. 27-34.

Hollands, R. (2008). Will the real smart city please stand up? *City: analysis of urban trends, culture, theory, policy, action, vol. 12*(3), p. 303-320.

IBM. (2010). *Smarter thinking for a smarter planet.*

Jackson, C., Cowles, B. & Russell, S. (2017). Beyond the Beltway. The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science. *2017 NSF Cybersecurity Summit.* Bloomington, Verenigde Staten: Center for Applied Cybersecurity Research.

Janczewski, L. & Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism.* Hershey, Verenigde Staten: IGI Global.

Jennex, M. (2007). Cyber War Defense: Systems Development with Integrated Security. In: (L. Janczewski & A. Colarik. 2007) *Cyber Warfare and Cyber Terrorism*, p. 241-253. Hershey, Verenigde Staten: IGI Global.

Jin, J., Gubbi, J., Marusic, S. & Palaniswami, M. (2014). An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet of Things Journal, vol. 1*(2), p. 112-121.

Johnston, A. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly, vol 34*(3), p 549-566.

Kanter, R. & Litow, S. (2009). *Informed and Interconnected: A Manifesto for* Smarter *Cities.* Harvard Business School General Management Unit Working Paper No. 09-141.

Kim, S., Wang Q. & Ullrich, B. (2012). A Comparative Study of Cyberattacks. *Communications of the ACM, vol. 55*(3), p. 66-73.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington DC, Verenigde Staten: CSIS.

Lin, P., Swimmer, M., Urano, A., Hilt, S. & Vosseler, R. (2017). *Securing Smart Cities: Moving Toward Utopia with Security in Mind.* Tokio, Japan: Trendmicro.

Maher, M. & Smokvina, V. (2006). Digital to intelligent local government transition framework. *Proceedings of the 29th International Convention of MIPRO.* Opatija, Kroatië.

Mayer, M. (2007). Contesting the Neoliberalization of Urban Governance. In Leitner H., Peck, J. & Sheppard, E. (2007), *Contesting neoliberalism: Urban Frontiers* (p. 90-115). New York,
Verenigde Staten: The Guilford Press.

Mármol, F., Sorge, C., Ugus, O. & Pérez, G. (2012). Do not snoop my habits : preserving privacy in the smart grid. *IEEE Communications Magazine, vol. 50*(5), p. 166-172.

Marsteller, J., Jackson, C., Sons, S., Allar, J. Fleury, T. & Duda, P. (2014). *Guide to Developing Cybersecurity Programs for NSF Science and Engineer Projects.* Bloomington, Verenigde Staten: Center for Trustworthy Scientific Cyberinfrastructure.

Meulen, N. van der & Lodder, A. (2014). Cybersecurity. *Recht en Computer,* p. 301-318. Deventer, Nederland: Kluwer.

Ministerie van Justitie en Veiligheid. (2013). *Nationale Cybersecurity Strategie 2.* Den Haag, Nederland.

MIVD. (2017). *Jaarverslag 2017.* Den Haag, Nederland: Ministerie van Defensie.

Moore, M. (1995). *Creating Public Value: Strategic Management in Government.* Cambridge, Verenigd Koninkrijk: Harvard University Press.

Morren, J. & Slootweg, H. (2016). *Investments in Distribution Automation as a Foundation for Smart Grids.* Helsinki, Finland: CIRED.

NCSC. (2014). *Cybersecuritybeleid Nederland 4.* Den Haag, Nederland.

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

NOS. (2018). *Zware DDoS-aanvallen: wie, wat, waar en waarom?* Geraadpleegd op 12 augustus 2018, van https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html

OESO. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.*

Oosterveld, W. (2017). *Nederlandse steden willen steun kabinet voor gezamenlijke Smart City Strategie.* Platform31. Geraadpleegd op 10 mei 2018, van https://www.platform31.nl/nieuws/nederlandse-steden-willen-steun-kabinet-voor-gezamenlijke-smart-city-strategie

Pardo, T. & Taewoo, N. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th Annual international Conference on Digital Government Research,* p. 282-291. New York, Verenigde Staten: ACM.

Philips. (2018). *CityTouch. Light management system.* Geraadpleegd op 13 augustus 2018, van http://www.lighting.philips.com/main/systems/lighting-systems/citytouch

PWC. (2015). *Information Security Breaches Survey 2015.* Londen, Verenigd Koninkrijk: Cyber and Government Security Directorate.

Rashman, L. & Hartley, J. (2002). Leading and learing? Knowledge transfer in the Beacon Council Scheme. *Public Administration, vol 80,* p. 523-542.

Reddick, C. (2010). Homeland Security Preparedness and City Governments. In: (R. Kemp. 2010) *Homeland Security: Best Practices for Local Governments,* p. 85-102. Washington DC, Verenigde Staten: ICMA Press.

Reuters. (2015). *Cyber attack on U.S. power grid could cost economy $1 trillion: report.* Geraadpleegd op 4 juli 2018, van https://www.reuters.com/article/us-cyberattack-power-survey/cyber-attack-on-u-s-power-grid-could-cost-economy-1-trillion-report-idUSKCN0PI0XS20150708

Rocheleau, B. (2003). Politics, accountability, and government information systems. *Public Information Technology: Policy and Management Issues.* Hershey, Verenigde Staten: Idea Group Publishing.

Rowe, D., Lunt, B. & Ekstrom, J. (2011). The Role of Cyber-Security in Information Technology Education. *Proceedings of the 2011 conference on Information technology education,* p. 113-122. New York, Verenigde Staten: ISBN.

Sager, T. (2011). Neo-liberal urban planning policies: A literature survey 1990-2010. *Progress in Planning, vol. 76,* p. 147-199. Trondheim, Noorwegen: NTNU.

Scott, W. (2013). *Institutions and Organizations: Ideas, interests, and identities.* Thousand Oaks, Verenigde Staten: Sage Publications.

Shackelford, S., Proia, A., Martell, B. & Craig, A. (2015). Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. *Texas International Law Journal, vol 50*(2-3), p. 305-356.

Schjolberh, S. & Ghernouti-Hélie, S. (2011). *A Global Treaty on Cybersecurity and Cybercrime.* Oslo, Noorwegen: AIT Oslo.

Vattapparamban, I, Yurekli, A., Akkaya, K. & Uluağaç, S. (2016). Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety. *2016 International Wireless Communications and Mobile Computing Conference (IWCMC),* p. 216-221. Piscataway, Verenigde Staten: IEEE.

Verschuren, P. & Doorewaard, H. (2015). *Het ontwerpen van een onderzoek.* Den Haag, Nederland: Lemma.

Via Satellite. (2017). *Transportation Sector Not Taking Cyber Threat Seriously Enough.* Geraadpleegd op 4 juli 2018, van https://www.satellitetoday.com/telecom/2017/07/21/transportation-sector-not-taking-cyber-threat-seriously-enough/

Waltz, E. (1998). *Information Warfare: Principles and Operations.* Norwoord, Verenigde Staten: Artech House.

Bijlagen

Bijlage I. Transcript interview Marijn Fraanje - Chief Information Officer bij gemeente Den Haag

van Haaren: Goedemiddag. Als eerst wil ik u bedanken voor de tijd die u genomen heeft voor dit interview. Mijn naam is Kevin van Haaren, vierdejaars student Geografie, Planologie en Milieu aan de Radboud Universiteit hier in Nijmegen. Op het moment ben ik bezig met het schrijven van mijn scriptie. Hiervoor doe ik onderzoek naar de dreigingen op het gebied van cybersecurity die omtrent smart cities lopen. de bijbehorende beleidsveranderingen en de kosten die hierbij komen kijken. Het interview zal ongeveer een half uur tot een uur duren en zal dan ook worden opgenomen. Heeft u hier problemen mee?

Fraanje: Nee hoor, dat is prima.

H: De antwoorden die gegeven worden in het interview worden gebruikt in het onderzoek en zullen later ook online terug te vinden zijn, onder andere in de scriptiedatabank van de universiteit. Ik wil u vragen of u hiermee dan ook akkoord gaat.

F: Ja hoor, is goed. Wanneer wordt de scriptie openbaar?

H: De scriptie wordt openbaar nadat hij door de eerste corrector en tweede corrector is nagekeken en deze moet een voldoende is afgesloten, dan komt hij openbaar te staan. Dat zal eind augustus zijn.

F: Okee.

H: Aan het eind van het interview is er nog de mogelijkheid voor u om vragen aan mij te stellen. Dan zou ik u eerst willen vragen of u zich even kort kunt voorstellen.

F: Ik ben Marijn Fraanje en ik ben de Chief Information Officer van gemeente Den Haag. Nu bijna op de kop af twee jaar en daarvoor heb ik bijna tien en een half jaar gewerkt bij gemeente Amsterdam.

H: Welke studie heeft u hiervoor gedaan?

F: Planologie aan de universiteit van Amsterdam.

H: Welke functie heeft u gehad bij de gemeente Amsterdam voordat u hier kwam werken?

F: Ik ben daar begonnen als bestuursadviseur, dat heb ik vijf jaar gedaan. Dan vooral op de ruimtelijke dossiers, de bestuursvisie, AFAC Amsterdam, verkeer en vervoer, parkeerbeleid, dus eigenlijk vooral in de ruimtelijke sector. Daarna vijf jaar bij de ICT dienst, waarna ik eigenlijk als plaatsvervangende CIO hier naar toe ben gegaan.

H: U zei dat u uw huidige functie al twee jaar bekleedde bij de gemeente Den Haag. Heeft u in die tijd ook grotere problemen meegemaakt, sprongen die u moest overwinnen?

F: Ja, wat zijn grote problem? Echt grote problemen niet. Ik denk hetgene wat nog de meeste uitdaging gaat geven is de combinatie van de interne ICT kant, waar ik verantwoordelijk voor ben, met de smart city kant, waar ik sinds begin dit jaar verantwoordelijk voor ben.

H: Dat is dan intern, als binnen de gemeente Den Haag?

F: Ja, ja.

H: Komt er veel werk kijken bij die koppeling en wat voor een soort werk komt daarbij kijken?

F: Het speelveld is een andere. De interne kant gaat toch heel erg over circulaire applicaties en informatievoorzieningen die wij gebruiken en de ICT infrastructuur die daaronder zit en de manier waarop wij dat inzetten. Volgens primaire processen intern en onze dienstverlening naar buiten toe. En het smart city dossier zit hem toch meer in wat gaat de digitalisering en innovatie nou doen voor de stad zelf.

H: Okee. Om daarop in te spelen zou ik graag over willen gaan op Den Haag als stad zelf en de opkomst als smart city. Wat is volgens u de reden dat Den Haag zich wilt profileren als een smart city?

F: Ja, dat is eigenlijk een ingewikkelde. Ik zeg zelf altijd: welke stad is niet slim? Het is dus geen kwestie van Den Haag die zich specifiek wil profileren als een smart city. Ik vind smart city eigenlijk ook meer een mode woord voor zelfstandig nadenken over de innovatie ontwikkelingen van je stad in plaats van dat het nou ineens een hele andere realiteit is. Dat is iets wat elke stad natuurlijk wel probeert. Elke stad probeert wel na te denken over hoe organiseer ik mijn stad beter dan gister en dat is ook wel de reden dat we actief zijn op het smart city dossier.

H: Welke aspecten komen vooral naar voren bij Den Haag als smart city? Waar focust Den Haag zich vooral op?

F: Op een paar dingen. In het kader van de nationale smart city strategie zijn er vijf hoofdthema's benoemd, dat zijn: mobiliteit, circulaire economie, sustainability, dat zit hem een beetje in de duurzaamheidshoek, e-health en safety en security. Eigenlijk hebben de G5 steden toen besloten dat het thema's zijn die bij ieder spelen, maar gingen ze kijken of ze de onderwerpen onderling kunnen verdelen. Daarbij is het safety en security onderwerp bij Den Haag terecht gekomen en is afgesproken dat Den Haag samen met die steden, andere gemeenten en private partijen eigenlijk probeert een safety en security agenda op te stellen, die we dan weer gaan schakelen met de Rijksoverheid. En de andere onderwerpen zijn dan verdeeld onder de andere steden, dus e-mobility zit bij Eindhoven, e-health zit bij Utrecht, circulair bij Amsterdam en sustainability bij Rotterdam. En eigenlijk vervuld iedere gemeenten op dat onderwerp een soort boegbeeld rol. Het voorkomt dus dat we allemaal op dezelfde thema's lopen en dat we een helder kanaal hebben die in de lead is van het collectief.

