DE CYBERSECURITY GERELATEERDE INFORMATIE-UITWISSELING

Over het optimaliseren en faciliteren van publiek-private samenwerking in het economisch en maatschappelijk belang van Nederland

Bachelor Thesis

Siep van Sommeren

COLOFON

DE CYBERSECURITY GERELATEERDE INFORMATIE-UITWISSELING

Over het optimaliseren en faciliteren van publiek-private samenwerking in het economisch en maatschappelijk belang van Nederland

AUTEUR

De heer S.L.J (Siep) van Sommeren
svansommeren@me.com
+31 (0) 6 46713866

Version 1.0

Bachelor thesis Information Security Management
The Hague University of Applied Sciences, Faculty IT & Design

EERSTE BEGELEIDER

De heer L.C.M (Leo) van Koppen MSIT
l.c.m.vankoppen@hhs.nl
+31 *(0)* 6 49894062

TWEEDE BEGELEIDER

De heer Drs. J.A.J. (Jaap) de Bie
j.a.j.debie@hhs.nl
+31 *(0)* 6 19844785

OPDRACHTGEVER

Mevrouw Drs. E.C. (Elly) van den Heuvel
e.c.van.den.heuvel@cybersecurityraad.nl
+31 *(0)* 70 7515555 (secretariaat)

BEGELEIDER

Mevrouw Drs. A.A. (Andrea) Bakker
a.a.bakker@cybersecurityraad.nl
+31 *(0)* 70 7515555 (secretariaat)

The Hague, 2 june 2017

REFERAAT

Nederland digitaliseert. Door digitalisering zullen steeds meer ICT-toepassingen met elkaar worden verbonden, dit zal de komende jaren alleen maar toenemen als gevolg van het Internet of Things. De afhankelijkheid van andere bedrijven neemt door deze verbondenheid toe. De sterkte van de digitale keten wordt bepaald door de zwakste schakel.

Het bedrijfsleven, met name het midden- en kleinbedrijf (mkb), heeft behoefte aan een verbeterde informatiepositie. Binnen dit onderzoek is onderzocht op welke wijze de informatiepositie van het mkb kan worden geoptimaliseerd, ter bevordering van de weerbaarheid van de digitale ketens.

Dit onderzoek leidt tot een model waardoor de informatie-uitwisseling met betrekking tot cybersecurity kan worden geoptimaliseerd. Het model is geverifieerd en gevalideerd door experts op het terrein van cybersecurity en ontwikkeld aan de hand van literatuuronderzoek en interviews.

KERNWOORDEN:

Cyber security, cybersecurity, informatiebeveiliging, ketenveiligheid, ketenverantwoordelijkheid, kennisdeling, informatie-uitwisseling, samenwerking, publiek-private samenwerking, PPS, Digital Trust Centrum, DTC, het bedrijfsleven, midden- en kleinbedrijf, mkb, Cyber Security Raad en CSR

BIJ VOORKEUR CITEREN ALS:

Siep van Sommeren, *De cybersecurity gerelateerde informatie-uitwisseling – Over het optimaliseren en faciliteren van publiek-private samenwerking in het economisch en maatschappelijk belang van Nederland.* Den Haag, The Hague University of Applied Sciences 2017

VOORWOORD

Met het inleveren van dit onderzoeksrapport komt het einde van mijn afstuderen in zicht. Ik ben van februari 2017 t/m juni 2017 bezig geweest om dit onderzoek tot eigen tevredenheid en op een hoogwaardige manier tot een einde te brengen.

Met het inleveren van dit onderzoeksrapport komt niet alleen het einde van mijn afstuderen in zicht, maar ook aan de studie Information Security Management. In de afgelopen jaren heb ik met veel plezier kennis vergaard en ervaring opgedaan bij Koninklijke KPN en Royal Schiphol Group.

Een mooie periode in mijn leven loopt op zijn einde. Ik wil van de gelegenheid gebruik maken om een aantal mensen te bedanken. Allereerst wil ik, Elly van den Heuvel bedanken voor de kans die zij mij heeft geboden om bij Bureau Secretaris van de Cyber Security Raad af te studeren. De CSR is het hoogste onafhankelijke adviesorgaan van Nederland op het gebied van cybersecurity én uniek in de wereld. Daarnaast wil ik Andrea Bakker bedanken voor de begeleiding, feedback en de prettige samenwerking die ik met haar in de afgelopen afstudeerperiode heb gehad.

Daarnaast wil ik mijn examinatoren Leo van Koppen en Jaap de Bie bedanken voor hun begeleiding en de soms zeer stevige discussies tijdens mijn afstudeerperiode. In het bijzonder wil ik nogmaals Leo van Koppen bedanken voor de zeer goede en prettige begeleiding tijdens de afgelopen vier jaar. Ook wil ik Jaya Baloo en Sjoerd Blüm bedanken voor de kans die zij mij hebben geboden om stage te lopen bij Koninklijke KPN en Royal Schiphol Group.

Verder wil ik natuurlijk: mijn ouders en broer bedanken voor de onvoorwaardelijke steun. En als laatste wil ik mijn vriendin bedanken, die tijdens mijn afstudeerperiode in Berlijn woonde en werkte, voor de onvoorwaardelijke steun en liefde en het bieden van afleiding tijdens de weekenden waarin we samen in Berlijn waren.

Enorm bedankt! Zonder jullie was ik nooit gekomen tot waar ik nu sta en tot wie ik nu ben.

Siep van Sommeren

Juni 2017

DE CYBERSECURITY GERELATEERDE INFORMATIE-UITWISSELING

Over het optimaliseren en faciliteren van publiek-private samenwerking in het economisch en maatschappelijk belang van Nederland

Bachelor Thesis

Siep van Sommeren

INHOUDSOPGAVE

SAMENVATTING

Digitalisering biedt enorme kansen voor de welvaart in Nederland. Naast kansen zijn er ook bedreigingen die digitalisering meebrengt. Ook in de digitale keten doen zich veranderingen voor: bedrijfsprocessen zijn afhankelijk van andere bedrijven en dienstverleners als gevolg van de onderlinge verbondenheid. Om maatschappelijke ontwrichting en schade aan het bedrijfsleven in Nederland te voorkomen als gevolg van cyberdreigingen in de digitale keten, is een aanpak nodig om de informatie-uitwisseling te optimaliseren en te faciliteren.

Het NCSC faciliteert (sinds 2012) organisaties in de vitale infrastructuur en de rijksoverheid van informatie en expertise met betrekking tot cybersecurity. Als gevolg van het mandaat van het NCSC kunnen zij weinig betekenen voor het bedrijfsleven dat geen deel uitmaakt van de vitale infrastructuur. Voor het mkb ontbreekt een soortgelijke aanpak.

Vanuit deze probleemanalyse is onderzoek verricht naar de wijze waarop de kennisdeling en informatie-uitwisseling aan het mkb kan worden geoptimaliseerd ter bevordering van digitale ketens in Nederland. De onderzoeksdata is verzameld door middel van literatuuronderzoek en semigestructureerde interviews.

Uit dit onderzoekt blijkt dat Nederland de beschikking moet krijgen over een landelijk dekkend stelsel van initiatieven waar het mkb zich kan aansluiten. Dit stelsel moet een samenspel zijn van publieke, private, nieuwe en bestaande organisaties, instrumenten en initiatieven. Deze collectieve aanpak moet ervoor zorgen dat de informatie-uitwisseling het volledige Nederlandse bedrijfsleven omvat. Het is hierbij van essentieel belang dat in gezamenlijkheid de verantwoordelijkheid wordt genomen om de veiligheid van digitale ketens te waarborgen. Door het optimaliseren en faciliteren van de publiek-private samenwerking kan de informatiepositie van het mkb verbeteren. De toegevoegde waarde van de informatie-uitwisseling aan het mkb is dat het de weerbaarheid bevorderd van digitale ketens in Nederland van zowel organisaties in de vitale infrastructuur, rijksoverheid als het volledige Nederlandse bedrijfsleven. Dit is in het economisch en maatschappelijk belang van Nederland en zorgt ervoor dat Nederland haar vooraanstaande positie op het terrein van digitalisering kan behouden.

1 INLEIDING

In dit hoofdstuk wordt het onderzoek beschreven dat is verricht naar hoe kennisdeling en informatie-uitwisseling de informatiepositie van het midden- en kleinbedrijf (mkb) kan verbeteren. In dit hoofdstuk wordt beschreven het kader waarbinnen dit onderzoek is uitgevoerd. De inleiding heeft als doel duiding te geven over het onderzoek.

1.1 DIGITALISERING VAN DE SAMENLEVING VEREIST EEN NIEUWE AANPAK

Nederland digitaliseert. Het belang van digitalisering in onze economie en maatschappij wordt bekrachtigd. Digitalisering biedt enorme kansen voor de welvaart in Nederland. Om deze kansen te blijven benutten, is vertrouwen in digitalisering noodzakelijk. Nederland heeft zich in de loop der jaren ontwikkeld tot één van de meest gedigitaliseerde landen ter wereld. Dit komt mede door het uitstekende telecomnetwerk (Verhagen, 2016). Ruim vijf procent (CBS, 2016) van het bruto binnenlands product (bbp) wordt inmiddels verdiend met ICT. De digitale economie vormt naast de traditionele mainports: Luchthaven Schiphol en de Rotterdamse haven, de derde mainport van Nederland (kst-34300-XIII-45, 2015). De digitale mainport.

In bijna alle maatschappelijke sectoren is de digitale technologie het belangrijkste middel om informatie te verwerken, te verzenden en/of het primaire bedrijfsproces aan te sturen binnen organisaties in zowel de vitale infrastructuur als het mkb.

Het nemen van adequate en passende maatregelen in de digitale ketens is moeilijk, omdat inzicht ontbreekt in de digitale ketens. Dit komt omdat maar weinig bedrijven en overheden zicht hebben op de digitale ketens waar zij afhankelijk van zijn. Deze afhankelijkheid neemt steeds verder toe als gevolg van digitalisering (CSR, 2016). De digitale ketens in zowel de vitale infrastructuur als het mkb zijn dermate complex ingericht, of in de loop der jaren geworden dat inzicht in de cyberdreigingen in de digitale keten ontbreekt. Ketenveiligheid in de digitale keten is van cruciaal belang ter voorkoming van maatschappelijke ontwrichting en schade aan het bedrijfsleven. Hierbij geldt dat de sterkte van de keten wordt bepaald door de zwakste schakel. Binnen ketenverantwoordelijkheid is het van belang alle ICT-middelen in de digitale keten weerbaar te maken tegen cyberdreigingen.

Hierbij zal worden uitgegaan van het feit dat het mkb producten en diensten levert aan organisaties in de vitale infrastructuur. De digitale ketens worden daardoor kwetsbaarder en in potentie kan het effect hebben op onze economie en maatschappij (CSR, 2016). Het mkb neemt een belangrijke rol en positie in de ketenveiligheid van organisaties in de vitale infrastructuur. De veiligheid van zowel de vitale infrastructuur als het mkb loopt hiermee gevaar. Het belang van ketenveiligheid is aanzienlijk omdat het de bedrijfscontinuïteit omvat van organisaties in zowel de vitale infrastructuur als het mkb.

In januari 2012 is het Nationaal Cyber Security Centrum (NCSC) opgericht (Rijksoverheid, 2012), met de oprichting van het NCSC kwam er een centraal informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC levert een bijdrage aan het vergroten van weerbaarheid van de Nederlandse samenleving. Echter, behoren alleen de rijksoverheid en organisaties in de vitale infrastructuur tot de doelgroep van het NCSC (NCSC, 2017). Hierbij is geen rekening gehouden met de ketenveiligheid van de digitale keten.

Om maatschappelijke ontwrichting en schade aan het bedrijfsleven in Nederland als gevolg van cyberdreigingen te voorkomen is een aanpak nodig om de kennisdeling en informatie-uitwisseling van bijvoorbeeld incidenten en modus operandi op het gebied van cybersecurity te optimaliseren en te faciliteren. Deze aanpak ontbreekt voor het mkb.

1.2 PROBLEEMSTELLING, DOELSTELLING EN VRAAGSTELLING

De hiervoor beschreven ontwikkeling geeft een tegenstrijdig beeld. Er lijkt namelijk sprake te zijn van tegenstrijdige ontwikkeling. In 2012 is het NCSC opgericht om een bijdrage te leveren aan het vergroten van de weerbaarheid van de Nederlandse samenleving op het gebied van cybersecurity.

De kennisdeling en informatie-uitwisseling het NCSC is alleen toegankelijk voor de doelgroep (rijksoverheid en vitale sectoren). Het mkb beschikt niet over de informatie en expertise, terwijl ketens in vitale processen afhankelijk zijn van het mkb. Het probleem is tweeledig. Enerzijds heeft het mkb behoefte aan een verbeterde informatiepositie soortgelijk aan de informatiepositie van de vitale sectoren, waardoor het volwassenheidsniveau van het mkb toeneemt. Anderzijds levert het mkb producten en diensten aan organisaties in de vitale infrastructuur, waardoor de weerbaarheid van de digitale keten beïnvloed kan worden en dit heeft dus ook gevolgen voor organisaties in de vitale infrastructuur.

1.2.1 DOELSTELLING

Het mkb heeft behoefte aan een verbeterde informatiepositie bijvoorbeeld gelijksoortige aan de informatiepositie van de vitale sectoren. De aanpak ontbreekt om het mkb te voorzien van een soortgelijk model. Het doel van dit onderzoek is te komen tot een model om de kennisdeling en informatie-uitwisseling met betrekking tot cybersecurity in het mkb te optimaliseren en te faciliteren. Er zal worden uitgegaan van huidige succesvolle modellen in de vitale sectoren.

De datacenterbranche is geselecteerd om te voorzien van een model voor de kennisdeling en informatie-uitwisseling met betrekking tot cybersecurity. In paragraaf 1.3 wordt de keuze voor de datacenterbranche gemotiveerd.

"Het ontwikkelen van een model, met betrekking tot cybersecurity, ter bevordering van de kennisdeling en informatie-uitwisseling in het mkb, waarmee op basis van de behoeften van het mkb in de datacenterbranche, de weerbaarheid in de digitale ketens in Nederland kan worden verhoogd."

Bij de ontwikkeling van het model wordt rekening gehouden met de ambitie om het model in meerdere sectoren binnen het mkb in te richten. Het model zal enerzijds bestaan uit een algemeen deel, welke als blauwdruk kan gelden voor andere sectoren. Anderzijds zal het model bestaan uit een specifieke deel met de informatiebehoefte van de datacenterbranche.

1.2.2 VRAAGSTELLING

De vraagstelling van dit onderzoek is afgeleid van de doelstelling. Om deze doelstelling te beantwoorden zijn de centrale onderzoeksvraag en vijf deelvragen geformuleerd. De centrale onderzoeksvraag en deelvragen luiden als volgt:

Centrale onderzoeksvraag:

Op welke wijze kan, met betrekking tot cybersecurity, kennisdeling en informatie-uitwisseling aan het mkb worden geoptimaliseerd ter bevordering van de weerbaarheid van de digitale ketens in Nederland?

Deelvragen:

- *Wat is de toegevoegde waarde van kennisdeling en informatie-uitwisseling aan het mkb?*
- *Welke knelpunten zijn er in de huidige opzet van huidige beschikbare modellen?*
- *Welke randvoorwaarden liggen ten grondslag aan kennisdeling en informatie-uitwisseling?*
- *Hoe ziet de ideale kennisdeling en informatie-uitwisseling eruit voor het mkb?*
- *Wat is er nodig om de kennisdeling en informatie-uitwisseling te bevorderen?*

1.3 ONDERZOEKSPOPULATIE

De onderzoekspopulatie betreft het mkb en specifiek de datacenterbranche in het mkb. De reden om dit onderzoek te concentreren op de datacenterbranche komt voort uit het feit dat Nederland één van de meest gedigitaliseerde landen ter wereld is (Verhagen, 2016) en datacenters het fundament van die digitale infrastructuur zijn.

Het bedrijfsleven, met name het mkb, maakt veelvuldig gebruik van digitale diensten die zijn ondergebracht bij datacenters. Uit onlangs uitgevoerd onderzoek blijkt dat 25% van het bbp afhankelijk is van datacenters en cloud- en hostingproviders (DHPA, DDA, ISPConnect en theMETISfiles, 2017). Het rapport *"Nederland digitaal droge voeten"* besteedt ook aandacht aan de digitale economie, zoals eerder te lezen was in dit hoofdstuk.

1.3.1 DATACENTER KENMERKEN

Bedrijfskritische IT-apparatuur kan worden ondergebracht in een datacenter. Een datacenter beschikt ook over snelle netwerkverbindingen. Deze snelle netwerkverbindingen staan vaak in verbinding met internetknooppunten[1].

Een datacenter is vaak uitgerust met geavanceerde voorzieningen, zoals klimaatbeheersing, brandblussystemen, noodstroomvoorzieningen en van fysieke veiligheidsmaatregelen en 24x7 monitoringdiensten voorzien. De voorzieningen zijn al dan niet redundant uitgevoerd. Deze voorzieningen worden getroffen om de betrouwbaarheid van de dienstverlening te garanderen.

Diensten van cloud- en hostingproviders zijn vaak ondergebracht bij een datacenter om een betrouwbare dienstverlening te kunnen garanderen aan klanten. Diensten van cloud- en hostingproviders (DHPA, DDA, ISPConnect en theMETISfiles, 2017) variëren van colocation, dedicated hosting, shared hosting, packaged software, infrastructure-as-a-service, platform-as-a-service, software-as-a-service (Deloitte, 2016).

1.4 HYPOTHESE

De hypothese binnen dit onderzoek is dat het model voor het mkb eenzelfde structuur moet kennen als de Information Sharing and Analysis Centres (ISAC's). Het model zal in plaats van een sectorenaanpak gebruik maken van brancheverenigingen. Tevens zal binnen het model een rol weggelegd zijn voor de veiligheidsregio's aangezien zij belast zijn met het bewaken van de regio. In de Wet veiligheidsregio's (Ministerie van Justitie, 2017) wordt geen onderscheid gemaakt tussen fysieke of digitale veiligheid, ook is er geen sprake van uitsluiting van digitale veiligheid. Daarnaast zal er een rol zijn voor de Kamer van Koophandel (KvK) om het bestaan van het model kenbaar te maken aan het mkb. De KvK zou dit kunnen doen door het uitreiken van een flyer bij de inschrijving van een nieuwe onderneming en/of het ledenbestand met alle Nederlandse ondernemingen in te zetten.

1.5 LEESWIJZER

In dit hoofdstuk is het kader beschreven waarbinnen dit onderzoek is uitgevoerd. In hoofdstuk 2 wordt ingegaan op de methodiek van dit onderzoek. In hoofdstuk 3 wordt aandacht besteed aan het literatuuronderzoek. In hoofdstuk 4 wordt aandacht besteed aan de interviews. In hoofdstuk 5 worden de resultaten beschreven. In hoofdstuk 6 wordt aandacht besteed aan de optimalisatie van de informatie-uitwisseling. In hoofdstuk 7 wordt de conclusie van dit onderzoek gepresenteerd. In hoofdstuk 8 wordt de discussie over dit onderzoek beschreven.

[1] Een internetknooppunt is veelal een organisatie die haar klanten een netwerk-platform biedt waarop de aangesloten partijen IP-verkeer met elkaar kunnen uitwisselen.