H: Hoe is deze rol dan bij de gemeente Den Haag terecht gekomen?

F: Het heeft ook wel te maken met de karakter van de steden, daar hebben we ook naar gekeken. Den Haag is toch het regeringscentrum van het land. We hebben hier veel internationale instituten zitten, veel ambassades, het werkpaleis van de koning staat hier. We hebben de Tweede Kamer en de Eerste Kamer, dus we hebben hier vrij veel instituten zitten die potentieel toch een interessant doelwit zijn voor andere landen. Dat maakt dat veiligheid hier hoog in het vaandel staat en dat maakt het automatisch ook wel iets waar de stad toch wel extra op getriggerd is en dan niet alleen de stad zelf, maar ook heel veel partijen die hier in de stad zitten. We hebben TNO hier zitten, we hebben NATO zitten, de gerechtshoven en dat maakt dat het toch een beetje in het DNA van de stad zelf zit.

H: Okee. De stappen die Den Haag moeten nemen om hun rol te vervullen binnen de G5 aan steden. Welke stappen moet Den Haag nog nemen?

F: De eerste die eigenlijk belangrijk is en daar zitten we nu midden in, is het opstellen van een agenda. Daar zit wel een ingewikkeldheid in. Die agenda is niet een Den Haag agenda, maar het moet echt een agenda zijn waar alle elementen in zitten voor Nederland. Dus we zitten vooral in de rol dat we bij onze collega steden en andere partijen zoals de politie en Alliander en noem de partijen maar op aan het kijken zijn welke dingen zij aan die agenda willen koppelen en bijdragen, zodat er straks eigenlijk een goed samenhangend verhaal staat waarvan je zegt dat hier zitten de belangrijkste elementen voor de komende jaren wel in, in dit dossier. En dan is eigenlijk het meest ingewikkelde om alle puzzelstukjes bij elkaar te krijgen. Want het lijkt makkelijk, maar dat is het niet.

H: Naast dat jullie onderdeel zijn van de G5 binnen Nederland, zijn jullie internationaal ook onderdeel van de Resilient 100. Zijn daar ook nog bepaalde plannen of taken vanuit gekomen waar Den Haag zich voornamelijk mee bezighoudt?

F: We zitten nu eigenlijk in de agenda vormende fase daarvan en een van de onderwerpen is inderdaad ook cyber resilience. Dus dat matcht eigenlijk ook wel weer met het safety en security, met de cyberweerbaarheid van de stad.

H: Dus zowel op nationaal gebied als internationaal gebied houdt Den Haag zich bezig met de veiligheid op cyber gebied?

F: Ja, dat is één van de. Dat is inderdaad eentje die je op meerdere plekken terug ziet komen.

H: Los van deze veiligheidskwestie, wat voor een punten staan er voor de gemeente Den Haag nog meer hoog op de agenda voor de transformatie naar een smart city?

F: We zijn bezig met een project dat heet Living Lab Scheveningen. Wat we eigenlijk daarmee willen doen, is onderdeel van herstructurering van de boulevard van Scheveningen. Bij de vervangingen van de verlichtingen willen we eigenlijk een smart city netwerk aanleggen. Dus de insteek is dat er eigenlijk overal glasverbindingen komen en dat de lantaarnpalen als knooppunten fungeren voor allerlei digitale dienstverlening. Daaraan gekoppeld komt een open platform. Dus eigenlijk kun je allerlei toepassingen koppelen aan het open platform en is de insteek dat we daar eigenlijk een proeftuin maken van nieuwe smart city toepassingen. Kijken welke toepassingen we kunnen

koppelen en verbinden met elkaar. Dus eigenlijk een basis neerleggen voor de smart city ontwikkeling.

H: Zijn het allemaal openbaar toegankelijke smart toepassingen of is het meer intern voor de gemeenten zelf?

F: Het grappige is, het is een combinatie van alles. Voor een gedeelte zal het gemeentelijke dienstverlening zijn, maar als een collectief van burgers een goed idee heeft en daarvan gebruik willen maken, dan kan dat ook. Als bedrijven iets bedenken, dan kan dat ook. Dus het is wel de bedoeling dat het niet strikt voor de gemeente is of voor een of twee bedrijven of alleen burgers, maar echt een combinatie van.

H: Het moet dus iedereen ten goede komen eigenlijk?

F: Ja. Ik zeg eigenlijk altijd maar: eigenlijk leggen we een snelweg aan waarover iedereen moet kunnen rijden.

H: U had het net over burgers en eventueel bedrijven die zich daarin mengen. Zijn er ook bepaalde initiatieven waarmee de gemeente Den Haag samenwerkt die niet door de gemeente zelf is opgezet maar door de burgers of bedrijven?

F: Er gebeurt natuurlijk op zich altijd wel heel veel in de stad en dan is er de zoektocht van wanneer moet je je er mee bemoeien als overheid en wanneer moet je juist denken: weet je wat, het gaat juist zo goed omdat wij ons er niet mee bemoeien. Dus dat is altijd een beetje balanceren voor wat het wijst is, maar meestal zijn we daar wat terughoudend in tenzij de burgers ons actief opzoeken.

H: Dus ik neem aan dat wanneer de burgers jullie actief opzoeken, de gemeente Den Haag ook helpt bij het opstellen met plannen voor die burgers als zij een idee hebben?

F: Dat hangt er vanaf wat natuurlijk de vraag is. We hebben allerlei subsidieregelingen waar mensen een beroep op kunnen doen. Het kan inderdaad zijn voor hulp met kennis en expertise. Het zijn verschillende programma's en dingen die we hebben. We hebben het ook omgekeerd. We hebben een start-up Erasmus programma. Daar zetten we eigenlijk om het jaar een aantal vragen waar wij als stad voor staan eigenlijk open op de markt met het idee dat wie geïnteresseerd is zich kan inschrijven. Er zit wel een selectieproces aan vast en de partijen die geselecteerd worden mogen dan ook daadwerkelijk binnen de gemeente een toepassing ontwikkelen, ongeacht wat het is. Aan het einde van de rit hebben we nog een demo-day en kijken we of er toepassingen uitrollen waar we ook iets mee kunnen. Afhankelijk van of dat lukt of niet, kan een partij of een persoon die zich ingeschreven heeft dat product ook ontwikkelen of we zeggen: wat leuk geprobeerd, maar dat was het niet.

H: Op dit moment bestaat Den Haag als smart city uit een gemeente die smart city toepassingen invoert en de initiatieven waar we het over hadden. De integratie van ICT zal in de toekomst misschien worden geregeld door één orgaan. Denkt u dat dat hier in Nederland gaat gebeuren?

F: Ik denk niet dat dat gaat gebeuren.

H: Waarom denkt u dat?

F: Dat is het grappige, die digitalisering is zo hard gegaan dat het bij alles en iedereen zit. Dus het is niet meer toe te wijzen dat een partij in de regie is. Ik denk dat dat ook wel de zoektocht is voor zowel marktpartijen, als overheden, als kennisinstituten, dat als niemand er mee over gaat, hoe regelen we het dan op een manier waar we ons allemaal goed bij voelen? Je ziet het sterk terug in de ethische discussies, wat mag er wel of niet op het internet bijvoorbeeld. Dat is ook een dossier waar we vrij actief op zijn in Den Haag. Maar inderdaad ook de zoektocht naar hoe we ons tot elkaar moeten verhouden. Wat moeten we wel afspreken en wat niet? Dus ik geloof niet dat er opeens één entiteit komt die alles gaat beheersen en controleren.

H: Voor veel steden is het inrichten van stedelijke ruimte tegenwoordig voor marktgerichte economische groei. Het is vaak het belangrijkste doel geworden binnen een stad. Vind u dat dit ook van toepassing is op de stad Den Haag?

F: Het is terecht wat je zegt. Je ziet dat in veel steden terug en ik denk hier ook wel. Tegelijkertijd zie je dat het doel ook nog steeds is het leveren van een prettige publieke ruimte en het zo efficiënt en makkelijk mogelijk combineren van functies. Alle steden groeien. Alle steden proberen het toch binnenstedelijk op te lossen. Het is een extra druk op de bestaande verkeers- en vervoersstromen en op de openbare ruimte en hoeveelheid beschikbaar woningen. Dus daar ligt voor mij gevoel ook wel een deel van de vraagstukken voor smart cities. Hoe zorg je ervoor dat die stedelijke verdichting, die trouwens mondiaal is, toch op een goede manier kan verlopen?

H: Gaat dat op dit moment goed hand in hand, die toch nog blijvende economische groei en de goede inrichting van publieke ruimtes?

F: Daar is voor mijn gevoel niet één antwoord op te geven. Er zijn genoeg voorbeelden waar het prima samengaat en er zijn er waar je ziet dat het uit de bocht gevlogen is. Laat ik het zo zeggen: waar het bewust gecombineerd wordt zie je dat het prima samengaat. Waar je weinig rekenschap aangeeft, zie je toch wel het ene extreem ontstaan of het andere.

H: U had het net over publieke ruimtes en u had het al eerder over de plannen voor Scheveningen. Zijn er ook andere plannen hier in Den Haag om bepaalde publieke ruimtes te integreren met ICT?

F: De insteek van Scheveningen is wel dat als het proeflab slaagt, dat we dat dan stadsbreed kunnen uitrollen. Wat we nu wel aan het afwegen zijn, want we zitten nu eigenlijk in de planvormingsfase van Living Lab Scheveningen, zijn we nu aan het afwegen dat we meer kennis en expertise hebben op dit vlak en misschien moeten we maar eens kijken of op meerdere plekken tegelijk kunnen beginnen. Maar dan ook gecombineerd op de kansen die verschijnen op basis van de vervanging van de verlichting of omdat de weg opengebroken wordt. Dus we zijn een beetje zoekende naar een organische ontwikkelstrategie. Onze hoofdfocus blijft dan Scheveningen, maar we stappen ondertussen wel af van het idee dat het bij Scheveningen blijft.

H: Dus de plannen zijn er in het hoofd in ieder geval al wel om verder te gaan dan Scheveningen?

F: Ja.

H: Okee. Dan zal ik nu graag verder willen gaan op het gebied van cyberaanvallen waarmee de gemeente Den Haag te maken heeft. Heeft Den Haag op dit moment al veel te maken gehad met cyberaanvallen?

F: Ja, elke dag komen worden er zat pogingen gedaan om binnen te komen. Daar heeft elke partij last van. Maar hebben wij nou hele grote hacks gehad? Dat niet. Het wordt continu geprobeerd, maar dat geldt bijna voor elke organisatie. We hebben geen grote incidenten gehad.

H: Dus er is nog een grote schade aangericht?

F: Nee. We hebben geen Atlanta situatie hier. Kijk, wat wel grappig is. We hebben eind oktober vorig jaar op de laatste dag van de Cyber Security Week een ethische hacksessie gedaan met echte hackers. Dat was om te kijken wat er gebeurd als we een groep hackers los laten gaan op een live omgeving en niet een dummy omgeving. Hoe brengen we het daar vanaf? Dat is wel zodanig gegaan dat ik me eigenlijk geen beter resultaat had kunnen voorstellen. Dat is altijd wel even afwachten. Dat zijn de momenten waar je dan ook ineens, we hebben natuurlijk onze standaard test overeenkomst en dat doen we periodiek. Maar het maakt wel het verschil of je een partij hebt die dat structureel bij je test en probeert of dat je inderdaad een groep hackers hebt wiens hobby het is om te hacken en die dat dus proberen bij jou op de live omgeving. Zij vonden het leuk. Ze hebben me opgeroepen dat ze het graag volgend jaar nog een keer doen. Dus we zijn al bezig met de voorbereidingen voor de tweede ronde. Omgekeerd was het voor ons dan ook weer heel erg leerzaam om te zien hoe we het op dat vlak doen.

H: Het is inderdaad een interessante aanpak, omdat het waarschijnlijk andere dingen zijn waarmee je te maken krijgt dan met het bedrijf dat constant loopt te testen.

F: Het gebeurt op een andere manier. Dat is natuurlijk toch het verschil. Het zijn niet de standaard bedrijven die bij je proberen in te breken. Daar ga je in ieder geval niet vanuit. Het zijn voornamelijk alsnog die jongens en meisjes uit die hackcommunity die dat proberen en daarom was het grappig om dat een keer mee te maken. Wat ons betreft een blijvertje.

H: Ja, die hebben natuurlijk hun eigen manier om bepaalde dingen te omzeilen, die misschien niet gebruikt worden bij de constante tests.

F: Ja. En de zichtbaarheid was natuurlijk ook iets. We hebben het echt in het stadhuis gedaan, in het midden van de openbare ruimte. Mensen konden er ook omheen lopen en iedereen die werkt op het stadhuis dacht: hee wat gebeurt er nu? Dus ook voor de awareness en exposure van dit onderwerp was dit een hele goede.

H: Het was dus een goede reclame gemeente Den Haag natuurlijk. Bent u van mening dat de stad Den Haag zich op dit moment kwetsbaar opstelt voor cyberaanvallen na zo'n hackathon.

F: Ons beleid is om ons wel actief te laten testen. Of dat dat nou dit onderwerp is of we hebben recent dus de deadline voor de AVG gehad. Wij nodigen de autoriteit persoonsgegevens nu actief uit om te toetsen hoe we ervoor staan. Dat is ook wel een bewuste keuze, want op dat soort onderwerpen denk ik dat je er meer aan hebt om je proactief te laten toetsen en je zwakke plekken, als ze er zijn, te laten vinden. Ik zou maar zeggen het omgekeerde: we trekken de muur op en steken ons hoofd in het zand en we hopen dat het goed gaat. Tot we dan een keer in de krant lezen dat het niet goed gegaan is. Dus ik denk dat die aanpak je uiteindelijk veel meer oplevert, door juist die toetsing op te zoeken en partijen laten komen om te schieten, dan te denken we trekken de muur op en het komt vanzelf in orde. Niemand is 100% dicht.

H: Dus u bent eerder voor het preventief verdedigen tegen cyberaanvallen door een soort vaccinatie toepassen door mensen het te laten testen?

F: Ja, precies.

H: Zijn er bij de testen ook zwakke punten uitgekomen bij het smart grid in Den Haag? Wat zijn volgens u de zwakke punten die Den Haag op het momenten heeft op het gebied van cyberveiligheid?

F: Ik denk binnen de gemeente hebben we alles binnen het vizier en op orde en is onze monitoring vrij goed. Hetgene wat ik nog een uitdaging vind is alles wat er in de stad zit. Dan doel ik niet per se op alles van de gemeente, want daar zit ook wel de link met het regeringsprogramma. Stel ik pak een 3D model van Den Haag, waar zitten dan alle sensoren?

H: Dan inderdaad publieke sensoren, private sensoren

F: Ja, maar waar zitten ze? En zijn ze veilig?

H: Doet Den Haag daar ook iets aan? Houdt Den Haag surveys onder de bevolking en bedrijven waar die private sensoren dan zitten of toegangspunten tot?

F: Nee, ik ben nog een beetje aan het puzzelen naar de slimste manier om dat te doen. Kijk, digitaal is natuurlijk veel mogelijk en er is veel data bekend. Dus ik ben zelf nog een beetje aan het nadenken over wat de slimste manier is om dat in beeld te brengen. Dat is dus niet per se via een monitor, want ik denk eigenlijk dat je digitaal veel kan achterhalen.

H: Dus u bent van mening dat het wel moet gebeuren in principe?

F: Ik denk dat we er uiteindelijk niet aan kunnen ontkomen. Neem nou de monitoring van intern van de ICT. Dan hebben we natuurlijk monitoring van onze eigen websites, maar ook monitoring van gelieerde websites en of ze veilig zijn of niet. We hebben een eigen controlroom en daar zit één van die monitoren in. Dat is gedaan door een bedrijf uit The Hague Security Delta, een start-up. Die heeft dat ontwikkeld en dat gebruiken we. Daarmee zien wij de in Den Haag beheerde websites die zijn niet veilig en dan acteren wij daarop. Zoiets kan ik me ook best goed voorstellen voor de stad.

H: Het is inderdaad best wel een logische oplossing voor het vinden van die private sensoren en toegangspunten tot jullie netwerk.

F: Ja. Ik denk wat er wel onder zit is dat soort dingen nog een beetje open terrein zijn, het wordt een ruzie van wie het is. Het is een terrein waarop wij als gemeente traditioneel nog geen rol gespeeld hebben.

H: Dus het staat nog best wel in de kinderschoenen voor de gemeente Den Haag?

F: Ja. Je merkt wel dat mensen een beetje worstelen met het vraagstuk of wij wel onze stad cyber aware maken. Of het nou onze bevolking is, of het mkb bedrijfsleven dat we moeten helpen om weerbaarder te zijn. Maar hoe dan? En op welke manier? En wat is onze rol dan in dat open deel waar het niet duidelijk is wie er nou verantwoordelijk voor is. Dat is voor iedereen nog een zoektocht. Hoewel ik denk dat het toch gaat schuiven dat de gemeente een staande rol gaat pakken.

H: Okee. Dus u denkt niet dat een bepaalde bedrijvigheid zich op gaat focussen?

F: Dat kan. Maar dan is het nog steeds de vraag of ze zelfstandig doen of op verzoek van de gemeente.

H: Welke groepen zullen volgens u de meeste last ondervinden van een cyberaanval op Den Haag? Is dat de gemeente zelf, de bedrijven of zijn het de inwoners van de stad?

F: Dat hangt er natuurlijk vanaf op wie de aanval is gericht. Kijk, is de aanval gericht op de gemeente dan is in eerste instantie toch de gemeente en de gebruikers van onze dienstverlening diegene die er het meeste last van hebben. Is het gericht op een willekeurig bedrijf, dan is dat bedrijf natuurlijk als eerste de klos. Daar kun je eigenlijk niet met één antwoord invulling aan geven. Ik denk dat daar wel een punt zit. Uiteindelijk is iedereen potentieel doelwit en is het niet zo dat een bepaalde groep wel of niet aangevallen wordt.

H: Maar het kan dus wel zo zijn dat mocht de gemeente getroffen worden, dat er dan natuurlijk wel indirect gevolgen kunnen zijn voor inwoners en bedrijven?

F: Ja.

H: En heeft de gemeente daar ook een plan voor om dat te verhelpen? Om de schade die gedaan is te repareren.

F: We hebben natuurlijk voorzieningen staan. We hebben een back-up plan. Dus op zich voor de gemeentelijke kant hebben we het een en ander op de plank liggen. Dus op zich zit die kant wel goed. Ligt er nou een plan voor de hele stad? Stel er wordt een willekeurige partij in de stad hard geraakt, dan hebben wij geen back-up plan over hoe daar mee om te gaan. Elke partij heeft daarbij zijn eigen voorzieningen hoe daar mee om te gaan.

H: Het is dus meer een algemeen plan om bepaalde dingen te verhelpen dan een specifiek toegespitst plan voor bepaalde sectoren?

F: Ja. Dat is denk een worsteling voor alle sectoren zelf. Op beleidsniveau heb je natuurlijk wel de beleidslijn voor de kritische infrastructuur. Daar zit een aantal sectoren in die aan een aantal eisen moeten voldoen, omdat ze in de kritische infrastructuur sector zitten. Maar ook heel veel onderdelen niet. Ziekenhuizen zitten daar bijvoorbeeld los van. Die zitten niet in de kritische infrastructuur.

H: Zijn er wel een aantal systemen of sectoren die onderling in serie verbonden zijn binnen de kritische infrastructuur, dat wanneer de ene getroffen wordt de andere er ook last van heeft?

F: Het verschilt heel erg per sector. Er zijn inderdaad een aantal sectoren die onderling afspraken hebben en de bankensector om bij te springen als er echt iets mis is. Dus dat wisselt heel erg.

H: Dus het is niet per se zo dat dat soort systemen in parallel worden gezet om eventuele schade doorlopend naar elkaar te voorkomen?

F: Nee.

H: Dan zou ik het nu graag willen hebben over de maatregelen die Den Haag treft tegen cyberaanvallen. En dat te beginnen bij wat voor een vormen van cybersecurity Den Haag gebruikt om cyberaanvallen tegen te gaan. In wat voor een plekken zijn jullie actief om die cybersecurity toe te passen? Gebeurt het voornamelijk ex post of ex ante?

F: Ja, eigenlijk allebei. We hebben vrij actieve monitoring voor verschillende vlakken, of het nou de website is of het netwerkverkeer. Dat is een kant. Dat hebben we echt geconsolideerd in de controlroom. Die hebben we intern ook staan bij elkaar. En daarnaast hebben wij ook nog een 24/7 verbinding met de monitoring van Fox-IT. Dus dat staat weer bij hen. Ja, en daarnaast zijn er heel veel verschillende vormen die wij toepassen. Bij nieuwe applicaties gewoon uitgebreid testen van de oplossingen of ze veilig zijn of niet. De ethische hacksessie noemde ik al. Dat is proactief schieten. We steken ook heel veel tijd en energie in awareness. Dat is toch de menselijke kant van het verhaal. We hebben begin dit jaar een kleine app game ontwikkeld die je op je telefoon kan doen. Het was een combinatie van informatiebeveiliging en privacy. Nou, dat is eigenlijk best goed gegaan. De eerste ronde zat er al 1000 man op van de 8000, dus dat is dan toch verrassend hoeveel animo dat krijgt. Dus ja, dat zijn andere vormen.

H: Dus de cyber awareness wordt wel goed ontvangen binnen Den Haag?

F: Ja. Met zo'n app game is het natuurlijk wel even wachten wat de response is. Maar toen we de 1000 passeerde, hadden we toch even van dit is wel een hele grote groep. Maar dat is me positief meegevallen. Voor de rest doen we ook aan privacy spreekuren en informatiebeveiligings spreekuren. Dus daar kunnen mensen die eigenlijk vragen hebben op dat gebied terecht. Je hebt natuurlijk de functionele mailboxen van de CISO en de functionaris gegevensbescherming. Dus ja, we hebben eigenlijk van alles.

H: Okee, en bent u van mening dat Den Haag zich op dit moment goed kan verweren tegen cyberaanvallen?

F: Ja, ik denk dat we eigenlijk best wel veel op de rit hebben staan.

H: En op welke manier gebeurt dit?
F: Ik denk op verschillende manieren. We hebben sowieso een goed beeld van onze kritische systemen. We hebben een goed draaiend icms, waarin onze - wat we zo mooi noemen - kroonjuwelen instaan inclusief alle mitigerende maatregelen om de risico's af te dekken. We hebben goede monitoring en we hebben vrij goede response. Dus op het moment dat er wat is, zit er al vrij snel iemand bovenop.

H: En mocht één van deze verweringen uitvallen? Zal dat grote problemen met zich meebrengen of?

F: Nee, gelukkig hebben we… het is niet één muur waar je doorheen moet. Dus we hebben wel verschillende verdedigingslinies staan.

H: Zijn er bepaalde systemen binnen de kritische infrastructuur waar Den Haag zich voornamelijk op focust rond cybersecurity of wordt het verspreid over alle systemen?

F: Nee, de meeste dingen hebben we voor het geheel staan. En dan is het wel zo dat we bij de kritische systemen nog meer maatregelen hebben.

H: Kunt u iets meer vertellen over deze aanvullende maatregelen?

F: Dat kan ik niet doen. Dat zul je begrijpen.

H: We hadden het net al over de ex ante en ex post maatregelen. Zijn er ook echt bepaalde projecten waarbij een focus ligt op ex ante of ex post? U zei al er wordt naar beide gekeken, maar zijn er ook projecten die zich toespitsen op één van beide?

F: Ja, dat zijn de meeste componenten die wij implementeren. Dan zitten ze op de een of de andere kant. Dus of het nou op het gebied van de firewall zit of op de extra maatregelen in het kader van… nou, we zijn op dit moment bezig met cloud gang, die daaraan gekoppeld zitten. Maar dat zijn dus specifieke componenten die op de een of de ander zitten.

H: Hoe kan volgens u de kwetsbaarheid van Den Haag op het gebied van cybersecurity het best worden aangepakt op dit moment?

F: Lastige vraag. De reden waarom die lastig is… kijk, er is altijd wel een bepaalde balans die werkbaar is. Dus op een gegeven moment heb je je verdedigingslinie staan en dan voegt het ook niks meer toe om er nog een muur voor te zetten en nog een muur voor te zetten. Dus er zit wel altijd een bepaalde mate in als je dit allemaal hebt staan, hoeveel ga je er nog bovenop gooien? En ik denk dat het hem toch altijd zit in waar je altijd intensief mee bezig bent is die awareness. Die is gewoon cruciaal. De meeste manier waarop mensen toch binnen komen is door de persoonlijke fout van

iemand die op een link klikt en dan kan alles worden gepasseerd. Ja, en het proactief blijven toetsen van je verdediging.