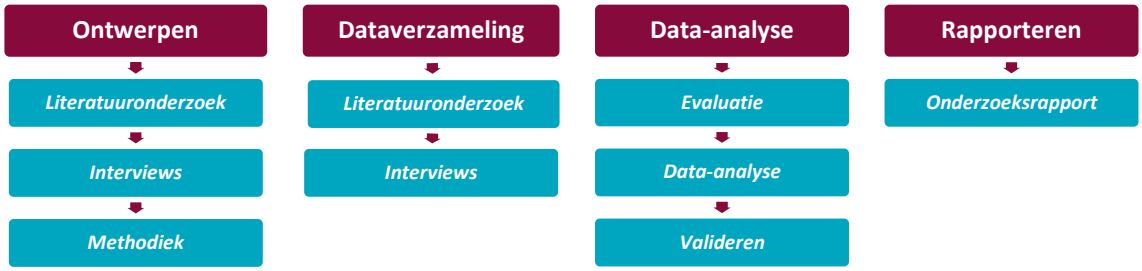
2 METHODIEK

In het voorgaande hoofdstuk is beschreven: het kader waarbinnen dit onderzoek is verricht. In dit hoofdstuk wordt beschreven hoe het onderzoek is uitgevoerd. De methodiek heeft als doel het onderzoek te reproduceren en de gemaakte keuzes binnen het onderzoek te verklaren.

Met dit hoofdstuk wordt de fase ontwerpen voortgezet. Methodiek is een onderdeel van de fase ontwerpen.

2.1 ONDERZOEKSOPZET

De fasen van het onderzoek die in dit hoofdstuk worden beschreven zijn gebaseerd op het boek: *Wat is onderzoek?* (Verhoeven, 2014). Het boek is een heldere inleiding in methoden en technieken van onderzoek. De nadruk ligt op het verrichtten van praktijkonderzoek, waarvan alle fasen worden doorlopen.



Afbeelding 1: Onderzoeksopzet

In de fase ontwerpen worden de aanleiding, probleemstelling en vraagstelling geformuleerd, en de kaders en aanpak van het onderzoek bepaald. De probleemanalyse is aan de hand van literatuuronderzoek en interviews geïdentificeerd. Vervolgens is de aard van het onderzoek vastgesteld. Dit onderzoek heeft een kwalitatief karakter. Hiervoor is gekozen om inzichten te verkrijgen in de verschillende interpretaties en opvattingen die de respondenten hebben over het model.

De methoden die zijn gehanteerd zijn literatuuronderzoek en interviews met experts op het terrein van cybersecurity. Voor literatuuronderzoek is gekozen om inzicht te verkrijgen in wat er in de literatuur staat beschreven. Voor interviews is gekozen om inzichten te verkrijgen in de meningen en opvattingen van respondenten.

In de fase dataverzameling wordt data verzameld ter beantwoording van de vraagstelling. De methoden die worden gebruikt voor het verzamelen van de data zijn literatuuronderzoek en interviews. In hoofdstuk 3 wordt de methode van het literatuuronderzoek inhoudelijk beschreven, hetzelfde geldt voor de interviews in hoofdstuk 4.

In de fase data-analyse wordt de verkregen data uit de dataverzameling geanalyseerd. Als eerste wordt de verzamelde data en de verkregen inzichten geëvalueerd. De evaluatie vindt plaats om te beoordelen of bijsturing van dit onderzoek nodig is. Vervolgens wordt op basis van de data-analyse een concept-model ontwikkeld. Het concept-model wordt vervolgens geverifieerd en gevalideerd bij stakeholders.

In de fase rapporteren wordt het onderzoeksrapport opgesteld. Hierin worden de fasen zoals hierboven beschreven gerapporteerd. Het onderzoeksrapport zal onder andere de aanpak, resultaten en conclusie en aanbevelingen van dit onderzoek bevatten.

2.2 BETROUWBAARHEID EN VALIDITEIT

Betrouwbaarheid is de mate waarin beïnvloeding van fouten en toevalligheden worden uitgesloten of gereduceerd. Bij de uitvoering van dit onderzoek zijn maatregelen getroffen om de betrouwbaarheid te waarborgen.

Binnen dit onderzoek worden methodische triangulatie en data-triangulatie toegepast om de betrouwbaarheid en validiteit van de onderzoeksresultaten te vergroten. Bij de methodische triangulatie worden verschillende dataverzamelingsmethoden toegepast. In dit onderzoek is dat, zoals aangegeven, literatuuronderzoek en interviews.

Bij data-triangulatie worden verschillende databronnen gebruikt. Binnen dit onderzoek worden onder andere de databronnen, zoals aangegeven, literatuuronderzoek en interviews gebruikt.

Om de betrouwbaarheid van dit onderzoek te waarborgen heeft de onderzoeker literatuur van de aangeleerde methoden over het uitvoeren van onderzoek en technieken voor het verzamelen van data uit de studie doorgenomen. In de aanloop naar dit onderzoek heeft de onderzoeker meermaals volgens deze methoden en technieken onderzoek uitgevoerd en interviews afgenomen.

Ter voorbereiding op de interviews heeft de onderzoeker een interviewtraining gevolgd bij het Centre of Expertise for Cyber Security (CoECS), waardoor de interviewvaardigheden zijn verbeterd.

De onderzoeker heeft ook gereflecteerd op zijn positie als interviewer. Dit leidde tot het inzicht dat het lid zijn van de Young Professionals Commissie van het Platform van Informatiebeveiliging (PvIB), de dataverzameling mogelijk kan beïnvloeden. De onderzoeker heeft door zijn lidmaatschap aan het PvIB een netwerk opgebouwd in de cybersecurity. Het lid zijn van de Young Professionals Commissie van het PvIB kan leiden tot willekeur en/of selectieve waarneming. Om dit te voorkomen is de onderzoeker waakzaam tijdens de interviews op het herkennen en doorvragen van uitspraken. De onderzoeker bespreekt twee transcript met zijn begeleider om te beoordelen of er sprake zou zijn geweest van willekeur en/of selectieve waarneming.

2.3 ONDERZOEKSBEPERKINGEN

Het onderzoek kent een aantal beperkingen. Het onderzoekstermijn is vastgesteld op 17 kalenderweken. Hierdoor is er een beperking in het aantal interviews dat kan worden afgenomen. Voor het onderzoek zal dit betekenen dat de respondenten, in de aangewezen periode voor dataverzameling, beschikbaar dienen te zijn. Als blijkt dat dit niet het geval is kunnen meningen en opvattingen van respondenten eenzijdig zijn.

Daarnaast bestaat de onderzoekspopulatie uit het mkb en specifiek de datacenterbranche in het mkb. Hierdoor kunnen alleen uitspraken worden gedaan over de informatiebehoefte die de datacenterbranche in het mkb toekent aan de kennisdeling en informatie-uitwisseling met betrekking tot cybersecurity.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel methodiek en de fase ontwerpen afgerond. In het voorgaande hoofdstuk zijn de onderdelen literatuuronderzoek en interviews beschreven. In het komende hoofdstuk wordt het onderdeel literatuuronderzoek beschreven. Hiermee wordt de fase dataverzameling gestart.

Afbeelding 2: ***Voortgang onderzoek***

3 LITERATUURONDERZOEK

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht en de onderzoeksopzet. In dit hoofdstuk wordt het literatuuronderzoek beschreven. Het literatuuronderzoek heeft als doel uitleg te geven over bepaalde begrippen en tot inzichten komen ter beantwoording van de vraagstelling.

Met dit hoofdstuk wordt de fase dataverzameling gestart. Het literatuuronderzoek is een onderdeel van de fase dataverzameling.

3.1 METHODE

Het literatuuronderzoek wordt verricht aan de hand van de BIG6 methode. De BIG6 methode is ontwikkeld door Mike Eisenberg and Bob Berkowitz en wordt wereldwijd toegepast om methodisch informatie te verkrijgen (BIG6, 2017). De BIG6 methode kent zes stappen die moeten worden gevolgd tijdens het zoekproces.

Afbeelding 3: De BIG6 methode

In de taakdefinitie wordt de zoekopdracht gedefinieerd. Als duidelijk is naar welke informatie je zoekt wordt de zoekstrategie bepaald. Hierin wordt de zoekplaats bepaald dat wil zeggen wat eventueel de geschikte informatiebronnen zouden kunnen zijn. Wanneer de informatiebronnen zijn geselecteerd wordt de zoekplaats vastgesteld. Hierin staat de vraag centraal waar de juiste informatie kan worden gevonden in de databron. Als de zoekplaats is vastgesteld moet de relevantie van de data worden bepaald. Het gaat binnen het bepalen van de relevantie om de data te bestuderen, te vergelijken en te bekritiseren. Als relevante data is geselecteerd dan volgt het organiseren en verwerken van de data. Hierbij gaat het erom dat de data wordt verwerkt waarmee de doelstelling van het literatuuronderzoek wordt behaald. In dit onderzoek is dat het tot inzicht komen voor de beantwoording van de vraagstelling.

De BIG6 methode adviseert om een logboek bij te houden om databronnen vast te leggen. De onderzoeker heeft besloten dit niet te doen, maar om de databronnen direct in te voeren in een tekstverwerker. Hierdoor worden databronnen effectief en efficiënt verwerkt. Nadien kan worden geverifieerd of er een verwijzing is naar de databronnen.

Dit onderzoek kan gebruik maken van primaire en secundaire bronnen (RUG, 2017). Als primaire bronnen worden onder andere maar niet uitsluitend wetenschappelijke publicaties, grijze literatuur en websites gecategoriseerd. Als secundaire bronnen worden onder andere rapporten, handboeken en naslagwerk gecategoriseerd.

Literatuuronderzoek wordt meermaals toegepast. Het eerste literatuuronderzoek is uitgevoerd om de probleemanalyse vast te stellen. Het tweede literatuuronderzoek, dat hieronder wordt beschreven, is uitgevoerd om data te verzamelen.

De inzichten waar dit literatuuronderzoek toe moet leiden is een verdieping geven over de versnippering van initiatieven in Nederland, zoals wordt gesteld in het rapport *"Nederland digitaal droge voeten"*. Ook zal ketenverantwoordelijkheid, de definitie van het midden- en kleinbedrijf (mkb) en de kenmerken van samenwerken in dit literatuuronderzoek worden beschreven.

3.2 DATA-ANALYSE

In deze paragraaf wordt de data-analyse uitgevoerd over het literatuuronderzoek. Als eerste zal worden ingegaan op: de versnippering van initiatieven op het gebied van cybersecurity in Nederland. Gevolgd door: de ketenverantwoordelijkheid in de digitale keten aan bod komen, het begrip midden- en kleinbedrijf (mkb) en tot slot de kenmerken van samenwerking worden beschreven.

3.2.1 VERSNIPPERING VAN INITIATIEVEN

Op verzoek van de Cyber Security Raad (CSR) heeft mevrouw Herna Verhagen, CEO PostNL onafhankelijk onderzoek[2] gedaan naar de stand van zaken in Nederland op het gebied van cybersecurity. Het onderzoek concludeert dat Nederland een versnippering kent waardoor het onduidelijk is welke partijen voor welke taak verantwoordelijk is.

> *"Dat de overheid een cruciale rol heeft in de digitale wereld is […] voor iedereen duidelijk. Maar de invulling ervan is nog niet uitgekristalliseerd. Dat heeft geleid tot een beperkte coördinatie en sturing. Ook is er sprake van versnippering over een groot aantal ongelijksoortige partijen."* (Verhagen, 2016, p. 25)

De overheid heeft een beperkte coördinatie en sturing op het gebied van cybersecurity. Dit komt omdat ten minste vijf departementen een beleidsverantwoordelijkheid voor ICT en specifiek voor cybersecurity kennen. Bovendien stelt hetzelfde onderzoek dat een tal van agentschappen, zelfstandige bestuursorganen (ZBO's) en toezichthouders actief zijn op dit thema. Een consequentie hiervan is dat de informatie-uitwisseling tussen overheidspartijen onderling en tussen private partijen en overheden onvoldoende is geborgd.

> *"Door versnippering verliest men zicht. Bovendien is onduidelijk welke partijen voor welke taak verantwoordelijk is, en blijft vaak onzichtbaar wat gebeurt aan opvolging. Budgetten zijn versnipperd."* (Verhagen, 2016, p. 26)

[2] De economische en maatschappelijke noodzaak van meer cybersecurity, "*Nederland digitaal droge voeten"*, Herna Verhagen (september 2016)

Door de beperkte coördinatie, sturing en versnippering is men het overzicht kwijt. Hierdoor is het mogelijk dat bevoegdheden en of wetgeving gedateerd is. Het risico wat Nederland hierdoor loopt is dat het ten koste kan gaan van zowel de veiligheid als innovatie en onze burgerrechten die wij in Nederland kennen.

> *"Maar er ligt in het digitale domein ook een nadrukkelijke taak voor de overheid waar het gaat om het maatschappelijk belang: het voorkomen en beperken van maatschappelijke ontwrichting in de samenleving, net zoals dat geldt voor de fysieke wereld en infrastructuur."* (Verhagen, 2016, p. 25)

> *"Op sommige terreinen ontbreken bevoegdheden of is wetgeving gedateerd, waardoor de overheid onvoldoende is uitgerust om te zorgen voor detectie en monitoring."* (Verhagen, 2016, p. 26)

Het thema publiek-private samenwerking is erg actueel en de overheid ondersteunt ook initiatieven bij het opzetten van publiek-private samenwerkingsverbanden. Het is belangrijk dat zowel overheid als bedrijfsleven elk hun verantwoordelijkheid nemen. Zonder publiek-private samenwerking is het lastig om als Nederland voorop te blijven in het digitale tijdperk.

> *"Met de doorontwikkeling van de cybersecurityaanpak moet Nederland de volgende stap zetten om in het digitale tijdperk mee te blijven komen. Overheid en bedrijfsleven moeten hierbij elk hun verantwoordelijkheid pakken."* (Rijksoverheid, 2016, p. 5)

In de door staatssecretaris Dijkhoff in 2016 aangegeven cybersecurityaanpak is een aantal concrete acties voortgekomen. Gezien de ernst van de cyberdreigingen zijn deze acties in publiek-private samenwerking opgepakt om Nederland weerbaarder te maken tegen cyberdreigingen. Een van de acties is het verder versterken en uitbouwen van het Nationaal Detectie Netwerk (NDN).

> *"Het kabinet zal, in het licht van de toenemende dreiging, de inzet op het verder versterken en uitbouwen van het Nationaal Detectie Netwerk (NDN) blijven continueren. In het NDN werken het NCSC, de AIVD en MIVD samen om cyberaanvallen op Rijksoverheid en vitale infrastructuur te onderkennen, zodat deze aanvallen sneller aangepakt kunnen worden en de effecten ervan beheersbaar worden gemaakt. Ook worden gegevens uitgewisseld met private partijen."* (Rijksoverheid, 2016, p. 5)

Een andere concrete actie is dat de luchthaven Schiphol en de Rotterdamse haven, twee belangrijke Nederlandse mainports, werken aan het versterken van de digitale keten en erkennen hiermee het belang van cybersecurity voor de regio.

> *"De twee belangrijke Nederlandse mainports, de luchthaven Schiphol en de haven Rotterdam, erkennen het belang van een goed functionerend cybersecurity ecosysteem. Daarom werken zij aan het versterken van de gehele keten, bestaande uit de aan deze mainports verbonden bedrijven en organisaties, op het gebied van digitale veiligheid. Deze initiatieven zijn publiek-private pilots die samen met de NCTV/NCSC worden uitgevoerd."* (Rijksoverheid, 2016, p. 5)

Een andere concrete actie uit de cybersecurityaanpak is dat VNO-NCW / MKB-Nederland en het ministerie van Economische Zaken een verkenning moeten uitvoeren ter versterking van de cybersecurity in het mkb. Een richting waaraan gedacht wordt is een branchegerichte cybersecurityaanpak.

> *"Ook werken VNO-NCW, MKB-Nederland en het ministerie van Economische Zaken aan een plan ter versterking van cybersecurity voor het mkb. Er wordt een branchegerichte cybersecurityaanpak ontwikkeld die het mkb in staat moet stellen haar cybersecurity te versterken. In het algemeen is het mkb beperkt in wat het kan investeren in cybersecurity en heeft het daarom sterke behoefte aan "hapklare brokken"."* (Rijksoverheid, 2016, p. 5)

Een voorlopig resultaat van dit plan is het Digital Trust Centrum (DTC). Momenteel wordt er veelvuldig gesproken over de invulling en positionering van het DTC. Het DTC zal een kennis- en adviescentrum worden die het mkb adviseert en ondersteunt op het gebied van cybersecurity.

> *"Vanuit het mkb wordt dan ook gepleit voor een Digital Trust Centrum. Dit kenniscentrum zou een adviserende en ondersteunende functie kunnen vervullen voor het mkb."* (Munnichs, Kouw, & Kool, 2017, p. 33)

Het rapport "*Nederland digitaal droge voeten"* geeft aan dat eerst de focus gelegd moet worden op de topsectoren en het innovatieve mkb, zowel topsectoren als het innovatie mkb zijn kennisintensieve bedrijven. Kennisintensieve bedrijven kennen een hoog aantal intellectueel eigendom en lopen potentieel meer risico dan het overige bedrijfsleven.

> *"Veel deskundigen adviseren om de ISAC-structuur […] uit te breiden naar andere delen van de economie, met name naar de kennisintensieve bedrijven. De aanwezige samenwerkingsstructuren die bestaan binnen de huidige topsectoren en het innovatie mkb bieden daartoe mogelijk een goede basis."* (Verhagen, 2016, p. 26)

Het Centre for Protection of the National Infrastructure (CPNI.NL) heeft de Information Sharing and Analysis Centres (ISAC's) opgericht en zijn beschikbaar voor de rijksoverheid en vitale sectoren. De ISAC's zijn in 2012 aangesloten op het Nationaal Cyber Security Centrum (NCSC).

> *"ISAC's zijn publiek-private samenwerkingsverbanden en zijn per sector georganiseerd. Hier wisselen de deelnemers onderling informatie en ervaringen uit over cybersecurity. Ook worden analyses gedeeld over de situational awareness in de desbetreffende sectoren. Dit gebeurt met name op tactisch niveau."* (NCSC, 2017)

Naast de luchthaven Schiphol en de Rotterdamse haven deelt ook KPN zijn kennis actief. Zo heeft KPN zijn cybersecuritybeleid gepubliceerd en een CISO-applicatie ontwikkeld. Het bedrijfsleven kan gebruikmaken van de CISO-applicatie om bijvoorbeeld hun eigen beleid te toetsen en cyberdreigingen door te vertalen naar financiële risico's.

> *"Hiermee kunnen securityprofessionals hun eigen beleid eenvoudig schrijven, toetsen en optimaliseren. De app bevat onder andere een mooie feature om de risico's van cyberdreigingen in kaart te brengen en door te vertalen naar financiële risico's. Zo maak je security-issues pas écht goed zichtbaar. Want financiële risico's, dat is een taal die iedereen spreekt."* (Baloo, 2017, p. 1)

3.2.2 KETENVERANTWOORDELIJKHEID

Ketenverantwoordelijk betekent dat inzicht wordt verkregen in de bedrijven en onderdelen die deel uitmaken van het bedrijfsproces. In de afgelopen jaren is een toenemende trend gaande dat bedrijven steeds vaker bedrijfsactiviteiten uitbesteden ten behoeve van het verhogen van de winsten. Dit heeft ertoe geleid dat bedrijfsprocessen steeds complexer zijn geworden doordat ketens nu veelal uit vele schakels bestaan waardoor het overzicht in de keten ontbreekt.

> *"Met ketenverantwoordelijkheid krijg je inzicht in het duurzame gedrag van spelers die deel uit maken van jouw bedrijfsketen."* (MKB-Nederland, 2017)

> *"Bedrijven besteden steeds meer activiteiten uit om kosten te besparen en risico's te spreiden. Dit leidt ertoe dat internationale productie- en toeleveringsketens steeds complexer worden; een product gaat langs vele schakels voordat het bij de eindgebruiker belandt."* (MKB-Nederland, 2017)

Het inzichtelijk maken van het bedrijfsproces wordt zowel door het bedrijfsleven als overheid gedaan. Het bedrijfsleven die maatschappelijk verantwoord wilt ondernemen moet het eigen bedrijfsproces inzichtelijk hebben. Dit is een goed voorbeeld van ketenverantwoordelijkheid.

> *"Als het gaat om de inkoop van (duurzame) grondstoffen, de herkomst van ingrediënten voor de voedingsindustrie of de inhuur van externe medewerkers bestaan al jaren goede voorbeelden van ketenverantwoordelijkheid."* (Verhagen, 2016, p. 38)

In tegenstelling tot het normale bedrijfsproces neemt het bedrijfsleven en overheid nog nauwelijks verantwoordelijkheid voor de digitale keten. Terwijl vergelijkbare initiatieven mogelijk zijn voor de digitale keten.

> *"De Cyber Security Raad constateert dat maar weinig bedrijven en overheden zicht hebben op de digitale ketens waar zij afhankelijk van zijn. Die afhankelijkheid neemt verder toe als gevolg van het 'Internet of Things'."* (CSR, 2016)

> *"Vergelijkbare initiatieven zijn mogelijk voor digitale productieketens. Dat betekent dat alle toeleveranciers, onderaannemers en afnemers die betrokken zijn bij de productieketen, elkaar verantwoordelijk mogen en moeten houden voor een cyber secure keten."* (Verhagen, 2016, p. 38)

Steeds meer ICT-toepassingen zullen met elkaar worden verbonden, dit zal de komende jaren als maar toenemen als gevolg van het Internet of Things (IoT). Zowel het bedrijfsleven als rijksoverheid nemen steeds vaker netwerk gebaseerde oplossingen. Hierdoor geven zij de regie uit handen waardoor het afnemende bedrijf afhankelijk is van de dienstverlener.

> *"Geen enkele organisatie is meer in staat om alle taken zelf uit te voeren. De kwetsbaarheid die deze afhankelijkheid van andere bedrijven en dienstverleners met zich meebrengt, wordt vaak onderschat. De zwakste schakel in de keten kan namelijk voor verstoringen van functies verderop in de keten zorgen."* (Munnichs, Kouw, & Kool, 2017, p. 26)

Vitale sectoren kennen een afhankelijkheid van het bedrijfsleven aangezien zij afhankelijk zijn van toeleveranciers uit het mkb die producten en diensten leveren. Deze afhankelijkheid kan bij vitale sectoren leiden tot maatschappelijke ontwrichting en economische schade.

> *"Bij vitale sectoren kan dat leiden tot vergaande uitval en maatschappelijke ontwrichting. De ketenafhankelijkheid en de daarmee gepaard gaande kwetsbaarheden gelden ook voor digitale diensten voor kleinere gebruikers, zoals webwinkels of mkb-bedrijven."* (Munnichs, Kouw, & Kool, 2017)

In de cybersecurityaanpak worden de cyberdreigingen erkend die digitale ketens met zich meebrengen. In de aanpak is expliciet opgenomen dat de luchthaven Schiphol en de haven Rotterdam de weerbaarheid van de digitale keten moeten verbeteren.

> *"De twee belangrijke Nederlandse mainports, de luchthaven Schiphol en de haven Rotterdam, erkennen het belang van een goed functionerend cybersecurity ecosysteem. Daarom werken zij aan het versterken van de gehele keten, bestaande uit de aan deze mainports verbonden bedrijven en organisaties, op het gebied van digitale veiligheid. Deze initiatieven zijn publiek-private pilots die samen met de NCTV/NCSC worden uitgevoerd."* (Rijksoverheid, 2016, p. 5)

3.2.3 HET MIDDEN- EN KLEINBEDRIJF

Het midden- en kleinbedrijf (mkb) vormt het fundament van de Nederlandse economie. Dit is niet voor iedereen altijd even zichtbaar, omdat het mkb uit zoveel verschillende bedrijven bestaat. Het mkb is vooral belangrijk voor de werkgelegenheid, het biedt werk aan meer dan vier miljoen mensen.

> *"[…] als we van al die midden- en kleinbedrijven één onderneming zouden maken, dan zou die met een omzet van meer dan € 860 miljard in 2015 verreweg het grootste bedrijf van Nederland zijn. Het mkb is vooral belangrijk voor de werkgelegenheid in ons land: het biedt werk aan meer dan vier miljoen mensen. Uit de meest recente cijfers blijkt dat dit belang ook nog toeneemt: het mkb zorgde voor groei van de werkgelegenheid, terwijl die in het grootbedrijf afnam."* (Nederlands Comité voor Ondernemerschap en Financiering, 2016, p. 6)

In 2003 heeft de Europese Commissie (EC) een definitie vastgesteld van middelgrote, kleine en micro-ondernemingen. Deze definitie wordt binnen dit onderzoek gehanteerd, omdat dit de definitie is die door de EC is vastgesteld en dient te worden gehanteerd in de Europese Unie. Het mkb bestaat uit ondernemingen met minder dan 250 werkzame personen. Van alle Nederlandse bedrijven behoort 99% in deze categorie.

> *"Als onderneming wordt beschouwd iedere eenheid, ongeacht haar rechtsvorm, die een economische activiteit uitoefent. Met name worden als zodanig beschouwd eenheden die individueel of in familieverband ambachtelijke of andere activiteiten uitoefenen, personenvennootschappen en verenigingen die regelmatig een economische activiteit uitoefenen."* (Europese Commissie, 2003, p. 4)

De EC heeft twee kenmerken gedefinieerd, namelijk het aantal werkzame personen en financiële drempels, voor het mkb. De kenmerken zijn opgesteld ter bepaling van onder welke categorie het mkb behoort. De EC heeft ook drie categorieën opgesteld. De eerste categorie is een algemene categorie voor kleine, middelgrote en micro-ondernemingen. De tweede categorie is een kleine onderneming. De derde categorie is een micro-onderneming.

> *"1. Tot de categorie kleine, middelgrote en micro-ondernemingen (KMO's) behoren ondernemingen waar minder dan 250 personen werkzaam zijn en waarvan de jaaromzet 50 miljoen EUR of het jaarlijkse balanstotaal 43 miljoen EUR niet overschrijdt."* (Europese Commissie, 2003, p. 4)

> *"2. Binnen de categorie KMO's is een „kleine onderneming" een onderneming waar minder dan 50 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt."* (Europese Commissie, 2003, p. 4)

> *"3. Binnen de categorie KMO's is een „micro-onderneming" een onderneming waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet of het jaarlijkse balanstotaal 2 miljoen EUR niet overschrijdt."* (Europese Commissie, 2003, p. 4)

Het rapport *"De staat van het mkb: Jaarbericht 2016"* van het Nederlands comité[3] geeft aan dat in deze categorieën ook de vier archetypen: zzp'ers, starters, scale-ups en mkb bedrijven met een gevestigde marktposities behoren.

> *"Binnen de grote variatie aan ondernemingen bestaan vier archetypen: zzp'ers, starters, scale-ups en mkb bedrijven met een gevestigde marktpositie."* (Nederlands Comité voor Ondernemerschap en Financiering, 2016, p. 6)

[3] Het Nederlands Comité voor Ondernemerschap en Financiering zet zich in om het groeipotentieel van het midden- en kleinbedrijf met als focus het kleinbedrijf in Nederland te versterken en zal hiertoe haar kennis, ervaring en netwerken inzetten.

3.2.4 SAMENWERKINGSKENMERKEN

Het principe van samenwerken is het verbinden van belangen, in dit onderzoek is het belang de digitale ketens weerbaar maken tegen cyberdreigingen. Samenwerkingsverbanden zijn in algemene zin populair. Dit komt omdat bedrijven enerzijds een belang hebben, binnen dit onderzoek: bij de aanpak om zichzelf weerbaar te maken tegen cyberdreigingen. Anderzijds zijn bedrijven afhankelijk van elkaar omdat de kennis, middelen en bevoegdheden om tot oplossingen te komen verspreid zijn over de verschillende bedrijven (Bruijn, Kickert, & Koppenjan, 1993). Het feit is dat problemen niet meer als verantwoordelijkheid van één bedrijf kan worden gezien, dit illustreert eens te weer de afhankelijkheid van elkaar in de digitale keten.

> *"Problems cannot be solved by organizations on their own. Hence, hierarchy as an organization principal has lost much of its meaning. The model of the 'lonely organization' that determines its policy in isolation is obsolete. Equally obsolete is the image of government at the apex of the societal pyramid"* (Koppenjan & Klijn, 2004)

Volgens Huxham is het succes van samenwerkingsverbanden mede afhankelijk van de mate waarin *collaborative advantage* kan worden gecreëerd. Huxham bedoelt hiermee te zeggen dat bedrijven door samenwerking iets bereiken waartoe zij zelf niet in staat zouden zijn geweest. De definitie die Huxham geeft aan *collaborative advantage* illustreert de wijze waarop het model vormgegeven moet worden.

> *"Collaborative advantage will be achieved when something unusually creative is produced – perhaps an objective is met – that no organization could have produced on its own and when each organization, through the collaboration, is able to achieve its own objectives better than it could alone. In some cases, it should also be possible to achieve some higher-level […] objectives for society as a whole rather than just for the participating organizations"* (Huxham, 1996)

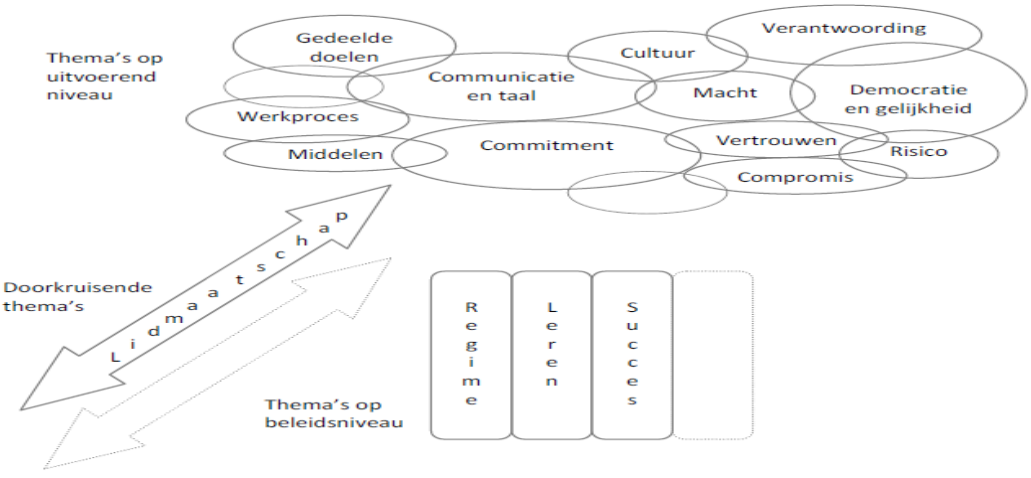
Hoewel de definitie van Huxham een goed uitgangspunt biedt voor de meerwaarde van samenwerkingsverbanden voegt Cropper er een nuance aan toe. Cropper stelt dat niet alleen de uitkomsten van het samenwerkingsverband van belang zijn, maar ook de waarde die aan het samenwerkingsverband wordt gegeven. Cropper heeft het over consequentiële waarde en consituererende waarde. Hiermee verwijst Cropper naar de meerwaarde die ontstaat als gevolg van samenwerken, bijvoorbeeld productiviteit, legitimiteit en efficiëntie. Met constituerende waarde verwijst Cropper naar het gevoel van vertegenwoordiging van het samenwerkingsverband.

> *"[…] organizations can become valued for what they are, and what they represent […] rather than for what, instrumentally, they can do."* (Cropper, 1996)

Het bieden van meerwaarde in complexe samenwerkingsverbanden is niet gemakkelijk, zo blijkt uit de literatuur. Samenwerkingsverbanden zijn van veel factoren afhankelijk die invloed kunnen uitoefenen op het samenwerkingsproces. Als voorbeelden worden de verschillende probleempercepties, oplossingsrichtingen en interpretatie van informatie gegeven die het samenwerken kunnen belemmeren (McGuire, 2006). In een samenwerkingsverband is het van belang dat bedrijven de onderlinge verbinding weten te vinden om de kennisdeling en informatie-uitwisseling succesvol te laten zijn (McGuire, 2006).

Om het samenwerkingsverband in stand te houden is het van essentieel belang dat er vertrouwen is tussen bedrijven onderling en in de afgevaardigde persoon of personen van bedrijven. Zodat er vertrouwen ontstaat dat afspraken worden nageleefd en dat er aan de verwachtingen kan worden voldaan (Vangen & Huxham, 2003) (McGuire, 2006). Factoren die samenwerking bevorderen zijn het tonen van commitment, het ontwikkelen van wederzijds begrip voor posities en belangen, een eerlijke verdeling van werklasten en de omgang met een onduidelijk machtscentrum (Vangen & Huxham, 2003) (Kaarts & Opheij, 2012).

In 2005 hebben Vangen en Huxham nader onderzoek gedaan naar *collaborative advantage* en *collaborative inertia*. Het uitgangspunt was de vraag hoe het mogelijk is dat verschillende samenwerkingsverbanden goed functioneren, terwijl andere samenwerkingsverbanden niet goed functioneren. In de vervolgstudie van Vangen en Huxham hebben zij casestudies en andere wetenschappelijke publicaties geanalyseerd. Deze studie leverde inzichten op die door onderzoekers en respondenten ter sprake worden gebracht met betrekking tot het al dan niet functioneren van de samenwerkingsverbanden. In bijlage I zijn de kenmerken van samenwerkingsverbanden bijgevoegd.



Afbeelding 4: Kenmerken samenwerkingsverbanden (Spoelstra, 2013)

Uit deze studie blijkt dat Vangen en Huxham twaalf kenmerken benoemen die regelmatig genoemd worden als bron van spanning en frustratie binnen samenwerkingsverbanden. De kenmerken kunnen de samenwerkingsverbanden ook een meerwaarde bieden, als deze kenmerken goed worden ingericht. Door respondenten die op beleidsmatig niveau bij de samenwerkingsverbanden zijn betrokken worden nog drie kenmerken benoemd.

Hoewel de kenmerken van Vangen en Huxham niet uitputtend zijn, biedt het inzichten in hoe een samenwerkingsverband vormgegeven zou moeten worden en biedt een kader voor het model.

> *"[…] it allows the material to be researched and presented in manageable chunks, each of which can be considered in isolation from the others, while taking account of the overlap with issues that the others raise."* (Vangen, S.; Huxham, C., 2005)

3.3 CONCLUSIE

Dit hoofdstuk begon met een beschrijving van de methode van het literatuuronderzoek. Vervolgens werd ingegaan op: de versnippering van initiatieven op het gebied van cybersecurity in Nederland. Gevolgd door: de ketenverantwoordelijkheid in de digitale keten, de definitie van het mkb en de kenmerken van samenwerkingsverbanden.

Het doel van dit hoofdstuk was om duiding te geven over bepaalde begrippen en tot inzichten komen ter beantwoording van de vraagstelling.

Nederland kent een versnippering van initiatieven op het gebied van cybersecurity. Uit de analyse blijkt dat er verschillende publiek-private samenwerkingsverbanden zijn en komen, waar het mkb zich kan aansluiten. Het mkb kan aansluiten bij het NDN, de regionale initiatieven, het DTC en/of de topsectoren.

Uit de analyse blijkt dat het bedrijfsleven en rijksoverheid onvoldoende verantwoordelijkheid nemen in de digitale keten. Terwijl er goede voorbeelden zijn van ketenverantwoordelijkheid die wel worden genomen bijvoorbeeld maatschappelijk verantwoord ondernemen.

In 2003 heeft de Europese Commissie (EC) een definitie vastgesteld van middelgrote, kleine en micro-ondernemingen. Tot deze categorie behoren ondernemingen waar minder dan 250 personen werkzaam zijn en waarvan de jaaromzet 50 miljoen euro of het jaarlijkse balanstotaal 43 miljoen euro niet overschrijdt. Deze definitie wordt binnen dit onderzoek gehanteerd, omdat dit de definitie is die door de EC is vastgesteld en dient te worden gehanteerd in de Europese Unie.

Om een samenwerkingsverband succesvol te laten zijn moet het voldoen aan de kenmerken die Vangen en Huxham hebben benoemd. De twaalf kenmerken kunnen zowel de kans op succes als de kans op falen vergroten. De succes- en faalfactoren is een goed uitgangspunt voor de inrichting van het model.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel literatuuronderzoek afgerond. In het voorgaande hoofdstuk is het onderdeel methodiek beschreven. In het komende hoofdstuk wordt het onderdeel interviews beschreven. De fase dataverzameling wordt hiermee voortgezet.

Afbeelding 5 ***Voortgang onderzoek***

4 INTERVIEWS

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht, de onderzoeksopzet en het literatuuronderzoek. In dit hoofdstuk worden de interviews beschreven. De interviews hebben als doel duiding te geven aan bepaalde onderwerpen en tot inzichten te komen voor de beantwoording van de vraagstelling.

Met dit hoofdstuk wordt de fase dataverzameling voortgezet. De interviews zijn onderdeel van de fase dataverzameling.

4.2 METHODE

De interviews die worden verricht zijn semigestructureerd opgezet en worden in persoon afgenomen vanwege de complexiteit van het onderwerp. Tegelijkertijd kan de onderzoeker tijdens het interview de respondent corrigeren wanneer de vraag verkeerd wordt geïnterpreteerd. Tijdens het interview wordt de luisteren, samenvatting en doorvragen (lsd-) methode toegepast.

De lsd-methode houdt in dat wordt geluisterd: de interviewer luistert naar woorden, de manier waarop woorden worden uitgesproken, zowel in toon als volume en kracht als lichaamstaal van de respondent, zowel in houding, gebaren als gezichtsexpressie. Dat wordt samengevat: de interviewer vat in eigen woorden het betoog van de respondent samen om te beoordelen of het betoog heeft begrepen en zo niet, dan heeft de respondent de gelegenheid om aanvulling te doen of zijn betoog te corrigeren. Dat wordt doorgevraagd: de interviewer vraagt door als er sprake is van vaagheden, subjectieve uitlatingen en aannames in het betoog van de respondent om waardevolle informatie te achterhalen en om aan objectieve waarheidsvinding te doen en op deze wijze objectieve informatie los te krijgen.

De respondenten ontvangen voorafgaand aan het interview de topiclist, zodat de respondenten zich kunnen voorbereiden op het interview. Door gebruik te maken van een topiclist (bijlage II) komen in ieder interview dezelfde thema's aan bod. De topiclist wordt voorafgaand aan het verzamelen van de data besproken met de opdrachtgever en begeleider.