H: Dus u denkt dat vooral de maatregelen voor de ontwikkelingen die nog zullen komen hand in hand gaan met de ontwikkelingen binnen de ICT?

F: Ja.

H: Dus mochten er nieuwe dreigingen komen, dan zal de gemeente Den Haag zich daarop aanpassen?

F: Ja, klopt.

H: Okee. Wordt er dan ook veel gedaan aan het beschermen van die individuen tegen cyberdreigingen en informatiediefstal binnen de gemeente Den Haag?

F: Ja. Dit gebeurt heel expliciet in awareness campagnes, omdat het toch elke keer weer de grootste bron is van een beveiligingslek.

H: Het gaat dus echt om de mensen zelf dan?

F: Ja, ja.

H: Maar er wordt dus niks door de gemeente Den Haag gedaan op het gebied van fysieke verdediging? Laten we zeggen dat er bepaalde systemen worden geïnstalleerd om bepaalde connectiviteit uit te sluiten of juist te promoten.

F: Ik snap wat je zegt. Nou, we monitoren dus wel heel actief het verkeerd. Dus elke keer als we zien dat het bij iemand door het dak heen gaat, dan zetten we diegene wel altijd even preventief dicht. Dus dat soort dingen worden wel bijgehouden. Dat is meestal naderhand er iets mis is dan ervoor.

H: U zei net al dat de gemeente Den Haag ook samenwerkt met andere bedrijven en instanties om Den Haag weerbaar te maken tegen cyberaanvallen. Wat voor een soort bedrijven zijn dit en wat voor een soort samenwerkingen zijn dit?

F: Den Haag vanuit economisch perspectief is de oprichting geweest van The Hague Security Delta. Dat is eigenlijk een organisatie die een soort broedplaats moet zijn voor cybersecurity start-ups. Daar is dus eigenlijk een hele community ontstaan van kleine bedrijfjes samen met grote bedrijven. En dat maakt eigenlijk dat het binnen Europa eigenlijk een van de grootste cybersecurity hubs is op dit vlak, dus daar maak je dan ook gebruik van. Van mijn collega's van de economische kant hoor ik wel eens: hey wat een interessant bedrijfje, leuk nieuw product, is het iets voor jou? Dus ik shop daar inderdaad wel eens met het idee wat heeft men daar weer bedacht, kan ik er wat mee?

H: Komen er nou veel verschillende soorten start-ups en innovaties vanuit The Hague Security Delta?

F: Ja, maar waarbij ze niet allemaal toepasbaar zijn voor de gemeente. Om de zoveel tijd zijn er een paar interessant, dus dan vraag ik die of ze hier willen komen pitchen. Dan merk je gemiddeld toch wel dat een idee briljant kan zijn, maar bij wijze van spreken meer wat voor het leger dan voor mij. Daar kan ik dan niet zo veel mee. En een andere idee, daar denk ik dan weer hier kan ik niks mee. Maar meestal zit er eentje tussen die de moeite waard is om te proberen.

H: Het moet natuurlijk wel toepasbaar zijn op de stedelijke omgeving.

F: Ja, en het moet matchen met de mate van dreigingen die je hebt. De eisen die het leger stelt zijn weer hele andere dan die ik stel.

H: Welke invloed oefenen deze externe actoren uit op de keuzes die de gemeente Den Haag maakt op het gebied van cybersecurity?

F: Ja, op die keuzes eigenlijk niet zo. Het is hoogstens dat het mij triggerd tot meer opties dan die ik zelf bedacht had. Dus ik zie het meer als een middel om te kijken wat er overal te vinden is en wat interessant is en wat niet.

H: Dus het is niet zo dat bepaalde bedrijven een monopolie opbouwen door te zeggen: wanneer u bent ons in dienst gaat, bent u ook verplicht om met deze andere actor in dienst te gaan?

F: Nee. Daar doen we niet aan.

H: Dus gemeente Den Haag heeft dus een eigen vrije keuze met waar voor een actoren zij een samenwerking mee aangaan?

F: Ja. Dat gaat voor alle terreinen op. Niet eens alleen voor deze.

H: Bent u van mening dat steden die veel met externe actoren samenwerkingen aangaan en zich laten beïnvloeden, ook de regie uit handen geven?

F: Nou, het hangt er vanaf in welke mate ze dit doen. Het moet altijd praktisch zijn, dus op het moment dat het je helpt een oplossing voor je probleem te vinden is prima. Maar het kan niet waar wezen dat je alles maar buiten de deur legt en dat het dan goed gaat. Dus je moet per casus bekijken wat verstandig is. Uiteindelijk blijf je wel zelf aan het roer zitten voor welke vragen heb je. Op het moment dat je dat buiten de deur zet, heb je toch wel een probleem.

H: Dus als ik het goed begrijp zal Den Haag altijd de regie in handen houden, maar wel taken delegeren naar andere instanties en bedrijven in bepaalde situaties?

F: Ja. Het kan zijn dat we bedrijven vragen gewoon eens te schieten op ideeën die je hebt, maar je moet die keuze natuurlijk wel zelf houden.

H: Dan zou ik het nu graag willen hebben over de implementatie van cybersecuritybeleid voor zowel Den Haag als Nederland. Bent u van mening dat op dit moment het beleidskader van de gemeente Den Haag toereikend genoeg is om de problemen omtrent cybersecurity goed op te kunnen lossen?

F: Ja. Met de kanttekening papier is geduldig. Op papier kun je alles heel leuk opschrijven, maar het gaat uiteindelijk toch om hoe je het uitvoert.

H: Dus er zijn geen bepaalde blokkades vanuit het gemeentelijk beleid dat al opgesteld is, om een eventueel nieuw beleid op te stellen?

F: Nee. Kijk, alle gemeenten hebben zich gecommitteerd aan de baseline informatiebeveiliging gemeenten, dus de BIG. Die is dus voor ons ook uitgangspunt voor ons informatiebeveiligingsbeleid en dat geldt voor alle gemeenten. Dat is weer gebaseerd op de BIR, die is van het Rijk. En die is praktisch gezien hetzelfde als de BIG, maar dan toegepast op de situatie van het Rijk. Dus wat dat betreft is het vrij consistent hoe gemeenten en het Rijk omgaan met informatiebeveiliging. Waar je de verschillen ziet in de manier waarop ze het in de praktijk doen.

H: En binnen het huidig cybersecuritybeleid van de gemeente Den Haag, denkt u dat hier nog wel een bepaalde uitbreiding mogelijk is?

F: Ik denk dat het vraagstuk zit op het punt wat ik al eerder noemde: hoe gaan we om met informatiebeveiliging in de publieke ruimte? Niet zozeer binnen de gemeentelijke context, maar binnen de stad. En wat voor een rol vinden wij dat wij als overheid erin moeten spelen.

H: Dus daar kan nog eventueel op worden uitgebreid?

F: Ja, daar zie je of het nou standaarden zijn rondom sensoren of het internet of things en hoe gaan we daar mee om en wat vinden we daarvan? Dat is toch voor mij het vraagstuk waar het minst van uitgewerkt is, omdat iedereen er in zit en niemand.

H: Dus de gemeente kan qua beleid uitbreiden op het gebied van de publieke ruimte. Mocht dit gebeuren, zijn jullie dan van plan om de inwoners en de bedrijven er meteen bij te betrekken of om eerst vanuit de gemeente Den Haag te bekijken wat er mogelijk is op dat gebied?

F: Uiteindelijk beide. Een gesprek voeren zonder dat je iets hebt staan, dat werkt ook niet. Dus je zal iets moeten hebben. Er zijn heel veel wegen naar Rome. We hebben natuurlijk ook de NEN. Die hebben allerlei standaarden op dit vlak. Dus dat is een route die je kan bewandelen. We werken ook veel samen in VEG verband, dus dat is een route. Zo zijn er wel meerdere partijen met wie we dit zouden kunnen bespreken en zouden doen.

H: Er zijn natuurlijk meerdere bedrijven die zich specialiseren op het gebied van cybersecurity, zoals Ernst & Young. Werkt gemeente Den Haag daar ook mee samen om eventueel tot een beter of nieuw beleid te komen of komt het puur uit de beleidsmakers van de gemeente Den Haag zelf?

F: Het komt toch voornamelijk uit de beleidsmakers van de gemeente zelf.

H: Wordt er eventueel ooit een samenwerking aangegaan?

F: Ja, hoor. Het gebeurt wel, maar je merkt wel dat het eerste initiatief vanuit de eigen organisatie is.

H: En komt dit dan doordat de organisatie zelf het best weet wat de problemen zijn en hoe deze kunnen worden opgelost?

F: Ja.

H: Het feit dat er zo min mogelijk naar externe actoren geweken wordt, is omdat de gemeente zelf al de expertise bezit en eventueel dus ook weet wat de beste oplossing is.

F: Ja.

H: Okee. Dan zijn we bij het laatste kopje aangekomen. De urgentie en kosten die komen kijken bij de cybersecurity. Hoe hoog staat op dit moment het verbeteren van de cybersecurity op de algemene agenda van de gemeente Den Haag?

F: Ja, hoog en eigenlijk ook wel op verschillende manieren. Dus als ontwikkeling van de economische sector in de stad staat hij vrij hoog. Maar ook om het niveau wat we nou hebben vast te houden en waar mogelijk nog verder te verbeteren. Dus hij staat er eigenlijk op twee manieren in.

H: Is het zo dat andere sectoren of posten worden gedrukt ten behoeve van de verbetering van cybersecurity of is het een kwestie van nieuw budget zoeken om die verbeteringen door te voeren?

F: Nee, het zit meestal mee in nieuwe ontwikkelingen, dus niet als iets separaats. Meestal zijn ze integraal onderwerp van het terrein waar nu ontwikkelingen op zijn.

H: Bent u wel van mening dat ondanks het niet separaat gebeurt, de gemeente wel voldoende investeert in cybersecurity?

F: Ja.

H: Dus volgens u hoeft er binnen de gemeente Den Haag niet meer geld terecht te komen bij cybersecurity, omdat daar al genoeg in geïnvesteerd wordt. Zijn er wel categorieën binnen de cybersecurity waar beter in geïnvesteerd kan worden, vanuit het eigen potje?

F: Niet met subsidiële bedragen, maar dat komt omdat het op dit moment best goed is. Er zitten geen enorme achterstanden om op te krikken.

H: U zei net al dat de gemeente Den Haag voldoende investeert in cybersecurity. Zou er meer mogelijk zijn met een groter budget of is het plafond al bereikt?

F: Het is relatief. Op een gegeven moment… zoals ik al eerder zei: hoeveel muren en slotgrachten wil je om je huis hebben. Hoe effectief is de extra investering die je doet dan nog?

H: Het opzetten van cybersecurity komt dus eigenlijk op hetzelfde neer als bij het budget. Er wordt gewoon al genoeg in geïnvesteerd.

F: Nee, ik heb geen miljoenen liggen bij het stadsbestuur van dat we onder water staan en ik heb dringend geld nodig voor cybersecurity.

H: Okee. Dan is dit het einde van het interview. Dan wil ik u graag bedanken voor uw tijd.

F: Graag gedaan.

H: Heeft u zelf nog enige vragen omtrent dit interview of het onderzoek dat ik uitvoer?

F: Nee.

H: Okee. Dan zou ik graag nogmaals willen benadrukken dat de antwoorden gegeven in dit interview online komen te staan en dat het gedeeld zal worden met de eerste en tweede corrector van mijn scriptie. Ook is er eventueel de mogelijkheid dit onderzoek te ontvangen nadat het is afgerond. Heeft u hier interesse in?

F: Ja.

H: Dan nogmaals bedankt voor het maken van tijd en het helpen bij het interview. Prettige dag verder nog.

F: Graag gedaan.

Bijlage II. Transcript interview Wessel Sluis - Algemeen directeur bij SIM-CI

van Haaren: Goedemiddag, goedemorgen trouwens.

Sluis: Jij ook nog.

H: Als eerst wil ik u bedanken dat u de tijd heeft genomen voor dit interview. Mijn naam is Kevin van Haaren, vierdejaars student geografie, planologie en milieu aan de Radboud universiteit in Nijmegen. Op het moment ben ik bezig met het schrijven van mijn scriptie. Hiervoor doe ik onderzoek naar de dreiging op het gebied van cybersecurity omtrent smart cities, de bijbehorende beleidsveranderingen en de kosten die hierbij komen kijken.