De interviews worden opgenomen met een voicerecorder en worden na afloop volledig getranscribeerd (letterlijk vertaald) met behulp van het programma f5transkript. F5transkript maakt het mogelijk interviews efficiënter te verwerken door de opname vertraagd af te spelen. Daarnaast bezit het programma meerdere opties, zoals het automatisch terugspoelen van aantal seconde nadat het fragment is gepauzeerd (F5transkript, 2017).

De respondenten ontvangen het volledig getranscribeerde interview, waarover goedkeuring moet worden verleend om verdere verwerking mogelijk te maken. De semigestructureerde interviews worden na transcriptie uitgewerkt aan de hand van Grounded Theory (Glaser & Strauss, 1999).

Grounded Theory is een benadering die een onderzoeker de mogelijkheid biedt onder de oppervlakte te kijken. In dit onderzoek wordt de Grounded Theory iteratief toegepast, dit betekent dat dataverzameling en data-analyse elkaar afwisselen. Hiervoor is gekozen om tijdens het afnemen van de interviews al een gedetailleerder beeld te vormen over de inrichting van het model.

De voorkeur gaat uit naar een eigen interpretatie van de Grounded Theory om effectiever en efficiënter de transcripten te verwerken. De reden hiervoor is dat de voorkeur is uitgegaan naar het transcriberen van de interviews in plaats van het continu beluisteren van de interviewopname en omdat de eerste twee stappen van de Grounded Theory gecombineerd kunnen worden bij het transcriberen.

Afbeelding 6 Eigen interpretatie Grounded Theory

In de eerste stap wordt open codering toegepast. De transcripten kunnen direct worden doorgenomen en aan relevante fragmenten wordt een code toegekend. Open coderen is het toekennen van woorden aan fragmenten van het interview. Dit kan gedaan worden omdat de interviews al eerder zijn getranscribeerd waardoor op hoofdlijnen bekend is wat de repondenten hebben aangegeven.

In de tweede stap wordt axiale codering toegepast. De open codering wordt doorgenomen en beoordeeld of fragmenten dezelfde codering hebben en beoordeeld waar de verschillen en overeenkomsten zitten. Axiaal coderen is het vergelijken van fragmenten met dezelfde coderingen op verschillen en overeenkomsten.

In de derde stap wordt selectieve codering toegepast. De selectieve codering wordt toegepast om inzicht te verschaffen op uitzonderingen in de axiale coderingen. Selectief coderen is het zoeken naar uitzonderingen op de gevonden coderingen.

In de vierde stap worden de coderingen gerapporteerd. Nu alle relevanten fragmenten zijn voorzien van coderingen is het noodzakelijk om hierover te rapporteren. De gecodeerde fragmenten worden gebruikt om duiding te geven als blijkt dat het noodzakelijk dient te zijn. De coderingen worden overigens niet in een mindmap opgenomen, omdat de onderzoeker de voorkeur geeft gecodeerde fragmenten te gebruiken tijdens de data-analyse, waardoor de toegevoegde waarde van een mindmap verdwijnd.

Het doel van het doorlopen van de Grounded Theory is om theoretische verzadiging te bereiken. Theoretische verzadiging wordt bereikt wanneer het punt is bereikt waarbij geen nieuwe data meer toegevoegd kan worden waardoor de dataverzameling afneemt. Als blijkt dat het verzadingspunt is bereikt worden de interviews alsnog afgenomen. Dit wordt gedaan om toegvalligheden uit te sluiten.

Voor het coderen wordt het programma F4analyse gebruikt. F4analyse biedt de mogelijkheid om transcripten in te voeren en coderingen handmatig te koppelen aan relevante fragmenten (F4analyse, 2017). Daarnaast bezit het programma de opties om de coderingen te exporteren naar meerdere bestandstype.

De interviews met de respondenten worden in geanonimiseerde vorm verwerkt. De reden hiervoor is dat de respondenten vrijuit kunnen spreken zonder rekening te hoeven houden met uitspraken die zij doen, omdat het interview wordt opgenomen op een voicerecorder.

De respondenten zijn experts op het terrein van cybersecurity, op één respondent na. Deze respondent is expert op het terrein van datacenters. De respondenten zijn betrokken bij een vorm van informatie-uitwisseling of dit nu een initiatief, een onderzoek of een facilitator is. Een voorstel van de geselecteerde respondenten is voorgelegd aan de opdrachtgever. De selectie van respondenten is in overleg met de opdrachtgever definitief gemaakt.

De namen en functies van de geselecteerde respondenten worden in eerste instantie niet openbaar gemaakt, tenzij de respondent aangeeft hier geen bezwaar tegen te hebben. Dit is gedaan om de respondenten tijdens het interview vrijuit te kunnen laten spreken, het vertrouwen te geven dat fragmenten niet zonder overleg worden gepubliceerd en om de vertrouwelijkheid van dit onderzoeksrapport tot een minimum te beperken.

Fragmenten uit interviews worden voorafgaand aan de publicatie van dit onderzoeksrapport overlegd met de respondenten. De respondenten krijgen gelijktijdig de vraag voorgelegd of het fragment op naam en functie of geanonimiseerd moet worden verwerkt. Het kan dus zo zijn dat de naam en functie van een of meerdere respondenten bij de fragmenten staan in de uitwerking van de data-analyse. In bijlage III is de lijst van publieke respondenten bijgevoegd.

Na de beoordeling van de onderzoeker worden zowel de bandopnames als de transcripten op verantwoorde wijze verwijderd, waardoor interviewdata definitief is verwijderd.

4.3 DATA-ANALYSE

In deze paragraaf wordt de data-analyse uitgevoerd over de interviews. Als eerste wordt ingegaan op: de kansen en bedreigingen die gepaard gaan met digitalisering. Gevolgd door: de initiatieven waarin veel wordt geïnvesteerd en initiatieven waarvan de toegevoegde waarde al van is bewezen en tot slot op wat de oplossing voor het verbeteren van de informatiepositie van het mkb kan zijn.

4.3.1 DIGITALISERING: KANSEN EN BEDREIGINGEN

Om cybersecurity in een bredere context te plaatsen is binnen de interviews eerst ingegaan op digitalisering, waarbij de nadruk is gelegd op de kansen en bedreigingen die digitalisering met zich meebrengt. De respondenten geven aan dat digitalisering veel kansen biedt voor de positie van Nederland, waar zowel de economie als de samenleving van kan profiteren.

> *"In mijn woorden ongekende kansen. Nederland als economie en samenleving heeft volop geprofiteerd van zijn strategische ligging, in zeg maar het niet-digitale tijdperk. De uitdaging en kansen in één die we nu als land hebben is om dezelfde positie te claimen in de digitale wereld." (A, Paragraaf 2)*

> *"Dat bedrijven, zeg maar, Nederland […] zien als een plek waar je je prima kunt vestigen in het digitale spel. In die zin enable je daarmee, zeg maar, dan maak je het aantrekkelijk voor buitenlandse ondernemingen dan wel Nederlandse ondernemingen om zich hier te vestigen." (E, Paragraaf 6)*

In Nederland ontbreekt het besef dat digitalisering ook een enorme kans meebrengt voor het versterken en verder ontwikkelen van de Nederlandse cybersecurityindustrie, die mede wordt bepaald door het vestigingsklimaat en de strategische ligging van Nederland.

> *"Wat daarbinnen nog in onze optiek ontbreekt is dat het ook een enorme kans geeft aan het ontwikkelen van een cybersecurityindustrie. Dat biedt vanuit cybersecurity perspectief wellicht aanleiding. Dat is iets waarvan wij vinden dat daar nog te weinig aandacht voor is." (Auke Huistra, TNO)*

Naast kansen zijn er bedreigingen die digitalisering met zich meebrengt. Als gevolg van de toenemende digitalisering neemt de frequentie van impactvolle veranderingen toe. Dit heeft effect op de manier hoe mensen leven, maar ook op hoe bedrijfsprocessen worden ingericht.

> *"Er gaat zo-veel veranderen in hoe wij nu als mensen leven, als samenlevingen, economieën draaiend houden en als landen met elkaar omgaan" (A, Paragraaf 6)*

Door de onwetendheid en een gebrek aan vertrouwen bij mensen over digitalisering ontstaat angst voor de adaptatie van nieuwe technologieën die digitalisering meebrengt. Een exemplarisch voorbeeld is de introductie van internetbankieren eind jaren '90. De jongere generatie adopteerde de nieuwe technologie, terwijl de oudere generatie, over het algemeen, terughoudend was in het gebruik.

> *"Door de onwetendheid van die digitalisering zie je heel veel angst ontstaan, […]. Dus er is heel veel angst, terwijl het ook echt heel veel kansen biedt." (Stijn Grove, Dutch Datacenter Association)*

> *"Alleen dan krijg je dus vertrouwen en vertrouwen dat is er op dit moment niet." (Piet Bel, Eindhoven Cyber Security Group)*

In het bedrijfsleven zijn andere bedreigingen dan angst aan de orde. Onwetendheid is ook in het bedrijfsleven aanwezig. Het gaat daarbij niet zozeer over de onwetendheid van nieuwe technologie, maar over de consequentie die digitalisering met zich meebrengt voor het bedrijfsproces.

> *"Een organisatie in het digitale domein bestaat uit heel veel andere organisaties, want je hebt heel veel leveranciers en je hebt heel veel ketenpartners waar je van afhankelijk bent." (E, Paragraaf 38)*

> *"Dat betekent dat eigenlijk, zeg maar, het kritische bedrijfsproces, dat is niet alleen afhankelijk van wat zij zelf doen, maar is ook sterk afhankelijk van wat anderen doen." (E, Paragraaf 38)*

Door deze verbondenheid is geen enkele organisatie meer in staat om alle taken zelf uit te voeren. Dit vergt een nieuwe aanpak om digitale ketens weerbaar te houden, omdat het bedrijfsleven moet samenwerken. Het bedrijfsleven heeft door de afhankelijkheid in de digitale keten een nieuwe vorm van ketenverantwoordelijkheid, waarbij het bedrijfsleven een gezamenlijke verantwoordelijkheid heeft om de weerbaarheid van de digitale keten te waarborgen.

Cyberdreigingen kunnen bewaarheid worden als het bedrijfsleven de weerbaarheid in de digitale keten niet op orde heeft. Voorbeelden van cyberdreigingen zijn: phishing, malware, hacking, cyberspionage en –diefstal en kunnen leiden tot verstoring van bedrijfsprocessen maar ook van de digitale samenleving met potentiële effecten.

> *"Dan heb je het nog niet over het misbruiken van data of het beïnvloeden van verkiezingen, wat recent natuurlijk heel actueel is geweest. Zo zijn meerdere invloeden op die digitale samenleving of bedreigingen zijn daar mogelijk. Daar zijn meerdere voorbeelden van in de wereld te zien." (Auke Huistra, TNO)*

De mate van weerbaarheid van digitale ketens draagt bij aan het vertrouwen in digitalisering en daarmee nieuwe technologieën. Bij het waarborgen van vertrouwen en het benutten van de kansen hoort ook het nemen van verantwoordelijkheid.

> *"Bij het benutten van de kansen hoort ook het nemen van je verantwoordelijkheid op de nieuwe type dreigingen die met de kansen gepaard gaan." (A, Paragraaf 8)*

4.3.2 INITIATIEVEN: NIEUW EN BESTAAND

Rondom Informatie-uitwisseling met betrekking tot cybersecurity zijn behoorlijk wat acties gaande. Het kabinet heeft vorig jaar toegezegd voor de komende vijf jaar, 55 miljoen euro te investeren in het NDN (Security.nl, 2017).

Het NDN wordt als samenwerkingsverband gezien voor het effectief en efficiënt waarnemen van cyberdreigingen en cyberrisico's en erover te waarschuwen. Het NDN wordt gezien als centraal middelpunt voor het delen van dreigingsinformatie.

"Maar je ziet bij het NCSC natuurlijk ook het Nationaal Detectie Netwerk. Eigenlijk, is dat ook een samenwerkingsverband. Wat je eigenlijk doet, […]. Als je hier het NDN hebt en hier heb je allemaal organisaties." (E, Paragraaf 78)

Het delen van dreigingsinformatie gebeurt vanuit het NDN richting de bedrijven die zijn aangesloten. De voorwaarde is dat een bedrijf de beschikking heeft over een Security Operations Centre (SOC) en behoort tot de doelgroep van het NCSC.

"Die organisaties hebben allemaal een SOC en wat je eigenlijk doet is, je verbindt die SOC's met elkaar. Even heel makkelijk gezegd." (E, Paragraaf 78)

Het NCSC beschikt ook over ISAC's. De oprichting van de ISAC's is ongeveer tien jaar geleden begonnen. Bij de oprichting is ook internationaal gekeken wat voor initiatieven er rondom informatie-uitwisseling waren. Het Engelse, CPNI-model en het Amerikaanse, ISAC model zijn destijds met name bestudeerd.

"Het ISAC's traject is gestart zo'n beetje 10 jaar geleden, denk ik. Destijds bij de ICTU, gefinancierd door het Ministerie van Economische Zaken." (Auke Huistra, TNO)

"Daar is toen met name gekeken naar het Engelse model, het CPNI model. Die hadden een model voor Information Exchanges. En er is ook gekeken naar het Amerikaanse model, het ISAC model." (Auke Huistra, TNO)

De ISAC's zijn uiteindelijk als publiek-private samenwerkingsverbanden opgezet waarbij is gekozen voor een sectorale aanpak. De gehanteerde aanpak komt overeen met het CPNI model, maar de Amerikaanse term wordt in Nederland gehanteerd.

"Het verwarrende is dat we eigenlijk het model uit Engeland gekopieerd hebben, maar de Amerikaanse term gebruiken" (Auke Huistra, TNO)

In Nederland zijn de ISAC's vrij succesvol gebleken. Dit komt mede door de sectorale aanpak waarvoor gekozen is, omdat bedrijven in een specifieke sector veelal gebruik maken van overeenkomstige IT-systemen.

"En ISAC's zijn uiteindelijk vrij succesvol gebleken" (Auke Huistra, TNO)

"Wat in het verleden gedaan is: ze hebben de ISAC's opgericht, gedifferentieerd naar sectoren. En waarom is dat wel aardig om in een sector te doen, omdat bijvoorbeeld drinkwaterorganisaties, hebben in bepaalde mate, gebruiken ze overeenkomstige systemen" (E, Paragraaf 12)

Daarentegen moet een kanttekening worden geplaatst bij de meerwaarde en functioneren van afzonderlijke ISAC's. Dit is een goede aanleiding om de ISAC's te evalueren.

"Je kunt ze niet echt vergelijken met elkaar. Dat heeft met de, wat ik zojuist ook al zei, […] de ene sector is veel meer IT-driven dan de andere sector." (E, Paragraaf 34)

"Uiteindelijk is het ook wat ze zelf willen." (E, Paragraaf 34)

"Wij proberen natuurlijk wel een beetje mee te sturen en te helpen, maar ze moeten uiteindelijk wel hun eigen broek ophouden." (E, Paragraaf 34)

In de cybersecurityaanpak (Rijksoverheid, 2016) zijn een aantal concrete acties beschreven. Een van deze acties was dat de luchthaven Schiphol en de Rotterdamse haven, twee belangrijke Nederlandse mainports, werken aan het versterken van de digitale keten in de regio.

Het resultaat van deze actie is de totstandkoming van twee regionale initiatieven die werken aan de cybersecurity in de regio. Ook in Eindhoven is een regionaal initiatief opgericht. Deze regionale initiatieven zijn top-down gedreven opgericht, zowel de behoefte als de noodzaak zijn top-down gedreven.

"Dat is een hele interessante. […] Er is zoiets als de Eindhovensche Fabrikantenkring, dat zijn de CEO's en algemeen directeuren van de Eindhovense bedrijven. […] We zijn gewoon begonnen op aandringen van de CEO's, niet op aandringen van de technische afdeling." (Piet Bel, Eindhoven Cyber Security Group)

"Het is met name onze burgemeester geweest, Aboutaleb. Hij (Aboutaleb, red.) zei van cybersecurity, digitale veiligheid, op een gegeven moment kwam het onderwerp steeds vaker aan bod. […]. Dus hij (Aboutaleb, red.) is eigenlijk degene die het op tafel heeft gelegd tijdens het driehoeksoverleg. […]. Die hebben eigenlijk met zijn drieën de knoop doorgehakt van daar gaan we iets mee doen. (Sarah Olierook, Port of Rotterdam)

De benadering om de doelgroep te bereiken wordt op eenzelfde manier vormgegeven. Het is daarbij zo dat de grote bedrijven uit de regio de kleinere bedrijven helpen.

"De grote helpen de kleinere met best practices, tips en incidenten" (Piet Bel, Eindhoven Cyber Security Group)

Daarnaast benaderen de regionale initiatieven de doelgroep vanuit een positieve insteek. De aanpakken zijn overeenkomstig aan elkaar. De regionale initiatieven hebben lang nagedacht over een duidelijk verhaal waarin hulp en ondersteuning aan de doelgroep voorop staat en wat niet bedreigend is.

"In eerste instantie is veiligheid een thema waar iedereen zijn kaarten graag voor de borst houdt. Je stelt graag vragen over hoe heb jij het voor elkaar maar iets zeggen over jezelf, dat doe je niet snel. Vertrouwen is key." (A, Paragraaf 25)

Naast de overeenkomsten in de benadering komen de instrumenten waarmee de regionale initiatieven de doelgroep bereikt ook overeen. De regionale initiatieven bieden een platform, in de vorm van een website aan en organiseren bijeenkomsten voor de doelgroep, waarvan de duur en frequentie variëren.

> *"Elke twee maanden komen we bij elkaar en daarnaast bellen we regelmatig." (Piet Bel, Eindhoven Cyber Security Group)*

> *"Dat verschilt. Destijds was het een keer in de zes tot acht weken. Tegenwoordig hebben ze een beetje een mix van fysieke bijeenkomsten en teleconferenties. Het hangt heel erg van de sector af. De ene sector komt vaker bij elkaar dan de andere sector." (Auke Huistra, TNO)*

> *"Hopelijk op termijn wellicht, daar zijn we nu nog niet, een soort van beveiligde login, een soort platform gaan bieden waar bedrijven elkaar ook kunnen gaan vinden." (Sarah Olierook, Port of Rotterdam)*

De doelgroep wordt op overeenkomstige manier geselecteerd. De doelgroepen kenmerken zich door locatie en/of regio waar het zich bevindt.

> *"Bedrijven die werkzaam zijn op Schiphol. Die vormen met elkaar het ecosysteem waarmee wij "veiligheid synergie" willen halen in CYSSEC: samen sterker, samen veiliger. Dat zijn eigenlijk de randen van wat CYSSEC is." (A, Paragraaf 18)*

> *"Nee, we hebben in principe gezegd al onze klanten in het Rotterdamse havengebied en gebruikers, dus binnenvaart, scheepvaart. Jullie zitten in onze doelgroep." (Sarah Olierook, Port of Rotterdam)*

De doelgroep kan zich aansluiten bij een regionaal initiatief, waardoor zij toegang krijgen tot de informatie. De regionale initiatieven bieden verschillende soorten publieke informatie aan van bijvoorbeeld het NCSC en/of KPN. Naast publieke informatie bieden de regionale initiatieven ook vertrouwelijke informatie bijvoorbeeld over casussen en cyberaanvallen die gepleegd zijn binnen bedrijven. Eén regionaal initiatief heeft een interessante opvatting over het aanbieden van informatie. De informatie wordt namelijk via Gartner's Adaptive Security Architecture (Gartner, 2017) ingedeeld.

> *"De SOC's van de bedrijven delen nu reeds IoC en best practices met elkaar" (Piet Bel, Eindhoven Cyber Security Group)*

> *"Ik ga altijd even mijn kapstok van predict, prevent, detect en respond af, want dat is ook de structuur die wij ook intern hanteren." (A, Paragraaf 27)*

Het ontbreekt bij de regionale initiatieven aan het uitwisselen van dreigingsinformatie uit de ISAC's van het NCSC. Terwijl de regionale initiatieven juist behoeften hebben aan dreigingsinformatie die als de code rood, oranje en groen is geclassificeerd.

"Wij hebben dus behoefte aan echte code rood informatie uit het NCSC." (Piet Bel, Eindhoven Cyber Security Group)

Buiten de regionale initiatieven van luchthaven Schiphol, haven Rotterdam en Eindhoven zijn er andere regionale initiatieven actief. Deze regionale initiatieven zijn buiten beschouwing gelaten binnen dit onderzoek.

"Er is een soortgelijk initiatief in Groningen, Twente, Geleen, Rotterdam, Amsterdam, Eindhoven en in de Zorg." (Piet Bel, Eindhoven Cyber Security Group)

Bij de verkenning van VNO-NCW / MKB-Nederland en het ministerie van Economische Zaken, ter versterking van de cybersecurity in het mkb zijn ook de topsectoren aan bod gekomen. Het rapport "*Nederland digitaal droge voeten"* gaf aan dat de focus gelegd moet worden op de topsectoren en het innovatieve mkb.

Bij de oprichting van de topsectoren aanpak zijn, net zoals bij de ISAC aanpak, verschillende internationale modellen bestudeerd. De eerste bevindingen zijn dat het ISAC model, zoals dat werkt voor de vitale sectoren, niet één-op-één zal werken voor de topsectoren. Daarom worden er andere modellen, met name het Information Sharing and Analysis Organization (ISAO) bestudeerd. Het ISAO model is een ander model dan het ISAC model, al heeft het wel bepaalde overeenkomsten in de kenmerken.

"Daarvan hebben wij gezegd dat zou een model zijn wat wel goed zou kunnen passen op topsectoren. Dan zul je het nog wel moeten toespitsen op de Nederlandse situatie. Dat is een slag die nog gemaakt moet worden." (Auke Huistra, TNO)

Een kenmerkend verschil tussen het IASO model en het ISAC model is een centraal punt die de analyse en informatie-uitwisseling voor de doelgroep verzorgd. De schaalbaarheid van het ISAO model is ook een voordeel voor de topsectoren doelgroep.

"Het idee van dat ISAO model is dat er veel meer een fusion centre in het midden zit, die eigenlijk een hoop van de analyse functionaliteit en de informatie-uitwisseling op zich neemt." (Auke Huistra, TNO)

"Dat is ook de enige mogelijkheid om het schaalbaar te maken." (C, Paragraaf 35)

Schaalbaarheid is belangrijk om de doelgroep te kunnen bedienen. Eén van de reden dat het ISAC model niet zal functioneren is, omdat het bij de topsectoren gaat het over een diverse en wisselende verzameling aan bedrijven. In tegenstelling tot de vitale sectoren waarbij het gaat om een redelijk homogene verzameling.

"Niet helemaal, maar omdat topsectoren natuurlijk een heel ander soort verzameling van bedrijven dan de vitale infrastructuur zijn." (C, Paragraaf 18)

"Als je het hebt over topsectoren dan is dat een hele brede groep aan bedrijven die ook nog eens voortdurend wisselt." (C, Paragraaf 18)

Een belangrijk gegeven is dat binnen de topsectoren aanpak ruimte is voor het mkb. Het mkb die behoort tot topsectoren kan zich aansluiten bij de topsectoren aanpak. Bedrijven zijn verbonden aan topsectoren als zij de subsidiemogelijkheden benutten die voor topsectoren zijn vrijgemaakt.

"En dat is bovendien ook van groot tot klein, grote multinationals, maar ook hele kleine mkb-bedrijven die daaraan meedoen." (C, Paragraaf 18)

"Je bent gelieerd aan een topsector als je ook gebruik maakt van de subsidiemogelijkheden die er in de topsectoren zitten." (C, Paragraaf 18)

Bij dezelfde verkenning van VNO-NCW / MKB-Nederland en het ministerie van Economische Zaken, ter versterking van de cybersecurity in het mkb voor de topsectoren is tevens een branchegerichte aanpak bestudeerd.

Hetzelfde principe van de sectorale aanpak bij de ISAC's, geldt ook voor brancheverenigingen. De informatie die wordt verstrekt moet wel relevant zijn. Organisaties in een specifieke sector maken veelal gebruik van overeenkomstige IT-systemen. Bij brancheverenigingen geldt dat bijvoorbeeld dreigingsinformatie specifiek moet worden beschreven naar één of meerdere situatie die voor de branche van toepassing kan zijn is.

"En een geluid wat wij heel erg horen ook vanuit brancheverenigingen, dat als je iets aanlevert aan bedrijven dan moet het echt op maat zijn. Wat betekent dit dan voor mijn specifieke branche." (Tjarda Krabbendam-Hersman, TNO)

Opmerkelijk is wel dat brancheverenigingen weinig aandacht hebben voor cybersecurity. Eén reden kan zijn dat brancheverenigingen niet bewust zijn van de verantwoordelijkheid die het bedrijfsleven heeft met betrekking tot cybersecurity.

"Nou in ieder geval het beeld wat ik nu heb is dat brancheverenigingen veel vragen hebben en dat ze op dit moment niet de kennis hebben op basis waarvan ze zelf maatregelen kunnen nemen." (Tjarda Krabbendam-Hersman, TNO)

De actie die moet worden ondernomen is de brancheverenigingen bewust te maken van de noodzaak van cybersecurity en te informeren over wat zij kunnen bijdragen.

"Het gaat dan in eerste instantie om het bijpraten en informeren van bedrijven van wat cyberdreigingen zijn en bijvoorbeeld het maken van risicoanalyses per sector." (Tjarda Krabbendam-Hersman, TNO)

Daar staat tegenover dat een aantal brancheverenigingen de verantwoordelijkheid op zich hebben genomen en informatie delen. Het aantal brancheverenigingen is minimaal en zal op redelijk termijn moeten toenemen.

> *"Ja, absoluut. Wij delen kennis op verschillende manier." (Stijn Grove, Dutch Datacenter Association)*

4.3.3 DE OPLOSSING VOOR HET MKB

Voor het creëren van een verbeterde informatiepositie voor het mkb is er niet een absolute oplossing in de vorm van één initiatief die de volledige informatie-uitwisseling omvat. Het is belangrijk dat de oplossing in een publiek-private samenwerking zal worden opgezet. Het doel zou moeten zijn om een landelijk dekkend stelsel te vormen van initiatieven waar het mkb zich kan aansluiten.

> *"Want je hebt een goed verhaal van je hebt niet een model. Wat wij ook zeggen is dat als je informatiedeling wilt opstarten kan je dat op meerdere manieren doen. Je kan dat per keten doen, per sector of per branche." (Tjarda Krabbendam-Hersman, TNO)*

> *"Het mooiste is als een soort van grid krijgt waarin partijen die zeg maar verbonden zijn […] gebruik kunnen maken van allerlei dienstverlening die met een bepaalde manier aan elkaar vast zit." (E, Paragraaf 50)*

Bij het vormen van een landelijk dekkend stelsel is het belangrijk dat er een inventarisatie wordt gedaan van bestaande initiatieven. Op basis van deze inventarisatie kan worden beoordeeld bij welke initiatieven energie zit en welke kunnen bijdrage aan het doel.

> *"Wat ik voornamelijk belangrijk vind dat er heel erg gekeken moet worden naar reeds bestaande situaties." (Stijn Grove, Dutch Datacenter Association)*

> *"Wil je heel Nederland dekkend krijgen dan moet je denk ik starten, daar waar al energie zit. Dat is onze ervaring in ieder geval. Daar waar al iets van actie is en dat zou dan kunnen gaan werken als een olievlek." (Tjarda Krabbendam-Hersman, TNO)*

Organisaties die momenteel ook betrokken zijn bij de informatie-uitwisselingen zouden een rol op zich moeten nemen. Ook organisaties als het Openbaar Ministerie, de Kamer van Koophandel (KvK) en de Veiligheidsregio's worden incidenteel benoemd. Daarnaast worden met regelmaat initiatieven als de regionale initiatieven en topsectoren benoemd.

> *"Dat zijn denk ik partijen die daar nu ook al mee bezig zijn zoals VNO-NCW, VenJ, EZ, brancheverenigingen, maar ook de AIVD en Politie zijn partijen die daarbij betrokken veelal zijn er wel bij betrokken. Dus alleen nog niet in een samenhangend model op dit moment." (Tjarda Krabbendam-Hersman, TNO)*

> *"Je zult iets als topsectoren moeten gaan doen, iets als regio's moet gaan doen, iets als multinationals moet gaan doen." (D, Paragraaf 48)*

Belangrijk is wel dat binnen het landelijk dekkend stelsel op eenzelfde manier informatie wordt gedeeld. Randvoorwaarden zouden hiervoor moeten worden opgesteld om het vertrouwen te waarborgen. Het Traffic Light Protocol (TLP) van het NCSC zou een manier kunnen zijn om informatie in vertrouwen te delen. Een voorwaarde zal wel moeten zijn dat informatie kan worden gerubriceerd om deze informatie uit te wisselen.

> *"Het belangrijkste daarvoor is het gebruik van dat Traffic Light Protocol, waarbij organisaties aan kunnen geven onder welke kleurcodering die informatie gedeeld gaat worden. Waarbij het onderlinge vertrouwen bestaat dat de andere deelnemers daar ook rekening mee houden" (Auke Huistra, TNO)*

> *"Vertrouwen creëer je door met elkaar een aantal afspraken op papier te zetten." (E, Paragraaf 18)*

Een ander aspect van het landelijk dekkend stelsel is toegankelijkheid. De toegankelijkheid kan op twee manieren worden geïnterpreteerd: zichtbaarheid en financieel. Het mkb zal wel kennis moeten krijgen van de mogelijkheden die worden aangeboden. Ook zal een financiële bijdrage drempelverhogend werken voor het mkb.

> *"Ik zie een model wat je eigenlijk, wat eerder jou vindt dan dat jij het model vindt." (A, Paragraaf 53)*

> *"Ik denk het een groot, een kant waar je niet op moet is daar van dag één heel veel geld voor vragen. Want dat zal namelijk weer tot, dan moet het als je veel geld vraag voor iets wat mensen niet helemaal begrijpen en niet helemaal overzien zal dat simpelweg niet gebeuren. Dus ik zie een model voor mij met een hele lage tot aan nihile instap barrière." (A, Paragraaf 53)*

4.4 CONCLUSIE

Dit hoofdstuk begon met een beschrijving van de methode van de interviews. Vervolgens werd ingegaan op: de kansen en bedreigingen die gepaard gaan met digitalisering. Gevolg door: initiatieven waarin veel wordt geïnvesteerd en/of waarvan de toegevoegde waarde al van is bewezen en wat de oplossing voor het verbeteren van de informatiepositie voor het mkb kan zijn.

Het doel van dit hoofdstuk was om duiding te geven aan bepaalde onderwerpen en tot inzichten komen voor de beantwoording van de vraagstelling.

Door de toenemende verbondenheid die digitalisering met zich meebrengt is het belangrijk dat het vertrouwen in nieuwe technologie wordt gewaarborgd. Bij het benutten van de kansen van digitalisering hoort ook het nemen van verantwoordelijkheid voor nieuwe soorten dreigingen. In bedrijfsprocessen zijn, door de toenemende verbondenheid, afhankelijkheden ontstaan van andere bedrijven waar de weerbaarheid van de digitale keten van afhangt. Het is belangrijk dat het

bedrijfsleven in gezamenlijkheid de verantwoordelijkheid neemt om de veiligheid van de digitale ketens te waarborgen.

Om in gezamenlijkheid de verantwoordelijkheid te nemen is het van belang dat het mkb zich kan aansluiten bij initiatieven. Initiatieven kunnen het mkb helpen en ondersteunen om de weerbaarheid van de digitale keten te verhogen. Uit de analyse is gebleken dat het mkb kan aansluiten bij initiatieven die vanuit de brancheverenigingen, de regio en/of topsectoren zijn georganiseerd.

Aansluiting van het mkb bij deze initiatieven is mogelijk als zij voldoen aan bepaalde voorwaarden. De voorwaarden per initiatief variëren van een lidmaatschap bij een brancheverenigingen tot het werkzaam zijn in een bepaalde regio of het gebruik maken van de subsidiemogelijkheden voor topsectoren. Er zijn nog wel weinig brancheverenigingen die cybersecurity als prioriteit hebben gesteld.

Voor het creëren van een verbeterde informatiepositie voor het mkb is het noodzakelijk dat er initiatieven zijn waar het mkb op kan aansluiten. Zoals uit de bovenstaande analyse blijkt kan het mkb zich bij verschillende initiatieven aansluiten. Het is een illusie te denken dat er een absolute oplossing, in de vorm van één initiatief, is die de volledige informatie-uitwisseling voor het mkb omvat. Het is voor de verbetering van de informatiepositie van belang dat bestaande initiatieven op een effectieve manier gaan samenwerken. Deze collectieve, publiek-private aanpak moet leiden tot een landelijk dekkend stelsel.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel interviews en de fase dataverzameling afgerond. In het voorgaande hoofdstuk is het onderdeel interviews beschreven. In het komende hoofdstuk worden de onderdelen evaluatie en data-analyse beschreven. De fase data-analyse wordt hiermee gestart.

Afbeelding 7: Voortgang onderzoek

5 RESULTATEN EN DATA-ANALYSE

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht, de onderzoeksopzet, het literatuuronderzoek en de interviews. In dit hoofdstuk worden de resultaten beschreven. Het doel van dit hoofdstuk is de data uit de verschillende dataverzamelingsmethode te combineren om te komen tot nieuwe inzichten ter beantwoording van bepaalde deelvragen.

Met dit hoofdstuk wordt de fase data-analyse gestart. De evaluatie en data-analyse zijn onderdelen van de fase data-analyse.

5.1 METHODE

De bevindingen zijn tot stand gekomen door het combineren van de hypothese met het literatuuronderzoek, de interviews en de resultaten van de 0-meting van het Centre of Expertise for Cyber Security van The Hague University of Applied Sciences. Daarnaast is ook een overzicht gemaakt van Nederlandse initiatieven.

De 0-meting bestond uit een enquête om inzicht te krijgen in de huidige situatie met betrekking tot cybersecurity in het mkb. Het onderzoek bestond uit een online vragenlijst die ingevuld moest worden door de directeur en/of eigenaar van het mkb-bedrijf. De online vragenlijst is uitgezet binnen tien verschillende brancheverenigingen. De 0-meting had 441 respondenten. Een publicatie[4] over de resultaten van de 0-meting wordt op een nog nader te bepalen moment verwacht.

Het overzicht van Nederlandse initiatieven is vanuit behoefte aan een overzicht tot stand gekomen, zowel bij het afnemen van de interviews (zie pagina 36) als bij de werkzaamheden voor de Cyber Security Raad. Het overzicht biedt inzicht in de Nederlandse initiatieven die aangemerkt zijn als zichtbaar, betrouwbaar en voldoende bereik hebben. Het gevolg hiervan is dat de lijst niet uitputtend is.

5.2 DATA-ANALYSE

Het bedrijfsleven heeft behoefte aan een verbeterde informatiepositie. Om een verbeterde informatiepositie te bewerkstelligen kan het volwassenheidsniveau van het bedrijfsleven toenemen. Uit de enquête blijkt dat 76,5% van de respondenten aangeeft graag te worden geholpen.

> *"Bent u geïnteresseerd in concrete handvatten om de veiligheid uw IT-gekoppelde bedrijfsvoering te verbeteren?*
>
> *a. Ja (76,5%)*
> *b. Nee (23,5%)"*

[4] Publicatie, *"Cybersecurity in het mkb"*, R.J. Notté en L.K. Slot, Centre of Expertise for Cybersecurity (verwacht 2017)

De manier waarop de informatie-uitwisseling tot stand zou moeten komen, blijkt dat 82,5% van de respondenten een voorkeur geeft aan een brancheverenigingdie het bedrijf voorziet van informatie, 19,4% geeft aan via betaalbare commerciële dienstverleners en 18,4% via een landelijke website.

> *"Zo ja, via welke weg kan dit het best aangeboden worden <meerdere antwoorden mogelijk>:*
>
> *a. Branche vereniging (82,5%)*
> *b. Landelijke website (18,4%)*
> *c. Concullega's (4,9%)*
> *d. Een lokale helpdesk (9,7%)*
> *e. Betaalbare commerciële partijen (19,4%)*
> *f. Anders, namelijk (7,3%)"*

Het bedrijfsleven, met name het mkb, heeft behoefte aan voorlichting op het gebied van cybersecurity, bedrijfsanalyses en penetratietesten. Uit de enquête blijkt dat 59,9% van de respondenten aangeeft graag voorlichting te willen ontvangen. Opmerkelijk is dat 33,2% van de respondenten aangeeft behoefte te hebben aan een online helpdesk functionaliteit.

> *"In welke vorm zou u de handvatten willen krijgen om uw bedrijfsvoering veiliger te krijgen <meerdere antwoorden mogelijk>*
>
> *a. (Gratis) tools zoals virusscanners (38,1%)*
> *b. Betaalde tools (zoals virusscanners) (20,8%, n=72)*
> *c. Voorlichting (59,9%)*
> *d. Life cursus (17,3%)*
> *e. Digitale cursus (20,3%)*
> *f. Een inloopspreekuur (4,0%)*
> *g. Een balie (3,5%)*
> *h. Een online vraagbaak (33,2%)*
> *i. Een telefonische vraagbaak (17,3%)*
> *j. Een expertgesprek (27,8%, n=72)*
> *k. Een bedrijfsanalyse (43,1%, n=72)*
> *l. Een penetratietest (43,1%, n=72)*
> *m. Anders, namelijk…. (8,9%)"*

Het overzicht van Nederlandse initiatieven bevestigt het beeld van het rapport *"Nederland digitaal droge voeten"* dat Nederland een versnippering in de informatie-uitwisseling kent.

> *"De kaart bevestigt de versnippering in de informatie-uitwisseling met betrekking tot cybersecurity en cybercrime in Nederland. In rapport Verhagen werd eerder al aandacht besteedt aan de versnippering. De huidige informatie-uitwisseling is hoofdzakelijk gericht op de Rijksoverheid en organisaties in de vitale infrastructuur."*

Naast de brancheverenigingen, regionale initiatieven en topsectoren zijn er verschillende soorten initiatieven in Nederland. Deze initiatieven variëren van doelgroep, informatieniveau en informatiedeling. Het bedrijfsleven kan zich aansluiten, de voorwaarde is meestal wel dat het bedrijf lid moet zijn van een beroepsvereniging of een koepelorganisatie.