S: Ja.

H: Het interview zal ongeveer een half uur tot een uur duren en zal ook worden opgenomen. De vragen die u geeft zullen in dit interview gebruikt worden voor het onderzoek en zullen ook later onder anderen online terug te vinden zijn in de scriptiedatabank van de Radboud Universiteit. Ik wil u dan ook vragen of u hiermee akkoord gaat.

S: Ja, dat zeker.

H: Mooi. En aan het eind van het interview is natuurlijk nog voor u de kans om mij vragen te stellen eventueel. Ik zou graag willen beginnen met de vraag of dat u zich even kort kunt voorstellen.

S: Ik ben Wessel Sluis en ben sinds begin dit jaar werkzaam als inmiddels als algemeen directeur, ik ben begonnen als service delivery manager bij SIM-CI. Wat wij doen? Wij maken simulatiesoftware om kritische systemen, of kritische infrastructuren, daar staat SIM-CI ook voor, Simulating Critical Infrastructures, te kijken hoe weerbaar die zijn door diverse invloeden van buitenaf. Dat kunnen dus weersklimatologische of geografische invloeden zijn, maar het kunnen dus ook invloeden zijn zoals cyber hacks.

H: Okee, en van welke studie heeft u mogen genieten voordat u aan de slag ging?

S: Ik heb bachelor werkbouwtuigkunde en master studie industrieel ontwerp in de TU Delft gedaan.

H: Okee en heeft u het idee dat die opleidingen van toepassing zijn op de baan die u nu doet?

S: Inmiddels doe ik eigenlijk altijd wel een beetje hetzelfde. Ik denk vanuit design thinking achtige theorie. Design thinking is pas denk ik jaar of tien, twaalf een term die genoemd wordt maar het slaat heel erg aan bij industrieel ontwerpen. Waar het om gaat is dat het vanuit een empathie en een diep inlevingsvermogen van naar de klant eerst gaat verzamelen wat nou het probleem is voor de klant en van daaruit gaat ontwerpen. Er zijn eigenlijk altijd verschillende fases in, namelijk het divergeren en het configureren. In het divergeren ben je dus eigenlijk heel erg vrij in en open voor nieuwe ideeën en invloeden. Met configureren probeer je op basis van criteria die je eerst hebt verzameld een selectie te maken en zo uiteindelijk to narrow the solution down.

H: Okee, en heeft u hiervoor ook andere functies mogen bekleden voor u hieruit kwam?

S: Het begon echt als product ontwerper. Daarna heb ik als business developer en innovatie consultant hele tijd in de energiemarkt gewerkt. Vandaar ook op geven moment Software ervaring opgedaan. Tot mijn opleiding deden alleen maar fysieke producten en geen software. Maar toen heb ik softwareproducten ontworpen, want schermen kan je eventueel ook vormgeven. Ik ben een tijdlang commercieel directeur bij een groot constructiebedrijf geweest en daarna hier aangetreden

H: Dat is een hele interessante loopbaan. Zou ik nu graag willen beginnen met het te hebben over smart cities en de opkomst hiervan. Wat is volgens u de reden dat steden zich eventueel willen profileren als smart cities?

S: Ik denk, smart cities is een middel en geen doel. Maar een stad, is een plaats die onderdak wil bieden aan burgers die daar behoefte kunnen vervullen. Daarom woon je in een stad, veiliger en kan je makkelijker dingen uitwisselen. Er zijn allerlei voordelen van die stad. Er zijn ook een aantal nadelen. Dat is namelijk dat je hebt, gedeelde infrastructuur, gedeelde mogelijkheden, je hebt alles zo aangelegd dat het voor veel ongemak gaat zorgen als je weer infrastructuur moet blootleggen of andere zaken moet opzetten. Dus dat heeft ook weer een keerzijde die stad. Een smart city is in mijn beleving net zoiets als het plein, een ander organisme wat leert samenwerken op een heel klein stukje grond met beperkte middelen. Dat doe je dan op een handige manier. In een smart city maken mensen gebruik van elkaars auto of elkaars zaken. Een auto die, ik heb nog steeds op ouderwetse manier een auto. Mijn auto die staat thuis niks te doen. Die zou eigenlijk de hele dag voor andere mensen ingezet kunnen worden. En die is misschien dan ook op binnen twee jaar. Maar goed, dan heb je een betere cyclus, en zo zouden we veel efficiënter met elkaar middelen om kunnen gaan. En dat is waarom smart city denk ik een concept voor de toekomst is, het is een beetje een buzzword geworden.

H: Okee, u denkt dat eventueel wel de nadelen die u al benoemd heeft opgelost zullen worden door het concept smart city te gaan omarmen?

S: Ja, we zullen dat wel moeten denk ik. Want mensen zijn ook dingen die, een organisme die stoffen in zich opnemen, consumeren en uit elkaar uitscheiden. We beginnen een beetje aan de limieten van deze planeet te komen. Dat wij niet meer voor iedereen dezelfde plek hebben. Vroeger kon je gewoon een enorme boerderij ergens aanleggen. Als je niet genoeg grond had dan nog een stuk grond erbij en dat kon je verbouwen. Tegenwoordig zullen we dat efficiënter met elkaar moeten doen.

H: In principe is het gewoon een kwestie van grondstoffen of in ieder geval ruw gezegd, die we hebben, delen met elkaar?

S: Ja, en zorgen dat we de grondstoffen ook op een goede manier weer kunnen terugbrengen in de cyclus.

H: Welke aspecten profileren als een stad zelfs als smart city. Wat maakt volgens u een smart city?

S: Smart city, er zijn een aantal mensen die daarover nagedacht hebben. Je hebt dan die zestien duurzaamheidsdoelstellingen van de Verenigde Naties. Je hebt dan de vertalingen in zeven of negen concepten die de resilient cities hebben bedacht. Dat zijn altijd van die top aspecten. Ik denk dat waar je kort cyclisch gaat meten en acteren op uiteindelijk wat die metingen voortbrengt, daarop gaat reageren. En dan bedoel ik kort cyclisch als in dat je niet één keer per jaar je afvalstoffen betaalt, maar dat je gewoon bijvoorbeeld per vuilniszak die je wegbrengt of per toiletspoeling die je doorgespoeld, dat je daar op basis van betaald. Als jij, dat jij vijf keer per dag doorspoelt en je buurman doet dat tien keer dat hij dat ook voelt, en merkt.

H: Dus dat mensen inderdaad belast worden voor de lasten die zij het milieu…

S: Maar evenzeer beloont, ook dat type gedrag gestuurd maar ook ondersteund wordt. Alleen sturing, dat gaat niet werken.

H: Dus hoe duurzamer de mensen handelt hoe meer mensen beloond worden, hoe minder belast wordt.

S: Bijvoorbeeld, kijk als jij een autofanaat bent en bijvoorbeeld in een zestien cilinder wil rijden. Waarom zou dat niet mogen. Op dit moment word je belast, bijvoorbeeld in de bijtelling maar ook via de auto en wegenbelasting op het gewicht van je auto, op de uitstoot die de auto veroorzaakt, dat soort dingen. Terwijl misschien, je als autofanaat rij je maar twee keer per jaar in dat ding. Het is zelfs best wel aannemelijk want het zijn vaak rijke mensen die dit soort auto's hebben en die rijden er niet zo ontzettend vaak in. Dus is de werkelijke belasting van die auto niet eens zo hoog. Het is misschien zelfs lager dan iemand die in een Toyota Prius met allerlei voordelen krijgt.

H: Dat is inderdaad een manier om naar te kijken.

S: En dat is natuurlijk smart. En dat heeft ook te maken met al die bandbreedte die de oplossing met internet, met je huisaansluiting, het elektriciteitsnet en het gasnet zijn overgegaan van een gebruik gerelateerd tarief naar een capaciteitstarief. Ze zeggen gewoon je aansluiting is zo groot, daar betaal je gewoon altijd hetzelfde bedrag voor. Ik zou zeggen als ik mijn aansluiting dus nauwelijks belast, waarom zou ik daar geen voordeel op kunnen geven want dat betekent dat iemand anders er wel meer op kan zetten.

H: Klopt. Het is zo dat mensen die vaak op reis zijn, voor hun werk weg zijn, veel minder gebruik maken van energie of gas dan mensen die constant thuis zitten.

S: Ja, precies, terwijl die wel meer zouden mogen betalen voor hun vluchten.

H: Dat is inderdaad een mooie manier om naar te kijken. Welke stappen zouden volgens u moeten ondernomen worden voor z'n transformatie naar een smart city. Waar moeten steden vooral rekening mee houden in in die transformatie?

S: Ik denk, er is dus een stukje nationaal beleid, een stukje gemeentelijk beleid, een stukje bedrijfsleven, een beetje semioverheid. Dat zie je natuurlijk allemaal in die smart city achtige concepten. Je ziet dat een heleboel partijen zich rond de drinkplaatsen verzamelen om te kijken wat kunnen we hieruit halen. Wat kunnen we doen. Iedereen moet dit metertje installeren of dat doen, maar volgens mij moeten we met elkaar kaders scheppen. Waar ik echt in geloof. We hebben een economie gecreëerd met elkaar die gebaseerd is op het produceren van dingen die we willen en het negeren van dingen die we niet willen. Tot een grote schaal. Volgens mij is het enige wat ze zouden moeten doen, open nou die economie van de dingen die we niet willen, die op te ruimen. En stel dat je dus op basis van de daadwerkelijke CO^2 uitstoot afgerekend zou worden, dan zou je dus op je zestien cilinder nog wat auto welbeschouwd een CO^2 meter kunnen plaatsen, die letterlijk de CO^2 uitstoot meet en daar betaal je voor. En als je dat dus opent, dat je dan zegt, ik ga dus een economie maken die stof die je niet wil, CO^2, fijnstof. En daar gaan we voor betalen om het opruimen. Dan komen er zelf partijen die daar een oplossing voor maken. Nu zijn we met elkaar om elkaar heen aan het draaien, een smart city concept, een smart nog wat. Ik heb jarenlang in een smart grids werkgroepen gezeten en ook een smart energy collective. Het begon al tien jaar, twaalf jaar geleden om te praten met elkaar. Waarom moet het elektriciteitsnet slimmer worden.

H: Maar kan het bijvoorbeeld ook zijn dat deze veranderingen nog niet gebeuren omdat mensen nog niet genoeg bewust van zijn, dat de awareness er nog niet is. Of denk je dat de mensen die dat bewustzijn wel hebben alleen zich vast aan het oude systeem zoals nu is, want het zal allemaal wel, het loopt goed, klaar.

S: Het is hetzelfde met je gezondheid. Mensen gaan acteren op het moment dat ze werkelijk nadelig effect hebben. In het ziekenhuis zie je nog steeds mensen in een rolstoel zitten die zie je hier ook buiten zitten. Mens is best wel hardleers daarin. En je zal overtuigende voorbeelden moeten hebben. En daar bedoel ik dus het economische of het marktgerichte aspect. Ondernemers zijn altijd een beetje de pioniers geweest en de ontdekkingsreizigers. Ondernemers vroeger, de VOC, dat zie ik nu een beetje als de roofheren van toen, maar het waren de ondernemers van toen. Die pakte een boot, die gingen daarheen, die gingen stoffen handelen. Nou, dat vinden we nu allemaal verkeerd, dat begrijp ik, het is ook zo. Ons inzicht is gegroeid, maar het zijn over het algemeen altijd degenen die iets nieuws bedenken en dat andere door inspiratie te weten om te gooien dat iets nieuws ontstaat. Smartphones is een resultaat daarvan.

H: Dus de mensen die dingen aanpakken, die de ideeën naar voren brengen en eventueel dus andere mensen bewust van maken.

S: Je moet gewoon een klimaat hebben waarin ideeën ondersteund worden en waar ook met elkaar zeggen: dit is de kant die wel op willen.

H: Bij welke gebieden legt een bedrijf als SIM-CI de focus op om eerst te kijken naar smart cities, en dan vooral de kritische infrastructuren?