> *"Er wordt zeker ook informatie gedeeld met het bedrijfsleven buiten de vitale infrastructuur. Voorwaarde is dan meestal wel dat je lid moet zijn van een beroepsvereniging (bijv. PvIB, NOREA) en of koepelorganisatie (bijv. VNO-NCW). Het aantal brancheorganisaties dat een actieve bijdrage levert aan cybersecurity en preventie van cybercrime is bescheiden."*

Publiek-private samenwerkingen worden hoofdzakelijk door de rijksoverheid geïnitieerd. Dit beeld komt overeen met de in 2016 aangegeven cybersecurityaanpak en de concrete acties die hieruit zouden moeten voortvloeien.

> *"Publiek-private samenwerkingen worden hoofdzakelijk geïnitieerd door de Rijksoverheid. Deze initiatieven wisselen voornamelijk op operationeel en tactisch niveau informatie uit."*

5.3 BEVINDINGEN

In de hypothese staat beschreven dat het model eenzelfde structuur moet kennen als de ISAC's en dat via de brancheverenigingen het mkb kan worden bereikt. In hoofdstuk 1 is de volledige hypothese terug te lezen.

Het mkb kan via verschillende initiatieven als brancheverenigingen, regionale initiatieven en topsectoren aan dreigingsinformatie en handelingsperspectieven komen. Voor het creëren van een verbeterde informatiepositie voor het mkb is er niet een absolute oplossing in de vorm van één initiatief dat de volledige informatie-uitwisseling omvat.

Daarnaast kan het mkb aansluiten bij verschillende soorten initiatieven in Nederland. Deze initiatieven variëren van doelgroep, informatieniveau en informatiedeling. De voorwaarde is meestal wel dat het bedrijf lid moet zijn van een beroepsvereniging of een koepelorganisatie.

Gedurende dit onderzoek is steeds duidelijker geworden dat er behoefte is aan een landelijk dekkend stelsel van initiatieven waar het mkb zich kan aansluiten. Als gevolg hiervan is de hypothese van dit onderzoek verworpen, omdat het model niet uit één initiatief bestaat, maar uit verschillende initiatieven. Het landelijk dekkend stelsel wordt gevormd door publieke, private, nieuwe en bestaande organisaties, instrumenten en initiatieven.

BELANGRIJKE INFORMATIE

Als gevolg van deze bevinding wordt afstand genomen van de hypothese en zal dit onderzoek worden bijgesteld naar hoe samenwerking de informatie-uitwisseling, met betrekking tot cybersecurity, kan optimaliseren en faciliteren. Ook zal de onderzoekspopulatie worden verruimd van de datacenterbranche naar het mkb.

5.4 ARGUMENTATIE

Het overzicht van Nederlandse initiatieven geeft aan dat er verschillende soorten initiatieven zijn. Het bestaansrecht van deze initiatieven wordt niet in twijfel getrokken. Voor het model kan er niet voldoende regie op de verschillende soorten initiatieven worden uitgevoerd. Of het is zeer arbeidsintensief om inzicht te verkrijgen, bijvoorbeeld welk deel van het bedrijfsleven gebruik maakt van één of meerdere van deze verschillende soorten initiatieven.

Voor het optimaliseren en faciliteren van samenwerking om de informatiepositie van het mkb te verbeteren is het noodzakelijk dat het model overzichtelijk is voor bijvoorbeeld een implementatie voor een proof-of-concept.

Om het overzicht te behouden is besloten met een beperkt aantal initiatieven het model te ontwikkelen. De brancheverenigingen, regionale initiatieven en topsectoren worden bij de ontwikkeling van het model betrokken. De reden hiervoor is dat bij de regionale initiatieven en topsectoren veel energie zit, zoals blijkt uit de data-analyse, waardoor de kans van slagen van het model wordt vergroot.

De brancheverenigingen zijn geselecteerd, omdat het bedrijfsleven veelal is aangesloten bij een branchevereniging. Het bedrijfsleven kan via de branchevereniging worden benaderd. Voor het model kan er voldoende regie op de brancheverenigingen worden uitgevoerd door het betrekken van een schakelorganisatie als VNO-NCW / MKB-Nederland.

Door het betrekken van brancheverenigingen, regionale initiatieven en topsectoren bij de ontwikkeling van het model wordt het bedrijfsleven grotendeels vertegenwoordigd. Wel moet in acht worden genomen dat niet alle Nederlandse bedrijven zijn aangesloten bij een branchevereniging, regionaal initiatief of topsector.

5.4 CONCLUSIE

Door de nieuwe ontwikkeling binnen dit onderzoek zal de aanvankelijke doelstelling niet worden behaald. Daarentegen wordt de doelstelling bijgesteld naar hoe samenwerking de informatie-uitwisseling kan optimaliseren en faciliteren. Deze doelstelling moet leiden tot de optimalisatie van de informatie-uitwisseling, waardoor dit onderzoek meerwaarde biedt ten opzichte van de aanvankelijke doelstelling. Omdat het de volledige informatie-uitwisseling omvat voor het mkb waarbij de gewenste situatie wordt beschreven.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk zijn de onderdelen evaluatie en data-analyse afgerond. In het voorgaande hoofdstuk zijn de interviews beschreven. In het komende hoofdstuk wordt het onderdeel verificatie van de fase data-analyse en het onderdeel onderzoeksrapport van de fase rapporteren beschreven. De fase data-analyse wordt hiermee voortgezet en de fase rapporteren wordt hiermee gestart.

Afbeelding 8: Voortgang onderzoek

6 OPTIMALISATIE VAN DE INFORMATIE-UITWISSELING

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht, de onderzoeksmethode, het literatuuronderzoek, de interviews en de resultaten en data-analyse. In dit hoofdstuk wordt de optimalisatie van de informatie-uitwisseling beschreven. Het doel van dit hoofdstuk is duiding te geven aan hoe samenwerking de informatie-uitwisseling kan optimaliseren en faciliteren.

Met dit hoofdstuk wordt de fase data-analyse voortgezet en de fase rapporten gestart. De verificatie is een onderdeel van de fase data-analyse en onderzoeksrapport is onderdeel van de fase rapporteren.

6.1 ONTWIKKELING

Bij de ontwikkeling van het model is gebruik gemaakt van de resultaten van dit onderzoek en de resultaten van de enquête van het Centre of Expertise for Cyber Security van The Hague University of Applied Sciences.

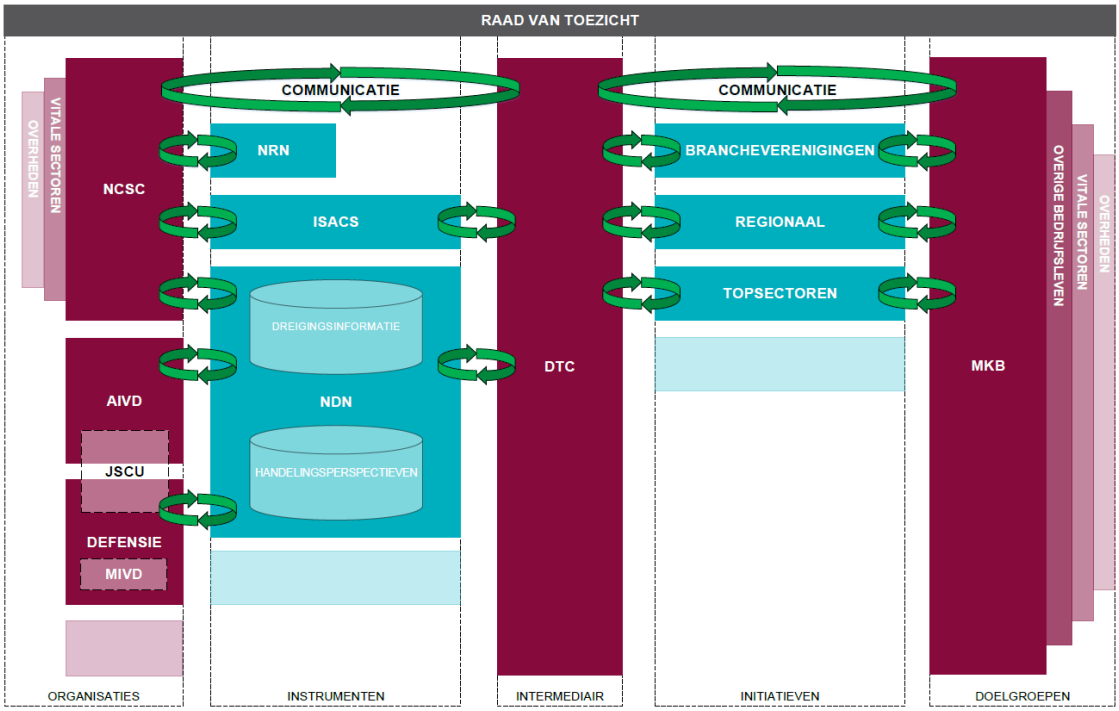
Door het combineren van onderzoeksdata met inzichten die de onderzoeker gedurende dit onderzoek heeft verkregen, is het model ontwikkeld. Er heeft een verificatie en validatie van het model plaatsgevonden. Stakeholders en respondenten hebben feedback geleverd op het concept-model. Deze feedback is verwerkt in het model. De stakeholders waren allemaal experts op het terrein van cybersecurity.

Door de verificatie en validatie zou het model in voldoende mate uitgekristalliseerd moeten zijn, waardoor het model geen radicale wijzigingen meer hoeft te ondergaan. Doordat bijvoorbeeld stakeholders ontbreken, instrumenten en initiatieven niet zijn opgenomen en/of een verschil van inzicht in de inrichting van het DTC.

6.2 OPTIMALISATIEMODEL

Voor het optimaliseren en faciliteren van publiek-private samenwerking is een model ontwikkeld. Het model is ontwikkeld ter optimalisatie van de huidige informatie-uitwisseling. In bijlage IV is het model bijgevoegd.

Binnen het Collaboration Architecture Model of Information Sharing Organizations (CAMISO) is de gewenste situatie beschreven. Er zijn verschillende opties voor wat betreft de inrichting die invloed hebben op zowel de implementatie als de werking van het model. In onderstaande paragraaf zal de keuzemogelijkheid worden gemotiveerd.



Afbeelding 9: Collaboration Architecture Model of Information Sharing Organizations (CAMISO)

6.2.1 INRICHTING MODEL

De verschillende opties komen voort uit de kenmerken waar informatie aan moet voldoen, zoals te lezen is in hoofdstuk 5. De drie kenmerken die worden toegekend aan informatie zijn: toegevoegde waarde, betrouwbaarheid en toegankelijkheid. Als gevolg hiervan zijn er verschillende opties. De opties gaan over het besluit waar de verantwoordelijkheid voor het vertalen van dreigingsinformatie en handelingsperspectieven moet worden belegd.

Dreigingsinformatie en handelingsperspectieven zullen moeten worden vertaald, omdat het bedrijfsleven niet in alle gevallen beschikt over een cybersecurity functionaris. Als gevolg hiervan zal een ICT-medewerker van het bedrijf de dreigingsinformatie en handelingsperspectieven moeten kunnen verwerken. Het is daarom van belang dat dreigingsinformatie en handelingsperspectieven door verschillende (ICT-) functionarissen binnen een bedrijf kan worden verwerkt om effectief en efficiënt om te gaan met dreigingsinformatie en handelingsperspectieven.

OPTIE I

Bestaande organisaties die dreigingsinformatie en handelingsperspectieven aanleveren aan het NDN zijn zelf verantwoordelijk voor het vertalen van dreigingsinformatie en handelingsperspectieven, zodat het toegankelijk is voor alle doelgroepen. Hierdoor hoeft het DTC alleen informatie uit het NDN te halen, te vertalen naar specifieke situaties voor de doelgroepen en vervolgens te verspreiden naar de aangesloten initiatieven. Zodat de aangesloten doelgroepen gebruik kunnen maken van dreigingsinformatie en handelingsperspectieven, met specifieke situaties, uit het NDN.

PLUSPUNTEN

+ Dreigingsinformatie en handelingsperspectieven worden vertaald door de bron waardoor (foutieve) interpretatie wordt gereduceerd.

+ Het DTC kan zich focussen op het bieden van ondersteuning aan de doelgroepen.

+ Financieel voordeliger bij de implementatie.

MINPUNTEN

– Bestaande organisaties krijgen extra taken toegewezen.

OPTIE II

Bestaande organisaties leveren dreigingsinformatie en handelingsperspectieven aan bij het NDN. De dreigingsinformatie en handelingsperspectieven worden gedeeltelijk vertaald en gestructureerd aangeleverd. Het DTC kan vervolgens de dreigingsinformatie en handelingsperspectieven uit het NDN halen en tweeledig vertalen. Enerzijds zal dreigingsinformatie en handelingsperspectieven, waar nodig, verder moeten worden vertaald. Anderzijds zal het DTC dreigingsinformatie moeten voorzien van specifieke situaties voor de doelgroepen, voordat het wordt verspreidt naar de aangesloten initiatieven.

PLUSPUNTEN

+ Dreigingsinformatie en handelingsperspectieven worden vertaald door zowel de bestaande organisaties als het DTC, waardoor er een gedeelde verantwoordelijkheid is.

+ De extra investering wordt gespreid, omdat zowel de bestaande organisaties als het DTC een bijdrage levert.

MINPUNTEN

– Dreigingsinformatie en handelingsperspectieven worden door twee organisaties verwerkt, waardoor miscommunicatie kan ontstaan.

OPTIE III

Bestaande organisaties leveren dreigingsinformatie en handelingsperspectieven aan bij het NDN. De dreigingsinformatie en handelingsperspectieven worden in een willekeurige vorm aangeleverd. Het DTC haalt informatie op uit het NDN, analyseert en vertaalt de dreigingsinformatie en handelingsperspectieven voor de aangesloten initiatieven. Vervolgens zal het DTC dreigingsinformatie moeten voorzien van specifieke situaties voor de doelgroepen, voordat het kan worden verspreid naar de aangesloten initiatieven.

PLUSPUNTEN

+ Bestaande organisaties behouden de taken die zijn toegewezen.

MINPUNTEN

– Het DTC wordt een grote organisatie met relatief veel personeel.

– Dreigingsinformatie en handelingsperspectieven worden vertaald door een intermediair waardoor (foutieve) interpretatie een mogelijk risico is.

– Financieel nadelig bij de implementatie.

AANBEVELING

Bij de ontwikkeling van dit model is gekozen voor optie I. De motivatie voor deze keuze is dat organisaties die beschikken over dreigingsinformatie en handelingsperspectieven ook de beschikking hebben over inhoudelijke experts, die specialistische kennis hebben over cyberdreigingen, waardoor zij in staat zijn complexe dreigingsinformatie en handelingsperspectieven te vertalen naar toegankelijke dreigingsinformatie.

Hierdoor wordt de kans verkleind dat dreigingsinformatie en handelingsperspectieven door bijvoorbeeld een intermediair foutief wordt geïnterpreteerd. De intermediair zal in veel gevallen niet de beschikking hebben over alle kennis en expertise, waar organisaties wel de beschikking over hebben, omdat deze over het algemeen de eigenaar zijn van de dreigingsinformatie en handelingsperspectieven.

Tevens is het financieel voordeliger om dreigingsinformatie en handelingsperspectieven door de bestaande organisaties te laten vertalen, omdat de dreigingsinformatie toch door hun moet worden verwerkt, kost het slechts één extra handeling om complexe dreigingsinformatie en handelingsperspectieven te vertalen. Hierdoor wordt de belasting voor het vertalen van dreigingsinformatie en handelingsperspectieven verspreid over bestaande organisaties, in plaats van het centraal vertalen van de dreigingsinformatie en handelingsperspectieven in het DTC. Een neven effect hiervan is dat het DTC zich kan focussen, zoals aangegeven, op het bieden van hulp en ondersteuning aan het bedrijfsleven (Munnichs, Kouw, & Kool, 2017, p. 33).

BELANGRIJKE INFORMATIE

Vanwege voorkeur voor optie I wordt in de rest van dit hoofdstuk optie I verder uitgewerkt. De opties II en III worden buiten beschouwing gelaten.

6.3 RAAD VAN TOEZICHT

Het oprichten van een raad van toezicht wordt geadviseerd. De oprichting van de raad moet bewerkstelligen dat er onafhankelijk toezicht wordt gehouden op het functioneren van de publiek-private samenwerking met betrekking tot de informatie-uitwisseling. De komst van de raad zal de continuïteit en kwaliteit moeten waarborgen.

Het advies is om de raad onder te brengen bij de hoge functionaris, zoals wordt bepleit in het rapport *"Nederland digitaal droge voeten"*, die onder directe verantwoordelijkheid van het kabinet opereert. Het mandaat van de raad is hiermee gelijk geborgd. De raad zou juridische en technische kennis moeten borgen.

Aan de raad van toezicht wordt geadviseerd onafhankelijke raadsleden te benoemen die niet direct betrokken zijn bij de informatie-uitwisseling. Ook wordt geadviseerd dat de raad als bemiddelaar optreedt in geval van een conflict. Bijvoorbeeld als de informatie-uitwisseling, op enige wijze, door één of meerdere betrokkenen wordt ondermijnd. Aan de hand van de resultaten zullen vervolgstappen worden ondernomen om de informatie-uitwisseling te herstellen en eventueel te optimaliseren.

6.4 ORGANISATIES

In deze paragraaf worden de organisaties beschreven die bij CAMISO zijn betrokken.

6.4.1 NATIONAAL CYBER SECURITY CENTRUM (NCSC)

Het NCSC is opgericht om een bijdrage te leveren aan het vergroten van de cybersecurity weerbaarheid van de Nederlandse samenleving. De doelgroep van het NCSC is in 2012 bij de oprichting beperkt tot Rijksoverheid en organisaties uit de vitale infrastructuur, omdat het NCSC onderdeel is van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), die het mandaat heeft om maatschappelijke ontwrichting te voorkomen. Als gevolg hiervan kan het NCSC weinig betekenen voor het bedrijfsleven dat geen deel uitmaakt van de vitale infrastructuur.

Een extra structurele investering in het NCSC is van belang, vanwege het mandaat dat het NCSC heeft is er weinig budget om het bedrijfsleven te ondersteunen. Deze investering moet bewerkstelligen dat het NCSC zich flexibeler kan opstellen tegenover het bedrijfsleven, dat geen deel uitmaakt van de vitale infrastructuur. Steeds meer ICT-toepassingen zullen met elkaar worden verbonden. Door deze verbondenheid is geen enkele organisatie meer in staat om alle taken zelf uit te voeren. Een consequentie hiervan is dat de afhankelijkheid van andere bedrijven en dienstverleners toeneemt. Dit vergt een nieuwe aanpak waarbij het NCSC een primaire rol moet nemen door dreigingsinformatie actief te delen waardoor cyberrisico's worden gemitigeerd ten behoeve van de weerbaarheid van digitale ketens in het economisch en maatschappelijk belang van Nederland.

De onderstaande zaken worden geadviseerd aan het NCSC:

- *Deel dreigingsinformatie en handelingsperspectieven uit NDN met het bedrijfsleven evenals uit het Nationaal Respons Netwerk (NRN) en ISAC's.*
- *Stel het NRN, NDN en ISAC's open voor het bedrijfsleven en stimuleer deelname aan het NRN, NDN, ISAC's of soortgelijke initiatieven voor het bedrijfsleven.*
- *Ondersteun actief bij de oprichting van het DTC een kennis- en adviescentrum voor het bedrijfsleven, waardoor een verbeterde informatiepositie voor het bedrijfsleven wordt gecreëerd.*
- *Ondersteun VNO-NCW / MKB-Nederland met haar taken, bijvoorbeeld met kennisdeling en het trainen van brancheverenigingen totdat zij een basisniveau cybersecurity hebben bereikt. Deze taak kan na de oprichting van het DTC worden overgedragen.*

- *Activeer en stimuleer deelnemers in de ISAC's om dreigingsinformatie, die volgens het Traffic Light Protocol (TLP) als code rood, geel en groen is classificeert, te rubriceren. Hierdoor kan zéér waardevolle informatie alsnog worden gedeeld met het bedrijfsleven via brancheverenigingen, regionale initiatieven en topsectoren.*
- *Ondersteun en stimuleer de oprichting van meer regionale initiatieven zoals luchthaven Schiphol met CYSSEC en de haven Rotterdam met FERM hebben gedaan, waarbij gestreefd moet worden naar een landelijk dekkend stelsel van regionale initiatieven. Deze taak kan na de oprichting van het DTC worden overgedragen.*
- *Ondersteun en stimuleer de oprichting van Security Operations Centers (SOC's) en Computer Emergency Respons Teams (CERT's) door praktische handreikingen te verstrekken aan het bedrijfsleven over hoe zij een SOC en/of CERT kunnen inrichten. Deze taak kan na de oprichting van het DTC worden overgedragen.*

6.4.2 ALGEMENE INLICHTINGEN EN VEILIGHEIDSDIENST (AIVD)

De AIVD onderzoekt complexe digitale aanvallen die de nationale (digitale) veiligheid schade kunnen toebrengen. De AIVD richt zich met name op cyberspionage en –sabotage door andere landen, cyberterrorisme en cyberextremisme. Binnen de AIVD geven verschillende afdelingen invulling aan deze taak en werken hierin nauw samen.

Een extra structurele investering in de AIVD is van belang. Deze investering moet bewerkstelligen dat de AIVD cybersecurity gerelateerde dreigingsinformatie vertaalt en deelt, tenzij het de nationale (digitale) veiligheid in gevaar brengt. De dreigingsinformatie die de AIVD bezit is zéér waardevol voor het bedrijfsleven en met name voor kennisintensieve bedrijven, die in verband met het bezit van intellectueel eigendom vaker te maken krijgen met cyberspionage- en diefstal. Dit heeft directe impact op het langere termijn verdienvermogen en de werkgelegenheid bij deze kennisintensieve bedrijven.

Een oplossing moet worden geboden om dreigingsinformatie uit bijvoorbeeld de interne intelligence based cybersecurity-cyclus te delen. Indien dit niet gebeurt kan het de nationale (digitale) veiligheid juist in gevaar brengen, omdat het bedrijfsleven kwetsbaar blijft voor cyberrisico's waar al een oplossing voor beschikbaar is.

De onderstaande zaken worden geadviseerd aan de AIVD:

- *Actief delen van cybersecurity gerelateerde informatie met partners als Defensie en NCSC en nieuwe organisaties als het DTC, om de weerbaarheid in de digitale ketens te verhogen. Indien dit niet gebeurd kan het de nationale (digitale) veiligheid juist in gevaar brengen.*

6.4.3 MINISTERIE VAN DEFENSIE (DEFENSIE)

ICT-toepassingen spelen een steeds grotere rol, door onderlinge verbondenheid, bij inlichtingen en veiligheid. Defensie heeft daarom besloten dat de krijgsmacht ook cyberdreigingen gaat aanpakken. Naast de zee, het land, de lucht en de ruimte is het cyberdomein daarmee het 5e werkgebied van de krijgsmacht. In 2014 is het Defensie Cyber Commando (DCC) opgericht, dit zet zich in voor de nationale digitale veiligheid.

Een extra structurele investering in Defensie is van belang. Deze investering moet bewerkstelligen dat Defensie cybersecurity gerelateerde dreigingsinformatie vertaalt en deelt, tenzij het de nationale (digitale) veiligheid in gevaar brengt. De dreigingsinformatie die Defensie bezit is zéér waardevol voor het bedrijfsleven en met name voor kennisintensieve bedrijven, die in verband met intellectueel eigendom relatief vaker te maken krijgen met cyberspionage- en diefstal.

Een oplossing moet worden geboden om dreigingsinformatie op een gerubriceerde manier te delen. Indien dit niet gebeurt kan het de nationale (digitale) veiligheid juist in gevaar brengen, omdat het bedrijfsleven kwetsbaar blijft voor cyberrisico's waar al een oplossing voor beschikbaar is.

De onderstaande zaken worden geadviseerd aan het ministerie van Defensie:

- *Actief delen van cybersecurity gerelateerde informatie met partners als de AIVD en NCSC en nieuwe organisaties als het DTC, om de weerbaarheid in de digitale ketens te verhogen. Indien dit niet gebeurd kan het de nationale (digitale) veiligheid juist in gevaar brengen.*

6.5 INSTRUMENTEN

In deze paragraaf worden de instrumenten beschreven die bij CAMISO zijn betrokken.

6.5.1 NATIONAAL RESPONS NETWERK (NRN)

Het NRN is opgericht om ervaring, kennis en capaciteit op het gebied van incident respons te delen. Binnen het NDN bundelen het NCSC en publieke- en private Computer Emergency Respons Teams (CERT's) de krachten, om adequaat te kunnen reageren op cyberincidenten waardoor schade kan worden beperkt. Essentieel hiervoor is dat de overheid en het bedrijfsleven elkaar weten te vinden. Door onderlinge samenwerking en het delen van dreigingsinformatie en handelingsperspectieven wordt de weerbaarheid van de digitale ketens verhoogd.

Het advies is om het NRN open te stellen voor het bedrijfsleven. Door het openstellen van het NRN groeit de capaciteit en aangesloten CERT's kunnen zich aan elkaar optrekken, wat de volwassenheid van CERT's in Nederland verhoogd. Deze kennis zou moeten resulteren in het delen van dreigingsinformatie en handelingsperspectieven. Zodat het bedrijfsleven kan profiteren van de kennis binnen het NRN. Het bedrijfsleven zal wel moeten voldoen aan een nader te bepalen instapniveau, alvorens het bedrijf kan aansluiten bij het NRN. De reden hiervoor is om aansluitingen vanuit het bedrijfsleven gestaagd te laten groeien en het algemene kennisniveau te borgen.

De onderstaande zaken worden geadviseerd:

- *Stel het NRN open voor het bedrijfsleven, zodat de capaciteit binnen het NRN groeit en aangesloten CERT's zich aan elkaar kunnen optrekken, wat erin resulteert dat het landelijke niveau van CERT's verhoogd.*
- *Deel dreigingsinformatie en handelingsperspectieven uit het NRN met het bedrijfsleven, dat niet aangesloten kan worden, zodat zij kunnen profiteren van de kennis. De weerbaarheid van digitale ketens in Nederland wordt hierdoor verhoogd.*

6.5.2 INFORMATION SHARING AND ANALYSIS CENTRES (ISAC's)

ISAC's zijn publiek-private samenwerkingsverbanden en zijn per sector georganiseerd. Binnen de ISAC's wisselen organisaties onderling informatie en ervaring uit, door informatie en ervaring in vertrouwen te delen.

Organisaties binnen de ISAC's wisselen informatie uit op basis van het Traffic Light Protocol (TLP). De organisatie die de informatie inbrengt, geeft zelf de vertrouwelijkheidsgraad aan. Op deze manier is het voor ieder organisatie duidelijk hoe zij met deze informatie om dienen te gaan.

Het Traffic Light Protocol kent vier classificaties (NCSC, 2017):

- Rood: geheime informatie die alleen bestemd is voor de deelnemers aan het overleg. Deze informatie wordt mondeling gedeeld en mag niet buiten de ISAC worden gedeeld.
- Geel: beperkt geheimgehouden informatie die alleen mag worden gedeeld met mensen binnen de eigen organisatie die deze informatie nodig hebben voor het uitvoeren van hun functie.
- Groen: deze informatie mag gedeeld worden met meerdere mensen binnen en buiten de organisatie, maar het publiceren of plaatsen op het web is verboden.
- Wit: openbare informatie die onbeperkt verspreid mag worden.

Het advies is verbeter de ISAC's door te leren van het rapport[5] *"Next Generation ISAC's"* en deel dreigingsinformatie en handelingsperspectieven uit de ISAC's. Door het verbeteren van de ISAC's kan dreigingsinformatie en handelingsperspectieven worden gewonnen die momenteel niet voorhanden is. Door de sectorale aanpak van de ISAC's kan het bedrijfsleven in de betreffende vitale sector profiteren van de dreigingsinformatie.

Door het onderling delen van dreigingsinformatie en handelingsperspectieven uit de ISAC's kan de weerbaarheid worden verhoogd van de digitale ketens in Nederland. Organisaties zullen wel bereid willend moeten zijn om code rood, geel en groen uit de ISAC's te rubriceren, tenzij organisaties aangeven geen bezwaar te hebben dat dreigingsinformatie niet geanonimiseerd wordt gedeeld. De

[5] Next Generation ISAC's – *ISAC development model and building blocks,* TNO

initiatieven (brancheverenigingen, regionaal, topsectoren), met name de regionale initiatieven, hebben behoefte aan code rood, geel en groen informatie.

De onderstaande zaken worden geadviseerd:

- *Verbeter de ISAC's door te leren van het rapport "Next Generation ISACS". De weerbaarheid van alle vitale sectoren wordt vergroot door de beproefde sectorale aanpak. Het positieve gevolg is dat dreigingsinformatie, die momenteel niet voorhanden is, wordt gewonnen.*
- *Verbeter het kennisniveau van de bestaande ISAC's. Binnen de afzonderlijke ISAC's bestaat een verschil in kennis. Het kennisniveau van de afzonderlijke ISAC's zou op een gelijkwaardig kennisniveau moeten komen, tenzij het de groei van afzonderlijke ISAC's remt. Dan zouden ISAC's onderling tips en tricks kunnen delen om het kennisniveau te verbeteren.*
- *Rubriceer dreigingsinformatie die in de ISAC's wordt gedeeld. Door het rubriceren van dreigingsinformatie kan worden besloten om deze informatie te delen.*
- *Deel dreigingsinformatie en handelingsperspectieven uit de ISAC's onderling en met het bedrijfsleven, zodat zij dreigingsinformatie en handelingsperspectieven ontvangen waar zij behoefte aan hebben. Dit heeft een bevorderende werking voor de weerbaarheid van de digitale ketens in Nederland.*

6.5.3 NATIONAAL DETECTIE NETWERK (NDN)

Het NDN is een samenwerkingsverband voor het effectief en efficiënt waarnemen van cyberdreigingen en cyberrisico's. Het delen van dreigingsinformatie zorgt ervoor dat organisaties vroegtijdig maatregelen kunnen treffen, waardoor schade kan worden beperkt.

Het advies is om het NDN open te stellen voor het bedrijfsleven. Door het openstellen van het NDN wordt de capaciteit vergroot waardoor cyberdreigingen sneller kunnen worden waargenomen. Het delen van dreigingsinformatie kan ervoor zorgen dat het bedrijfsleven minder schade ondervindt van cyberincidenten. Het bedrijfsleven zal wel moeten voldoen aan een nader te bepalen instapniveau, alvorens het bedrijf kan aansluiten bij het NDN. De reden hiervoor is om aansluitingen vanuit het bedrijfsleven gestaagd te laten groeien en het algemene kennisniveau te borgen.

Het advies is om zowel databases aan te leggen voor dreigingsinformatie en handelingsperspectieven. Deze databases moeten bijdragen aan de ideale situatie waar naast dreigingsinformatie ook direct handelingsperspectieven kunnen worden gekoppeld.

De onderstaande zaken worden geadviseerd:

- *Stel het NDN open voor het bedrijfsleven, zodat de capaciteit wordt vergroot waardoor cyberdreigingen sneller kunnen worden waargenomen. Het bedrijfsleven kan hierdoor vroegtijdig maatregelen treffen, waardoor schade kan worden beperkt.*

- *Richt het NDN in als het centrale informatieknooppunt voor dreigingsinformatie en handelingsperspectieven. De versnippering van dreigingsinformatie wordt hiermee tegen gegaan en regie kan over het NDN worden gevoerd.*
- *Deel dreigingsinformatie en handelingsperspectieven uit het NDN met het bedrijfsleven, dat niet aangesloten kan worden, zodat zij kunnen profiteren van de kennis. De weerbaarheid van digitale ketens in Nederland wordt hierdoor verhoogd.*
- *Leg databases aan voor dreigingsinformatie en handelingsperspectieven in het NDN, zodat in een ideale situatie naast dreigingsinformatie direct handelingsperspectieven kunnen worden gekoppeld. Het bedrijfsleven kan door deze koppeling effectief optreden.*

6.6 INTERMEDIAIRS

In deze paragraaf worden de intermediairs beschreven die bij CAMISO zijn betrokken.

6.6.1 DIGITAL TRUST CENTRUM (DTC)

Momenteel (mei 2017) worden door het ministerie van Veiligheid en Justitie, het ministerie van Economische Zaken, VNO-NCW / MKB-Nederland, FME, Nederland-ICT en CIO Platform Nederland gesprekken gevoerd over de oprichting van het DTC.

Een snelle oprichting van het DTC wordt geadviseerd. Het DTC moet zorgen dat er een verbeterde informatiepositie wordt gecreëerd voor het gehele bedrijfsleven. De komst van een kennis- en adviescentrum voor het bedrijfsleven wordt als noodzakelijk geacht, als gevolg van het feit dat de afhankelijkheid toeneemt. Hierdoor moet de weerbaarheid van de digitale ketens worden verhoogd. Dit komt doordat steeds meer ICT-toepassingen met elkaar zullen worden verbonden. Deze afhankelijkheid zal in de komende jaren steeds verder toenemen door de verdere ontwikkeling van het Internet of Things (IoT).

Het DTC is een niet bestaande organisatie. Momenteel is er discussies over de invulling, positionering en financiering van het DTC. Als gevolg hiervan is besloten om een adviesvoorstel te schrijven voor de inrichting van het DTC. De opzet van deze paragraaf is hierdoor anders dan andere paragrafen in dit hoofdstuk.

PUBLIEK-PRIVATE FINANCIERING

Een publiek-private financiering voor de totstandkoming van het DTC wordt geadviseerd. Het advies is dat de overheid in eerste instantie de eerste financiering verzorgt om de komst van het DTC te bespoedigen. In tweede instantie zal de private sector mee moeten financieren om de continuïteit te waarborgen.

Het bedrijfsleven bestaat voor 99% uit het mkb en heeft, zoals aangegeven, behoefte aan een verbeterde informatiepositie. De oprichting van het DTC is speciaal voor het mkb. Het is een illusie te denken dat de overheid de volledige financiering voor het bedrijfsleven op zich neemt. Het

bedrijfsleven heeft namelijk een eigen verantwoordelijkheid met betrekking tot cybersecurity wat valt onder het ondernemerschap. De overheid hoeft dit niet te financieren.

Voor de private sector zijn drie financieringsvormen beschreven:

OPTIE I

De eerste mogelijkheid is het heffen van lidmaatschapscontributie voor bedrijven die gebruik willen maken van het DTC. Een afbreukrisico is dat het bedrijfsleven, met name het mkb, de toegevoegde waarde niet ziet vanwege het gebrek aan noodzaak (awareness). Dit risico kan worden gemitigeerd door de kosten van de lidmaatschapscontributie te laten oplopen met het aantal werkzame fte's. Hierdoor zijn de kosten voor een kleinbedrijf met 10 fte lager dan voor een middenbedrijf met 249 fte. Een andere oplossing zou kunnen zijn om de kosten te koppelen aan de omzet. Hierdoor draagt ieder bedrijf hetzelfde percentrage van de omzet af, fiscale voordelen zouden een stimulerend effect kunnen hebben op deelname aan het DTC. Een andere mogelijkheid is om het contractueel te borgen, bijvoorbeeld dat ketenpartners producten en diensten mogen leveren als zij "in control" zijn en aangesloten bij het DTC.

PLUSPUNTEN

+ Het bedrijfsleven betaalt een gelijk percentage aan lidmaatschapscontributie voor deelname aan het DTC.

+ Fiscale voordelen kunnen een stimulerende werking hebben en het gevoel doen afnemen dat men dubbel betaalt doordat het bedrijfsleven ook belasting afdraagt.

MINPUNTEN

– Het bedrijfsleven draagt ook belasting af waarmee het publieke deel van het DTC is gefinancierd.

– Bedrijven die lid zijn van een brancheverenigingdragen dubbele lidmaatschapscontributie af voor het DTC.

OPTIE II

De tweede mogelijkheid is het heffen van lidmaatschapscontributie bij het bedrijfsleven en VNO-NCW / MKB-Nederland. Een afbreukrisico is dat bedrijven die gebruik willen maken van het DTC en lid zijn van een brancheverenigingdubbele lidmaatschapscontributie betalen. Dit risico kan worden gemitigeerd door fiscale voordelen te bieden voor deze bedrijven. Dit kan een stimulerend effect hebben op deelname aan het DTC.

PLUSPUNTEN

+ Bedrijven die lid zijn van een brancheverenigingkunnen gratis gebruik maken van het DTC.

+ Bedrijven die niet lid zijn van een brancheverenigingbetalen een gelijk percentrage aan lidmaatschapscontributie voor deelname aan het DTC.

MINPUNTEN

– Het bedrijfsleven draagt ook belasting af waarmee het publieke deel van het DTC is gefinancierd.

+ Fiscale voordelen kunnen een stimulerende werking hebben en het gevoel doen afnemen dat men dubbel betaalt doordat het bedrijfsleven ook belasting afdraagt.

OPTIE III

De derde mogelijkheid is dat VNO-NCW / MKB-Nederland een percentage van de contributie die aan brancheverenigingen wordt berekend investeert in het DTC. Een afbreukrisico is dat brancheverenigingen meebetalen aan het DTC terwijl een deel hun leden geen behoefte heeft vanwege een gebrek aan noodzaak (awareness) of cybersecurity zelfstandig naar behoren heeft ingericht. Voor het bedrijfsleven wat cybersecurity zelfstandig naar behoren heeft ingericht is geen passende oplossing, anders dan dat zij meefinancieren. De leden die door een gebrek aan noodzaak (awareness) meefinancieren kunnen door het creëren van bewustwording de nut en noodzaak van het DTC mogelijk op termijn gaan inzien.

PLUSPUNTEN

+ VNO-NCW / MKB-Nederland investeert een percentage van de contributie die aan de brancheverenigingen wordt berekend.

+ Het bedrijfsleven wat niet lid is van een branchevereniging hoeft geen lidmaatschapscontributie te betalen voor deelname aan het DTC.

MINPUNTEN

– Het bedrijfsleven wat lid is van een branchevereniging en wat geen gebruik maakt van het DTC financiert mee aan het DTC.

AANBEVELING

De voorkeur is optie II waarbij lidmaatschapscontributie zowel bij het bedrijfsleven als VNO-NCW / MKB-Nederland wordt berekend. De motivatie voor deze keuze is dat de continuïteit van het DTC een gedeelde verantwoordelijkheid is voor het bedrijfsleven als voor VNO-NCW / MKB-Nederland. Het bedrijfsleven als VNO-NCW / MKB-Nederland financieren door deze optie mee aan het DTC.