S: We kijken naar zowel de huidige als mogelijke toekomstige infrastructuren. Belangrijkste is wanneer je natuurlijk je telefoonverkeer, je dataverkeer, je gas, je elektriciteit en je water. En dan heb je water in twee vormen, het drinkwater. Als je het hebt over het daadwerkelijk bestaan van een

land of situatie in een stad, dan is drinkwater het allerbelangrijkste. Ze zeggen weleens, je kan drie dagen zonder water, drie minuutjes zonder lucht, maar je kan drieëndertig dagen zonder eten. Dus drinkwater, die infrastructuur, is gewoon heel belangrijk. Als we kijken naar de smart city, dan ga je dus dingen toevoegen. Je gaat namelijk meters toevoegen daar waar je het vroeger nog niet had. En waarom ga je ergens meten omdat je ergens wil bijsturen. Anders is het een loze meting. Je ziet dat er bedrijven zijn die daar al klein beetje op voorlopen, bijvoorbeeld in de industrie, daar zie je al heel veel initiatieven, zoals een Vopak of Shell. Die dus ook allemaal plaatsingen in hun installatie al metingen doorvoeren. Met het oogpunt om het hele proces efficiënter te maken. Waar Vopak bijvoorbeeld door filmpje, die hebben een drone, die onder dus de aanlegsteigers door foto's maakt van de hele installatie die al gescand worden zodat de hele installatie, de toestand, de kwaliteit daarvan, als voorbereiding op een project bijvoorbeeld om leidingwerk te vormen. Die doet dat dan. Dat zijn natuurlijk ook de middelen die we hier op een gegeven moment zullen moeten toestaan. Maarja, hier krijgen we natuurlijk, van ja een drone, dat je mag het boven je eigen terrein een drone laten vliegen. Of laten varen of dat soort zaken. Terwijl de staat de onderkant van een gebouw, de staat wil inspecteren met een drone, dan moeten ze eerst toestemming vragen. Dat zijn ook weer logisch dingen, ik zeg ook niet dat het verkeerd is, maar het zijn wel zaken waar we rekening mee moeten houden,

H: Dan kom je een beetje de kwestie van het gebruik van drones in openbare ruimtes en de privacy van andere mensen. Hebben jullie daar als SIM-CI veel mee te maken, dat jullie daar tegen aanlopen?

S: Nee, niet zozeer. Wij maken, op basis van gegevens maken wij een simulatie. Wij maken iets wat gebaseerd is op de werkelijkheid en daarin laten wij scenario's los om te kijken wat er dan gebeurt. Dus daar zijn wij, nee, wij zijn niet gelimiteerd door de werkelijkheid. Wij kunnen data uit de werkelijkheid gebruiken. We zijn ook niet gelimiteerd in onze fantasie en kunnen ook toekomstige situaties voorspellen. Bijvoorbeeld zeggen van we maken een assessment voor klanten tussen waar een brug wel of niet zou moeten te komen staan. Vanuit logistiek perspectief.

H: Is SIM-CI nauw betrokken bij de transformatie van steden naar smart cities in Nederland, en dan met name in Den Haag?

S: Ja, bij een aantal initiatieven zijn me aangesloten of worden we uitgenodigd. Wij zitten bij bij The Hague Security Delta. Wij zitten bij een aantal van die smart werkgroepen, wij bespreken ook weleens smart werkgroepen. Nogmaals, ik denk dat wij daarin eerder volgend zijn dan echt sturend.

H: Het is dus niet dat SIM-CI een bepaalde invloed uitoefent op de gemeenten, alleen, een adviesrol?

S: Wij helpen de beste beslissingen te maken.

H: Op dit moment bestaan smart cities eigenlijk meer uit losse initiatieven, in plaats van dat het echt gestuurd wordt door een bedrijf, een orgaan. Denk je dat het in de toekomst wel zo zal gebeuren of zal het voor altijd blijven dat meerdere initiatieven samen werken onder een bepaald orgaan, zoals de gemeente?

S: Dat vind ik lastig. Uiteindelijk moet er een bepaald speelveld zijn waarbinnen je kan opereren. Maar meestal ontstaat regelgeving natuurlijk pas nadat een technologie of ontwikkeling zich heeft ingezet. De regels voor het wegverkeer zijn naderhand bedacht. Niet eerst de auto bedacht, toen gingen alle verkeersregels, eerst een heel wetboek met waar je wel mocht staan en waar je niet mocht staan. Nee, het probleem ontstond door ongelukken. We moeten regels hebben voor de voertuigen, we moeten regels hebben van hoe je je gedraagt op de weg. Het is altijd een lastige. Met name nu in een tijd dat een technologie zich zo snel ontwikkeld. Je hebt gewoon de tijd niet meer. En je moet in twee/drie en soms zes jaar, moet je je technologie ontwikkelen en daarin een commercieel succes van maken en dan moet je alweer door ontwikkeld zijn.

H: Dus in principe is dit een soort van versnelt proces van trial and error waar de ICT nu tegenaan loopt eigenlijk?

S: Kijk, daar moet ook de ruimte voor zijn en dat je accepteert dat er geen perfecte producten meer zijn. Waardoor je gewoon elke keer toewerkt naar een nieuwe generatie. Daarmee moet je denk ik als gemeente, maar ook als eigenlijk degene die het belang heeft bij kritieke assets, moet je dat omarmen, en ook de producten en de partijen omarmen die dat kunnen. Daar zie je nog weleens dat er hele ingewikkelde aanbestedingsprocedures, allerlei ingewikkelde manieren worden gevonden om dus een project of iets te acquireren wat ze willen hebben. Waarbij bij het proces het al even lang duurt als de tijd waarin de technologie alweer achterhaald is.

H: Gister werd mij ook verteld dat met name met smart cities, dat het nooit 100% veilig is en nooit 100% aangepast aan huidige technologie. Morgen is er al weer iets nieuws bedacht wat de huidige technologie overtreft.

S: Dat kan ook niet anders. Ik ben wel een aanhanger van de denkwijze van Nicholas Taleb, The Black Swan, acht jaar geleden geschreven. En de metafoor, The Black Swan is, we dachten allemaal dat zwanen wit waren tot dat men Australië ontdekte, en zo zijn ook zwarte zwanen. De wereld is op een handelsspoor. Hij relateert dat bijvoorbeeld aan de 9/11 aanvallen op New York. Op dat moment was die aanval verschrikkelijk, en toen zijn wij ook hele denken, zijn wij het vliegverkeer veilig gaan maken door allemaal extra maatregelen. En door allemaal extra zaken te bedenken. Maar wat was de eerstvolgende aanval, een metrostation. En daaropvolgend een bus. Als een mens kwaad wil dan zal hij er uiteindelijk in slagen. En het enige wat je kan zeggen is, de integriteit van het systeem in het totaal moet bestaan. Je kan er een deuk inslaan, je kan een vliegtuig kapen en ergens in vliegen, maar daar maak je het heel systeem nog niet kapot. Dat is het enige wat je kan nastreven.

H: Ja, dus in principe de schade beperken die gedaan wordt.

S: Ja, precies. die nevenschade en het moreel, dat mensen niet bij de pakken neer gaan zitten als zoiets gebeurd maar er bijna weer sterker uitkomen. Met het enorme verlies natuurlijk van die mensen. Maar dat is gebeurd. Maar het wordt dan zeg maar als erger gezien dat je dan ook wel eens het moraal verliest.

H: Dan zou ik nu graag willen overstappen naar de dreigingen van cyberaanvallen. En dan om te beginnen met de vraag, in welke mate cyberaanvallen voorkomen gericht op smart cities.

S: Er is een stap nu als smart he. Ik denk dat als je het hebt over hackers, en doelbewuste cyberaanvallen, worden er altijd stukken infrastructuren of iets van wat waarde is, en zo hebben we natuurlijk gezien die aanval op APM Terminals. Dat is ook een gerichte aanval geweest. Je ziet het in het havengebied. Ik denk dat partijen als ASML. Ik hoor dat ook wel van de Belastingdienst, een aantal dingen, voor mij gaat het gewoon om daar waar de interessante dingen te halen zijn.

H: Ik weet niet of u de situatie in Atlanta heeft meegekregen?

S: Ja.

H: Denkt u dat dit in Nederland ook van toepassing kan zijn? Dat eventueel zo'n grote cyberaanval, zo groot schade effect kan meebrengen?

S: Ja, waarom niet.

H: Zou de kans daar groot op zijn?

S: De kans dat zoiets gebeurd, kijk, wat is een high priority target? Waarom ben je doelwit? Dat kan of zijn voor geld of voor veel business uit halen. Ofwel er is een politiek doel. Nou denk ik dat wij op dit moment niet zo hoog in de aandacht ladder politiek gezien zijn dat de kans groter is dat zoiets in Frankrijk of Duitsland of Engeland zal gebeuren, of Amerika. Dat zijn op dit moment de high priority targets. De kans is aanwezig, zeker. Wij zijn bondgenoten van een aantal, maar ook het Atlantisch verdrag. Daarmee zijn wij ook mogelijk doelwit.

H: Wat zijn volgens SIM-CI of volgens u de grootste cyberdreigingen voor een smart city? Wat is het ergste wat zou kunnen overkomen?

S: Ja, je hebt verschillende types he. Je hebt privacy, privacy gevoeligheid. Dat is aan de hele kant heel eng en aan andere kant, het is maar data. Zelfs al zijn er foto's van jou of van mij, in een heel erg gênante omgeving of posities terug te vinden. Ze zeggen weleens, het zijn maar woorden. Die doen je niet zozeer pijn, en daarmee wil ik het niet bagatelliseren. Als ik kijk naar de veiligheid van burgers. Wij hebben een aantal analyses uitgevoerd over verschillende steden. Daar zie ik bijvoorbeeld dat overstromingen, daar hebben wij al sinds jaar en dag aandacht aan besteed. Wij zijn in 1952 al een keer zwaar overvallen door. Dus op dat moment denk ik, ja, zijn wij er op dit moment nog niet zo, ja misschien van die extreme weersomstandigheden, dat dat nu of binnenkort iets zou kunnen gaan opleveren. Dus dat er dan nu net als nu, 40 dagen, is het echt koel en droog, het is echt droog. Dat er opeens een onweersfront komt wat dagen aanhoudt waar enorme hoeveelheid water uit plenst, dat zou best eens kunnen. Maar dat heeft niet echt met cyber te maken he.

H: Zou het kunnen zijn dat cyberaanvallen dan situatiegebonden zijn? Of periode gebonden? Dat situatie van zo'n storm, dat eventueel de sluizen worden opengezet. Waardoor juist die waterkering niet meer werkt?

S: Daar hebben wij wel naar gekeken naar dat soort effecten maar dat is fysiek niet mogelijk. De sluis is niet verbonden aan het internet. Tenzij je je internet, de afstand kunnen overbruggen, is de sluis veilig. Maar stel je zou nog steeds fysiek in kunnen breken bij de sluis, de sluis kan openzetten. Ik denk dat meest disruptive voor ons zal zijn als je een aanval zou kunnen bedenken die ons dagelijks leven echt zwaar ontwricht. Ik heb een boek gelezen over die bankencrisis en van Lehman Brothers en experts of wetenschappers zeggen dat toen het toen op een haartje na gebeurd was dat het hele internationale betalingssysteem kwam te vallen. Dat heb ik in de energiemarkt ook nog een keer meegemaakt dat een partij was omgevallen en dat die de betalingen niet meer kon garanderen aan andere clubs. Waardoor er een keten van effecten ontstaat. En als dat het resultaat heeft dat de pinautomaten in de winkels niet meer werken, buiten in de automaten niet meer werken. Sterker nog, dat jouw en mijn credit op de bank zijn volledig uitgewist. Niemand weet er iets meer van. Dan kunnen we een heel groot probleem krijgen. Als mensen moeten vecht voor voedsel wordt het heel naar.

H: Denkt u dat een aanval op bepaalde individuele kritieke systemen ook effect op elkaar kunnen hebben? Dat het uitschakelen van het ene systeem het andere systeem kan beïnvloeden?

S: Ja, dat is ook waar wij ons sterk naar kijken. Daar proberen wij ons mee te onderscheiden, met het simuleren van cascade effecten, waterval effecten. Dat je elke keer een trapje dieper erheen gaat. Dan zie je dus bijvoorbeeld dat water en elektriciteit, dat is vrij logisch, dat dat niet zo goed samengaat. Er zijn maar weinig mensen die weten welke netwerken er allemaal aan elektriciteit gebonden zijn. Dus dat je binnen de kortste keren geen mobiel internet meer hebt, daarna geen mobiele telefoons meer hebt, daarna geen C2000, en de nooddiensten. Ja dat soort cascade effecten die je kan krijgen. Dan kan er een soort panische situatie ontstaan. Die je weleens op televisie ziet.

H: Denk je dat steden op dit moment weerbaar genoeg zijn tegen dit soort cascade effecten?

S: Ik denk dat wij nog steeds cascade effecten boven water halen met z'n allen. Dus dat wij nog niet van alles bewust zijn. Dus dan kan je nog niet op alles voorbereid zijn. Of tenminste dan is de voorbereiding mogelijk geluk maar geen geplande activiteit.

H: Dus dat hoort een beetje bij het trial and error gebeuren?

S: Ja, eigenlijk wel en ik denk dat dat ook niet zo raar is. Ik denk dat steden doordat ze smart cities worden, ze steeds meer mensen in steden gaan wonen. Op dit moment zijn er berekeningen met dat meer dan 50% in steden woont aan de kust. En dat wordt in 2050 meer dan 70%. Maar dan is in 2050 vier miljard mensen meer. Dus, het wordt een enorm belasting op die stedelijke kustgebieden. Dus die steden worden gewoon intrinsiek ingewikkelder, net als auto's ingewikkelder zijn geworden en telefoons. Ons samenwerkings leven vormen wordt ook ingewikkelder.

H: Er wordt inderdaad gezegd dat de mensen die niet mee kunnen ontwikkelen, dus vooral niet de kennis hebben om ICT te gebruiken en informatie die ze uit ICT halen, het te kunnen verwerken, dat die achter zullen lopen later. In zo'n netwerkmaatschappij, ben jij van mening dat dit zo is? Dat mensen die niet bijblijven bij ontwikkelingen, die echt de nadelen gaan ondervinden?

S: Er zijn veel ontwikkelingen geweest, die zijn gerefereerd aan deze tijd, technologie. Dat ze de technologie niet begrijpen. Ik denk dat het een beetje vergelijkbaar is met de vorige grote ontwikkelings golf, die zich vooral richtte op automatisering. Zo dacht men dat robots alle mensen in fabrieken wel zouden vervangen. Maar op een of andere manier vindt dat systeem wel weer, robots moeten geprogrammeerd worden en ontstaan er weer andere banen. Laatst had ik een presentatie van een dame. Die liet mensen in Afrika de beelden maken die gebruikt worden om artificial intelligence pods te trainen. Zelfrijdende auto's moeten getraind worden op foto's die bijvoorbeeld door camera's boven de weg genomen worden maar die moeten wel weten waarop ze moeten letten. Die krijgen, een labeltje, dit is de spiegel, dat is een band. Dus dat is een hele nieuwe baan. Er zijn bakken vol met mensen die aan het werk worden gezet en daardoor heeft ze ook de armoede peil opgekrikt. Ja, dat kan natuurlijk ook, ik had er nog nooit over nagedacht.

H: Nee, dat is ook zeker niet voor mij. Het is een interessante oplossing om mensen mee te krijgen met de huidige ontwikkelingen in de ICT binnen deze wereld. Ook een van de ontwikkelingen is het zogenoemde smart grid, waar steden op aangesloten zitten. Wat zijn volgens u de zwakke punten van zo'n smart grid? Waar zou echt op gelet moeten worden als een stad te maken heeft met een smart grid?

S: Smart grid, is dat de combinatie van water, elektra, gas, alles in elkaar? Of is dat alleen elektra of alleen de data? Uiteindelijk zie ik een stad een beetje als een organisme. En dat organisme wordt gewoon complexer net als wij dat zijn. Het was eerst een, meervoudig kwal achtige organisme maar het wordt meer iets als dat wij een soort bewustzijn krijgen. Die netten zijn niet veel meer dan de voedingsbodem voor onze steden. Die data, de elektriciteit, het gas dat voedt ons als stad. Dat voedt onze functionaliteit. Dus dat zie ik als de aders, de levensbanen. En daar waar nodig heb je sensoren nodig om die aders te bedienen. Maar eigenlijk doen we daar niets mee. Je voelt het ook bijna nooit, een aderlijke bloeding. Het alarm mechanisme, je moet dat alleen hebben als je daarop moet gaan acteren. Dus in het systeem, in het netwerk, smart grid moet alleen smart zijn waar het nodig is. Als je niks met die data kan doen heb je het ook niet nodig.

H: Ik heb ook inderdaad meegekregen, een voorbeeld, als een parkeerplaats is uitgerust met sensoren kunnen mensen zien dat een parkeerplaats bezet is of vrij zijn. Maar dat een parkeerplaats op zichzelf is niet echt smart, want het blijft een fysiek object in de omgeving. Het zijn puur de sensoren die iets smart maken. Ik weet bijvoorbeeld dat Den Haag bezig is met een smart plek in Scheveningen om via lichtposten, sensoren, toegang tot bepaalde ICT te verschaffen voor mensen in de openbare ruimte daar. Echter is het nog wel een probleem dat de meer private gebieden, private sectoren in steden, vooral in Den Haag, nog niet aangesloten zijn. Ziet u daar mogelijkheden omdat het in ieder geval veranderd, of dat het problemen gaat opleveren dat het nog niet zo is?

S: Nee, ik laat het maar ontstaan. Ik denk bijvoorbeeld, voor de parkeerproblematiek zou je ook kunnen denken, ik verzorg gewoon dat er in elke auto een sensor zit. En als ik dan via mijn gps-systeem en alles weet waar alle auto's zijn, dan weet ik ook of een parkeerplek bezet is of niet. Je moet wel vanuit een bepaald doel gaan redeneren. En niet zeggen, we gaan daar een parkeerplaats smart maken. Want wat is het doel.

H: Er moet dus wel echt een doel achter zitten volgens u.

S: Kijk, het brengt natuurlijk ook met zich mee, allemaal onderhoud en vervolgacties. Een auto moet wel voor onderhoud ergens naar toe. Een parkeerplaats nog niet. En dan hebben we daar alweer een baan. Wij hebben nu ook al auto's erbij die overal mobiel scannen. Heb je alleen dat in kaart brengen nodig ook voor de rest. Je kan misschien op afgeleide data, je kan misschien heel veel daarop baseren.

H: Ik zou dan nu verder willen gaan op de maatregelen van een cyberaanval. Welke vormen van cybersecurity kunnen smart cities gebruiken om cyberaanvallen tegen te gaan? Wat voor fysieke en digitale middelen zijn er om dit te regelen?

S: Daar ben ik niet de expert in. Je hebt natuurlijk heel veel middelen om je te beschermen. En een daarvan is jezelf niet op internet aan te sluiten. Die ken ik dus ook van Sluis en andere echt kritische infrastructuren. Die kan je loshalen van internet en dan komt er niks voorbij. Dan moet iemand met een usb stick of iets anders fysiek de ruimte in. Op IT-gebied zijn er genoeg partijen en bedrijfjes die maatregelen gaan vinden. Waar het op neer komt, hetzelfde met het beveiligen van een vliegveld of haven, je moet redeneren wat iemand fout zou of kwaad zou willen doen in jouw infrastructuur of systeem. En daar moet je dan middelen en checks op gaan voeren.

H: Zijn in principe dus puur de situatie gebonden vormen van beveiliging die tot eventueel problemen kunnen leiden?

S: Wat wij elke keer natuurlijk doen, wij vinden maatregelen uit voor iets wat al een keer fout is gegaan. Als er bij ons ingebroken thuis, zetten we een camera voor de deur, want als er dan een inbreker komt met een spotlight, dat is al een keer gebeurd. Maar als hij dan via de achterdeur komt dit keer daar is dan nog niks geplaatst. Als we een beetje disruptief kunnen denken, zetten we hem voor en achter. Maar je denkt is dat soort mechanisme.

H: Het is puur waar het heeft plaatsgevonden, dat je het echt aanpakt.

S: Over het algemeen zie je dat wel. Je ziet in sommige gevallen nog dat er op andere manieren gedacht wordt, maar over het algemeen is het dus het lek dichten en daar naar kijken. Op sommige manieren wordt er nogal disruptief gekeken, maar ik vraag me ook af in hoeverre dit allemaal zin heeft. Als iemand echt kwaad wil, dan kan hij dat. Volgens mij moet je dan dus zorgen dat de dingen die jij echt belangrijk vindt, net zoals in je huis of ergens anders, dat je die goed beveiligd hebt. Met de rest moet je misschien genoegen nemen met minder.

H: Okee. Bent u van mening dat op dit moment steden de mogelijkheid hebben om zich goed te verweren tegen dit soort cyberaanvallen?

S: De stad zelf, als we het hebben over de gemeente. We zitten vlakbij het gemeentehuis van Den Haag. Ja, dan krijg ik gelijk een beeld in mijn hoofd van dat daar in een kamer mensen zitten met een heel dashboard vol schermen om te kijken wat er allemaal wel niet in Den Haag gebeurt en wat er mis kan gaan. Dat vermoeden heb ik niet, dat dat bestaat. Ik weet dat Stedin zo naar zijn net kijkt,

Linea kijkt zo naar de watervoorziening en een aantal bedrijven hebben wel een heel goed inzicht in hun netwerk en hun mogelijkheden. Een hoofdrol of overkoepelend beeld is er volgens mij niet.

H: Dus het is puur dat de kritieke infrastructuur, de systemen daarvan apart worden gemonitord in plaats van door één geheel samen in de gaten gehouden worden.

S: Ja, en de vraag is dan ook in hoeverre het wenselijk is dat een iemand alles bestuurt, want dan ga je het ook hebben over je prudentie. Wat als iemand ingrijpt in het netgebied of de architectuur van iemand anders?

H: Bent u dan niet van mening dat als er zoveel uit handen wordt gegeven, dat het dan juist kwetsbaarder wordt omdat de informatie die dan gedeeld wordt niet altijd 100% hoeft te zijn? Dat ze zich er niet van bewust zijn wat er speelt bij andere dingen? Dat de stad of het grid daar kwetsbaarder door wordt?

S: Ja. Maar kijk, alle systemen die uiteindelijk complexer worden zijn op een bepaalde manier ook wel weer kwetsbaarder. Als je alles vergelijkt met een ééncellig organisme, een ééncellig organisme is manipuleerbaar vanaf de buitenwereld met een beperkt aantal dingen. Je kunt hem geen gedachten influisteren of op een andere manier manipuleren. Dat kan met een mens bijvoorbeeld wel. Dus je hebt altijd de voors en tegens van de complexiteit van een systeem. Maar ja, als wij als bewuste wezens naar een leven vol welzijn streven, dan zullen we een aantal dingen moeten accepteren.

H: Okee. U stelt dus in principe, hoe groter en complexer het organisme, hoe meer manieren en bedreigingen er zijn om het organisme te ontregelen.

S: In principe. Tenzij je alles en alles en alles voorziet van sensoren. Maar die sensoren moet je ook weer van intelligentie voorzien, want zonder intelligent gaat die sensor alleen maar een camerabeeld opnemen of iets anders. Je kan hele slimme systemen daaraan gaan koppelen, maar die slimme systemen moeten uiteindelijk weer bij iemand terecht komen die daar een beslissing over neemt.

H: Okee. Die cyberaanvallen brengen problemen mee die zowel vooraf als achteraf kunnen worden opgelost, ex post en ex ante. Focust SIM-CI zich ook op bepaalde plekken, zoals ex-ante of ex-post, wanneer jullie simulaties ontwikkelen en advies geven?

S: Meestal proberen we te kijken naar het voorkomen, maar op dit moment gebruiken we onze software ook voor trainingsdoeleinde. Dan kom je meer op de ex post oplossingen. Wat moet je doen op het moment dat dit zich voordoet? En het liefst zouden wij bezig zijn met hoe je het helemaal kan voorkomen. Zo ver zijn wij ook niet niet qua ontwikkeling.

H: Maar jullie houden zich juist al wel bezig met het compleet voorkomen van aanvallen?

S: Ja. Hoe eerder je in die keten komt van planning naar uitvoering. In de planningsfase kun je de kosten en dan bedoel ik de kosten in de breedste zin, van het leven tot de economische kosten, nog het meest beïnvloeden met de minste kosten.

H: De schade die eventueel achteraf komt kijken bij de aanval op een kritiek systeem, zijn er op dit moment de mogelijkheden om die goed op te lossen? Is er de mogelijkheid om daarbij op tijd in te grijpen om het niet compleet te laten escaleren?

S: Nou dat proberen wij te doen in die simulaties en wij berekenen in die simulaties ook de kosten, zoals wij denken dat het is. Het kan bijvoorbeeld de storingsminuten zijn die de netbeheerder moet terugbetalen tot en met, we hebben dan de WOZ-waarde in het kadaster gepakt om te kijken naar de waarde in het vastgoed. Dus we proberen daar een schatting van te maken en we proberen nu ook mitigaties voor te stellen om dat soort dingen te voorkomen. Stel dat het voorkomt dat de sluis bij Scheveningen toch gehackt wordt en open wordt gezet bij springtij, dat iemand dan weet wat hij moet doen. Hij moet dan het ziekenhuis veilig stellen en dit, dit, dit, dit, dit doen om erger te voorkomen.

H: Mocht er een aanval komen op een kritiek subsysteem en het lukt ook, welke partijen zullen daar dan de meeste last van ondervinden en dan met name te denken aan de overheid, bedrijvigheid, de inwoners zelf?

S: Ja, ik denk allemaal. Allemaal als de burgers van een stad. We kunnen er allemaal de invloed ervan ondervinden en de rest is een beetje een blaming en shaming verhaal. Is het de schuld van de burgemeester of is het de schuld van de netbeheerder? Dat heeft te maken met iemands baan, maar in eerste instantie bij een catastrofale oplossing gewoon om de burger.

H: Dus eigenlijk heeft iedereen te maken met de effecten, maar de verantwoordelijkheid wordt achteraf pas bepaald?

S: Meestal wel, ja.

H: Okee. Moet volgens u de bestuurlijke organisatie, zoals die van een stad als Den Haag, voornamelijk een samenwerking aangaan met externe actoren om tot een zo goed mogelijk oplossing te kunnen komen, of denkt u dat dit ook intern binnen de gemeente kan worden opgelost?

S: Tuurlijk, zolang je een bepaald mandaat hebt en een ontwikkelmogelijkheid maakt het volgens mij niet uit of het in de gemeente gebeurt of met een andere organisatie. Ik denk dat je altijd wel goed in de kaart moet hebben, want een organisatie is ook niet heel anders dan een organisme. Een hele groep mensen, cellen, die met z'n allen een bepaald doel nastreven. Dan heb je de wat agressieve roofzuchtige soorten en de vreedzame, maar ze hebben allemaal een bepaald doen. En als je de juiste mensen, bij het juiste doel en de mandaat rond de tafel hebt dan kan je iets oplossen. Wat ik wel zie, is dat er veel gepraat wordt en dat het veel in vaagheden blijft. Dat is helemaal niet erg en dat is die mensen ook niet kwalijk te nemen. Anders dan zich dat ook te realiseren en op een gegeven moment daaromheen gaan we een klein stukje van deze puzzel helemaal oplossen.

H: En mochten deze samenwerkingen wel worden doorgezet met eventuele externe actoren, hoe zou volgens u dan zo'n samenwerking het best kunnen verlopen? Wie zou wat moeten ondernemen in zo'n samenwerking?

S: Nou, de ondernemers is de ondernemer. Dus die is als het goed is ook wel initiatiefnemer bij deze. Maar ik denk dat de gemeente en andere actoren daar ook voor open moeten staan. Maar wat ik wel bemerk, is dat de urgentie en opvolging van dit soort zaken laat wel wat te wensen over. Ik wil best wel hard werken, hard lopen ergens voor, maar dan moet er ook wel een partij zijn die dat waardeert en ontvangt.

H: Dus het is puur het resultaat wat erbij komt kijken, dat eventueel de stimulans voor een externe actor kan zijn?

S: Ja, ik denk dat het liefste, en dat is voor gemeente en voor andere misschien alleen als aanbesteding weer lastig te doen, maar die aanbesteding hebben natuurlijk ook deels hun beste tijd wel gehad. Een aanbesteding kan je vooral doen in iets dat je al kent. Als ik nieuwe paperclips moet bestellen, dan kan ik daar prima een aanbesteding in doen. Als ik kijk naar ons type simulaties, dan verandert de zaak. Het is toch wel een lastig product, niet te vergelijken met dat van anderen. Dat moet je misschien niet altijd willen en misschien moet je niet altijd een project willen met een vast omlijnd einde. Je moet juist concrete afspraken met elkaar hebben, dat doel gaan we nastreven en deze werkafspraken maken we daarbij om de kosten te beheersen, om daar op een goede manier naar te kijken.

H: Maar verder dus wel alles flexibel houden?

S: Ja, nou ja. Bij een project kun je altijd wat zeggen over de kwaliteit, de tijd en het geld. Meestal de klassieke project pijlers en je kan er nog steeds één of twee vastzetten. Dat betekent dat bij de andere, dat daar wat slack in komt.

H: We hadden het net al gehad over hoe SIM-CI helpt bij een stad als Den Haag door advies te geven en simulaties uit te voeren en hoe de gemeente hiermee geholpen wordt. Welke rol speelt SIM-CI eventueel in het verder ontwikkelen van cybersecurity?

S: Daarin spelen wij de volgende rol: we zitten de bij HSD, omdat we daar aan grenzen. Uiteindelijk gaat het erom dat wij de gevolgen laten zien als je ergens inmiddels een hack hebt. Hoe die hackt tot stand komt en hoe je die kunt voorkomen zeggen wij niet zoveel over.

H: Het zijn dus puur de gevolgen achteraf…

S: Ja. Het zijn meer de gevolgen achteraf wat wij kunnen laten zien en dat maakt het ook weer heel spannend. Wij laten de kwetsbaarheden zien.

H: Dus jullie zijn eigenlijk een soort adviesorgaan voor cybersecurity?

S: Ja, maar ik denk eerder voor degene die de infrastructuur beheren.

H: Dan kom je vooral kijken bij bedrijven zoals Alliander en dat soort bedrijven allemaal.

S: Ja.

H: Okee. Deze externe actoren zoals Alliander, bent u van mening dat deze bedrijven eventueel deze keuzes van de gemeenten of overheden kunnen beïnvloeden door te zeggen van indien u deze samenwerking met ons wilt aangaan op dit gebied, dan moet u ook een samenwerking aangaan met andere bedrijven op dit gebied, want daar werken wij mee samen?

S: Nee, niet specifiek denk ik. De aandeelhouders van Alliander en andere netbeheerders zijn overheden en gemeenten. Er zit al een hele sterke band onderling en ik denk ook dat een netbeheerder zich daar niet te veel in zou moeten mengen.

H: Dus de rol van een externe actor zou dus niet een grote invloed hebben die verandering of beweging kan brengen in bepaalde ideeën?

S: Nee, dat zou ik niet zeggen.

H: Okee. Dan zijn we aangekomen bij het stukje over de implementatie van beleid over cybersecurity bij bestuurlijke organisaties. Bent u van mening dat het huidig beleidskader van de gemeenten en steden toereikend genoeg is om problemen op te lossen rondom cybersecurity?

S: Deze vind ik lastig te beantwoorden, want het gebeurt natuurlijk tot op een zekere hoogte nu. Maar er zijn ook weer meer voorbeelden van aanvallen. Dus ik ben van mening dat dit nog eigenlijk een beetje een onontginnen terrein is.

H: Dus dat het beleid dat er al is, de huidige problemen aanpakt. Maar de problemen die nog moeten komen, dat het beleid daar nog niet voor klaar is.

S: Dat is denk ik een beetje in het voorbeeld van auto's, dat er opeens een verhoogd aantal mensen dood gingen door verkeersongelukken. En bijvoorbeeld dat de eerste auto's een normale glazen ruit hadden, waardoor er ontzettend veel mensen met gezichtsletsel rondliepen omdat ze gewoon door die voorruit geklapt waren. Geen veiligheidsgordel, geen veiligheidsglas. Dat beleid dat vormt zich en naarmate dit soort DDoS aanvallen en andere dingen gebeuren, zullen we daar ook beleid op moeten gaan vormen.

H: En op welke manier kunnen smart cities of steden die smart cities willen worden hun beleid het best blijven toespitsen? Waarmee zouden ze rekening moeten houden? U zegt nu inderdaad dat het komt met de veranderingen, maar zijn er bepaalde ideeën waar zij rekeningen mee moeten gaan houden?

S: Nee, niet dat ik weet. Niet dat ik per se weet.

H: Dus het is inderdaad nog steeds een onbekend terrein zoals u al zei.

S: Ja, ik denk het een heel onbekend terrein is ja.

H: Lopen deze steden ook veel restricties uit het nationale cybersecuritybeleid tegen het lijf bij het opstellen van hun eigen beleid? Of worden ze er alleen maar in begeleid door dat beleid?

S: Ik denk het tweede.

H: Dus om het beleid van gemeente aan te scherpen of aan te sturen?

S: Ik denk het wel. Kijk, de gebeurtenissen in de werkelijkheid zijn natuurlijk een reden om afspraken te maken, he. Het feit dat we samen zijn gaan wonen in gemeenschappen en in dorpen en in steden, hebben ertoe geleid dat we afspraken maken dat we elkaar geen letsel toedienen of dat we elkaar ook niet bestelen. Het is natuurlijk ooit een keer gebeurt en dan moet je daar afspraken over gaan maken. Hetzelfde geldt voor het cyberbeleid en het cyberbeleid kan denk ook in verschillende vormen. Het kan ofwel het lekken van gevoelige informatie zijn. Het kan ofwel economische schade zijn. Het kan daadwerkelijk een fysieke aanval zijn. Dat zijn toch belangrijke dingen om in de gaten te houden.

H: Helpt SIM-CI de overheid of gemeenten bij het opstellen van dit soort beleid?

S: Niet zo zeer, niet zo zeer. Wij zijn meer een… met onze simulaties willen wij beslissingsbevoegden ondersteunen in het maken van de juiste beslissingen. Dat kan beleid zijn, maar daar willen we ook niet al te sturend in zijn.

H: Daar zijn jullie in ieder geval niet op toegespitst.

S: Nee.

H: Okee. Dan zijn we als laatst aangekomen bij de urgentie en kosten van cybersecurity. Hoe hoog staat het verbeteren van cybersecurity op de agenda bij gemeenten en eventueel bedrijven als SIM-CI?

S: Ja, hoog. Bij ons heel hoog. Wij hebben natuurlijk vertrouwelijkheid factor nummer één. Klanten moeten er echt op kunnen… kijk, als wij echt een gevoelige analyse maken dan laten wij zien wat het pijnpunt is en dat is ook gelijk weer informatie voor eventuele terroristen om te misbruiken. Dus wij hebben het heel hoog in het vaandel staan en iedereen die wij spreken heeft dat ook.

H: Dus u kunt in principe zeggen dat er voldoende geïnvesteerd wordt binnen SIM-CI en gemeenten op het gebied van cybersecurity?

S: Ja, voor zover te zien wel.

H: Denkt u dat er bij een groter budget voor cybersecurity meer mogelijkheden zouden kunnen zijn of denkt u dat het op dit moment een plafond heeft geraakt vanwege dat het mensen niet kan voorbereiden op wat komen gaat?

S: Er zijn altijd meer dingen die je kan doen. We zouden onze eigen satelliet de stratosfeer in kunnen schieten. Ik kan van alles bedenken. We kunnen een tank hier neerzetten. Ja, er zijn dus altijd meer mogelijkheden, maar je moet wel altijd zeggen van wat is het doel en wat zijn de middelen die ik daartoe heb en is dat genoeg? Of moet ik echt wel gaan schreeuwen om aandachten van dit is niet genoeg?

H: Maar het zal dus niet voorkomen dat er gewoon muur achter muur achter muur opgebouwd wordt om maar proberen iets tegen te gaan en dan onze kop in het zand te steken?

S: Ik denk vooral bewust zijn. Het gaat vooral, maar vooral over hoe je er mee samenwerkt en met je collega's dat je nadenkt over wat een slimme manier zou kunnen zijn voor indringers om binnen te kunnen komen.

H: Okee. Dan was dit het einde van het interview. Heeft u nog enige vragen omtrent het interview of het onderzoek dat ik uitvoer?

S: Nee hoor.

H: Okee. Dan zou ik nogmaals graag willen benadrukken dat de antwoorden gegeven in het interview online komen te staan en gedeeld zullen worden met mijn eerste en tweede corrector en de online scriptiedatabank van de Radboud Universiteit. Er is eventueel de mogelijkheid om mijn scriptie te ontvangen nadat hij afgerond is. Heeft u daar interesse in?

S: Ja, dat is leuk.

H: Okee. Ja, dan nogmaals bedankt voor het maken van tijd en met het helpen bij het interview. Dan wens ik u nog een prettige dag verder.

S: Ja, jij ook.