Voor het bedrijfsleven wat lid is van een branchevereniging kan gratis gebruik maken van de faciliteiten van het DTC. Het bedrijfsleven wat niet lid is van een branchevereniging betaald een gelijk percentage aan lidmaatschapscontributie. Hierbij zouden fiscale voordelen voor het bedrijfsleven een stimulerende werking kunnen hebben. Een positief neveneffect is dat het gevoel dat het bedrijfsleven dubbel betaald kan afnemen. Een andere mogelijkheid is om het contractueel te borgen, bijvoorbeeld dat ketenpartners producten en diensten mogen leveren als zij “in control” zijn en aangesloten bij het DTC.

POSITIONERING DTC

Het advies aan het DTC is: *richt een zelfstandige entiteit op*. Door het zijn van een zelfstandige entiteit hoeft het DTC zich niet te houden aan de gedragsregels (ACM, 2017) van de Wet Markt en Overheid (Rijksoverheid, 2011). Het voordeel ten opzichte van een overheidsinstelling is dat de gedragsregels van deze wet niet van toepassing is.

Autoriteit Consument en Markt (ACM) houdt toezicht op de naleving van deze gedragsregels en kan een onderzoek instellen als er een vermoeden is van concurrentievervalsing.

Als de Wet Markt en Overheid van toepassing is dan dient er rekening te worden gehouden met de concurrentiepositie van commerciële dienstverleners en zal moeten worden gezorgd dat eerlijke concurrentie mogelijk is. De ACM kan een boete opleggen voor elke dag dat de wet is overtreden.

AANSLUITING DOELGROEPEN

Het DTC moet zorgen dat er een verbeterde informatiepositie wordt gecreëerd voor het gehele bedrijfsleven. Het advies is om eerste de regionale initiatieven aan te sluiten op het DTC, omdat deze initiatieven al bestaan en benaderbaar zijn. Als tweede zouden de topsectoren moeten worden aangesloten, omdat dit kennisintensieve bedrijven zijn die in verband met het bezit van intellectueel eigendom vaker te maken krijgen met cyberspionage- en diefstal. En als derde zouden de brancheverenigingen moeten worden aangesloten, waar de prioriteit van aansluiten moet liggen op de volwassenheid van het thema cybersecurity en/of de branches die sterk gedigitaliseerd zijn, zoals bijvoorbeeld de datacenterbranche.

TAAKOPVATTING

Het advies ten aanzien van een DTC is om als primaire taak te nemen: *het selecteren, ontvangen en verspreiden van dreigingsinformatie en handelingsperspectieven naar de aangesloten initiatieven.* En als secundaire taak: *het ontvangen en verspreiden van handelingsperspectieven en het bieden van hulp en ondersteuning in de vorm van een helpdesk.* Onderstaand zullen de adviezen over de taakopvatting worden beschreven.

EERSTE TAAK

De eerste taak is het selecteren, ontvangen en verspreiden van de beschikbare dreigingsinformatie en handelingsperspectieven uit het NDN. Het NDN moet als centraal verzamelpunt fungeren waar alle toegankelijke en beschikbare dreigingsinformatie wordt verzameld. De reden hiervoor is dat de bestaande organisaties worden ontlast van informatie-uitwisselingsverzoeken en dat de dreigingsinformatie en handelingsperspectieven breder worden gedeeld. De initiatieven (brancheverenigingen, regionaal en topsectoren) selecteren, vertalen en verspreiden relevante dreigingsinformatie en handelingsperspectieven, eventueel in samenspraak met het DTC, naar de aangesloten doelgroepen.

Bij het ontvangen van dreigingsinformatie en handelingsperspectieven die afkomstig is van de initiatieven (brancheverenigingen, regionaal en topsectoren) of vanuit het bedrijfsleven is het DTC verantwoordelijk dat deze informatie wordt verzameld in het NDN.

TWEEDE TAAK

De tweede taak is het verzamelen en verspreiden van handelingsperspectieven. De essentie is het verzamelen van openbare handelingsperspectieven die door organisaties in de vitale sectoren, het bedrijfsleven en commerciële dienstverleners zijn gepubliceerd. Hierdoor kan dreigingsinformatie worden gekoppeld aan handelingsperspectieven. De onderzoeker heeft een overzicht gemaakt van Nederlandse initiatieven waar dreigingsinformatie en handelingsperspectieven worden gedeeld. Volgens de stakeholders van dit onderzoek is het overzicht waardevol en zou het up-to-date moeten worden gehouden. De onderzoeker heeft stakeholders actief benadert om het overzicht over te dragen, maar is hierin nog niet geslaagd. Het advies en persoonlijk verzoek aan het DTC is om het overzicht te adopteren en het up-to-date te houden. Het overzicht van de Nederlandse initiatieven is bij de Cyber Security Raad op te vragen.

DERDE TAAK

De derde taak is het bieden van hulp en ondersteuning vanuit een helpdesk, een afdeling cybersecurity-adviseurs, die bedrijven kunnen voorzien van antwoord opvragen die zij aan de helpdesk stellen. Het moet mogelijk zijn voor bedrijven om per (live-)chat, per e-mail of telefonisch vragen te kunnen stellen aan de helpdesk. De helpdesk moet als eerstelijns helpdesk fungeren. Als een adviseur het vermoeden krijgt dat er bij het bedrijf in kwestie een alarmerende situatie gaande is, moet er worden geadviseerd een commerciële dienstverlener in te schakelen.

De commerciële dienstverlener geldt in dit verband als tweedelijns helpdesk. De redenen hiervoor zijn om de eventueel marktverstorende werking in te perken, de onafhankelijkheid te waarborgen en commerciële belangen uit te sluiten. Als de commerciële dienstverlener de reden niet kan oplossen kan in uitzonderlijke gevallen via het DTC worden geëscaleerd naar het NCSC. Het NCSC geldt in dit verband als derdelijns helpdesk.

ADVIEZEN

De onderstaande zaken worden geadviseerd:

- *Bespoedig de komst van het DTC of een kennis- en adviescentrum voor het bedrijfsleven. Een verbeterde informatiepositie van het bedrijfsleven zal de weerbaarheid van de digitale keten verhogen.*
- *Maak de komst van het DTC middels publiek-private financiering mogelijk. Het advies is om de eerste financiering door de overheid te laten verzorgen om de komst van het DTC mogelijk te maken. De tweede financiering door de private sector is om de continuïteit te bewerkstelligen. Voor de private sector wordt gedeelde lidmaatschapscontributie als financieringsvorm geadviseerd.*

- *Maak van het DTC een zelfstandige entiteit. Het voordeel is dat de gedragsregels van de Wet Markt en Overheid niet van toepassing is ten opzichte van een overheidsorganisaties.*
- *Betrek VNO-NCW / MKB-Nederland bij de oprichting om brancheverenigingen te bereiken en te fungeren als schakelorganisatie tussen de brancheverenigingen en het DTC.*
- *Neem de aansluiting van de doelgroepen over voor het DTC. Als eerste de regionale initiatieven, als tweede de topsectoren en als derde de brancheverenigingen. Waar bij de brancheverengingen de prioriteit van aansluiten moet liggen* op de volwassenheid van het thema cybersecurity en/of de branches die sterk gedigitaliseerd zijn zoals bijvoorbeeld de datacenterbranche.
- *Ondersteun actief de aangesloten initiatieven (brancheverenigingen, regionaal en topsectoren) met de uitvoering van hun taken, zodat de doelgroepen op een juiste manier dreigingsinformatie en handelingsperspectieven ontvangen.*
- *Neem de volgende taakopvatting over voor het DTC. De primaire taak is: het selecteren, ontvangen en verspreiden van dreigingsinformatie en handelingsperspectieven naar de aangesloten initiatieven. De secundaire taken zijn: het verzamelen en verspreiden van handelingsperspectieven en het bieden van hulp en ondersteuning in de vorm van een helpdesk.*

6.6.2 VNO-NCW / MKB-NEDERLAND

VNO-NCW is een koepelorganisatie voor brancheverenigingen in Nederland. VNO-NCW heeft één gezamenlijk bureau met MKB-Nederland. Bij VNO-NCW zijn 155 brancheverenigingen aangesloten en ongeveer 500 ondernemingsleden. MKB-Nederland vertegenwoordigt ruim 170.000 ondernemers in Nederland.

Het advies aan VNO-NCW / MKB-Nederland is om brancheverenigingen bewust te maken van de verantwoordelijkheid die het bedrijfsleven heeft met betrekking tot cybersecurity. Dit kan worden bewerkstelligd door trainingen te verzorgen aan brancheverenigingen totdat zij over een basisniveau cybersecurity beschikken, omdat niet alle brancheverenigingen beschikken over voldoende capaciteit en middelen om deze basiskennis tot zich te nemen.

De onderzoeker is zich bewust van het feit dat dit buiten de traditionele taakopvatting van de koepelorganisatie valt. De reden om de taak alsnog bij VNO-NCW / MKB-Nederland te beleggen is tweeledig. Enerzijds wilt het bedrijfsleven een verbeterde informatiepositie en anderzijds ontbreekt het aan een gelijkwaardig alternatief van VNO-NCW / MKB-Nederland. Dit zorgt ervoor dat het bedrijfsleven door VNO-NCW / MKB-Nederland moet worden verzorgd, omdat zij via de brancheverenigingen het dichtste bij het bedrijfsleven staat.

De onderstaande zaken worden geadviseerd aan VNO-NCW / MKB-Nederland:

- *Fungeer als schakelorganisatie tussen het DTC en de brancheverenigingen, waardoor het bedrijfsleven kan worden bereikt.*
- *VNO-NCW / MKB-Nederland traint brancheverenigingen, eventueel in samenwerking met dienstverleners, totdat zij een basisniveau cybersecurity hebben bereikt. Omdat niet alle brancheverenigingen beschikken over voldoende capaciteit en middelen om deze basiskennis tot zich te nemen.*

6.7 INITIATIEVEN

In deze paragraaf worden de initiatieven beschreven die bij CAMISO zijn betrokken.

6.7.1 BRANCHEVERENIGINGEN

Een branchevereniging is een vereniging van bedrijven uit een specifieke branche. Een branchevereniging bezit nuttige kennis over zowel de markt als de branche. Bedrijven die aangesloten zijn kunnen gebruik maken van de kennis en ervaring die wordt aangeboden.

Het advies aan brancheverenigingen is om de aangesloten bedrijven bewust te maken van de verantwoordelijkheid die zij hebben met betrekking tot cybersecurity. Onlangs heeft de Cyber Security Raad de handreiking[6] *"Ieder bedrijf heeft zorgplichten"* aangeboden aan de minister van Economische Zaken, de staatssecretaris van Veiligheid en Justitie en de voorzitter van VNO-NCW. Deze handreiking biedt een goede aanleiding om in gesprek te gaan met de aangesloten bedrijven. Het aansluiten van brancheverenigingen op het DTC wordt mede geadviseerd. Op deze manier kan het DTC zijn intermediair rol vervullen.

De onderzoeker is zich bewust van het feit dat dit buiten de taakopvatting van brancheverengingen valt, behalve de brancheverenigingen die al actief bezig zijn met het informeren van leden. De reden om deze taak bij de brancheverenigingen te beleggen is tweeledig, enerzijds wilt het bedrijfsleven een verbeterde informatiepositie en anderzijds kennen de brancheverenigingen de informatiebehoefte van de leden. Dit zorgt ervoor dat het bedrijfsleven door de brancheverenigingen moet worden verzorgd, omdat zij de behoefte kennen van de leden en directe toegang hebben tot de leden.

De onderstaande zaken worden geadviseerd aan de voorzitters van de brancheverenigingen:

- *Maak de aangesloten bedrijven bewust van de verantwoordelijkheid die zij hebben met betrekking tot cybersecurity, waardoor de bewustwording van cybersecurity zal toenemen en het bedrijfsleven de verplichting van cybersecurity op zich neemt.*

[6] Ieder bedrijf heeft zorgplichten, "*Een handreiking voor bedrijven op het gebied van cybersecurity",* Cyber Security Raad (april 2017)

- *Sluit als brancheverenigingen aan op het DTC, hierdoor kan het DTC zijn intermediair rol vervullen. Dreigingsinformatie kan zo vanuit het DTC naar de brancheverenigingen stromen en omgekeerd.*

6.7.2 REGIONALE INITIATIEVEN

Regionale initiatieven zijn initiatieven die de weerbaarheid van het bedrijfsleven op het gebied van cybersecurity in regionaal opzicht willen verhogen. De regionale initiatieven bundelen en verspreiden kennis. Bedrijven die aangesloten zijn kunnen gebruik maken van de kennis en ervaring die wordt aangeboden.

Het advies aan de regionale initiatieven is om onderlinge samenwerking te bevorderen, waardoor de krachten worden gebundeld. Dit vergroot de toegevoegde waarde van elk individueel initiatief. Het aansluiten van regionale initiatieven op het DTC wordt geadviseerd. Op deze manier kan onderlinge samenwerking worden gestimuleerd en kan het DTC zijn intermediair rol vervullen en regionale initiatieven ontlasten.

De onderzoeker kent de behoefte van de regionale initiatieven door de afgenomen interviews voor dit onderzoek. De reden de regionale initiatieven te betrekken is tweeledig, enerzijds hebben de regionale initiatieven behoefte aan code rood, oranje en groen informatie uit de ISAC's en anderzijds kunnen de regionale initiatieven deze informatie te verspreiden aan bedrijven in de regio.

De onderstaande zaken worden geadviseerd aan de regionale initiatieven:

- *Sluit als regionale initiatief aan op het DTC, hierdoor kan het DTC zijn intermediair rol vervullen. Dreigingsinformatie kan zo vanuit het DTC naar de regionale initiatieven stromen en omgekeerd.*

6.7.3 TOPSECTOREN

Topsectoren zijn gebieden waar het bedrijfsleven en onderzoekscentra, die gevestigd zijn in Nederland, wereldwijd in uitblinken. Het bedrijfsleven, universiteiten, onderzoekscentra en overheid werken samen aan kennis en innovatie om deze positie te versterken. Ieder bedrijf kan zich aansluiten bij de topsectoren, dat geldt ook voor het mkb. Bedrijven zijn verbonden aan topsectoren als bedrijven de subsidiemogelijkheden benutten die voor topsectoren zijn vrijgemaakt.

Het advies aan de topsectoren is om onderlinge samenwerking te bevorderen, waardoor de krachten worden gebundeld. Dit vergroot de toegevoegde waarde van elke individuele topsector. Het aansluiten van topsectoren op het DTC wordt geadviseerd. Op deze manier kan onderlinge samenwerking worden gestimuleerd en kan het DTC zijn intermediair rol vervullen en topsectoren ontlasten.

De onderzoeker is zich bewust van het feit dat dit buiten de taakopvatting van topsectoren valt. De reden om deze taak bij de topsectoren te beleggen is tweeledig, enerzijds wilt het bedrijfsleven een verbeterde informatiepositie en anderzijds kennen de topsectoren de behoefte. Dit zorgt ervoor dat

het bedrijfsleven door topsectoren moet worden verzorgd, omdat zij de informatiebehoefte kennen en directe toegang hebben tot de bedrijven. Daarnaast voert TNO een verkennend onderzoek uit naar informatie-uitwisseling in topsectoren, hieruit kan worden opgemaakt dat topsectoren behoefte hebben informatie-uitwisseling. De uitkomsten van het onderzoek zijn nog niet bekend.

De onderstaande zaken worden geadviseerd aan de topsectoren:

- *Sluit als topsector aan op het DTC, hierdoor kan het DTC zijn intermediair rol vervullen. Dreigingsinformatie kan zo vanuit het DTC naar de topsectoren stromen en omgekeerd.*

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel verificatie en de fase data-analyse afgerond en is het onderdeel onderzoeksrapport gestart. In het voorgaande hoofdstuk zijn de onderdelen evaluatie en data-analyse beschreven. In het komende hoofdstuk wordt het onderdeel onderzoeksrapport voortgezet. De fase rapporteren wordt hiermee voortgezet.

Afbeelding 9: Voortgang onderzoek

7 CONCLUSIE EN AANBEVELINGEN

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht, de onderzoeksopzet, het literatuuronderzoek, de interviews, de resultaten en de optimalisatie van de informatie-uitwisseling. In dit hoofdstuk wordt de conclusie en aanbevelingen beschreven. Het doel van dit hoofdstuk is om de conclusie en aanbevelingen van dit onderzoek, op een duidelijke manier, te presenteren

Met dit hoofdstuk wordt de fase rapporten voortgezet. Onderzoeksrapport is een onderdeel van de fase rapporteren.

7.1 CONCLUSIE

Dit onderzoeksrapport begon met een beschrijving van het belang van digitalisering in onze economie en maatschappij. Waar Nederland zich in de loop der jaren heeft ontwikkeld tot één van de meest gedigitaliseerde landen ter wereld. Door digitalisering zullen steeds meer ICT-toepassingen met elkaar worden verbonden. De afhankelijkheid van andere bedrijven zal de komende jaren als maar toenemen als gevolg van het Internet of Things.

De centrale vraagstelling van dit onderzoek luidde als volgt:

Op welke wijze kan, met betrekking tot cybersecurity, kennisdeling en informatie-uitwisseling aan het mkb worden geoptimaliseerd ter bevordering van de weerbaarheid van de digitale ketens in Nederland?

Nederland moet de beschikking krijgen over een landelijk dekkend stelsel van initiatieven waar het mkb zich kan aansluiten. Dit stelsel is een samenspel van publieke, private, nieuwe en bestaande organisaties, instrumenten en initiatieven. Deze collectieve aanpak moet ervoor zorgen dat de informatie-uitwisseling het volledige Nederlandse bedrijfsleven omvat.

Het is belangrijk dat in gezamenlijkheid de verantwoordelijkheid wordt genomen om de veiligheid van de digitale ketens te waarborgen. Door het optimaliseren en faciliteren van de publiek-private samenwerking verbetert de informatiepositie van het mkb. De toegevoegde waarde van informatie-uitwisseling aan het mkb is dat het de weerbaarheid bevorderd van de digitale ketens in Nederland.

Om een verbeterde informatiepositie aan het mkb mogelijk te maken moet dreigingsinformatie en handelingsperspectieven op een begrijpelijke manier worden aangeleverd. Dit kan door de aangeleverde informatie te laten voldoen aan de kenmerken: toegevoegde waarde, betrouwbaarheid en toegankelijkheid. Door informatie te laten voldoen aan deze kenmerken wordt voldaan aan de randvoorwaarden toegevoegde waarde en vertrouwen, die ten grondslag liggen aan informatie-uitwisseling.

7.2 AANBEVELINGEN

Uit dit onderzoek is naar voren gekomen dat Nederland de beschikking moet krijgen over een landelijk dekkend stelsel van initiatieven waarbij het mkb zich kan aansluiten. Het optimaliseren en faciliteren van publiek-private samenwerking is noodzakelijk om de weerbaarheid van digitale ketens te verhogen.

Dit onderzoek heeft geleid tot CAMISO, een optimalisatiemodel waarmee de informatie-uitwisseling kan worden geoptimaliseerd. Het model is geverifieerd en gevalideerd door experts op het terrein van cybersecurity.

De aanbeveling is om eerst te inventariseren welke vervolgonderzoeken noodzakelijk zijn om het model in een proof-of-concept te implementeren. Voor de inventarisatie van vervolgonderzoeken worden in hoofdstuk 8 vervolgonderzoeken aangedragen ten aanzien van dit onderzoek. Hierna zou het model geïmplementeerd kunnen worden om te beoordelen of het ontwikkelde model ook praktisch toepasbaar is en/of meer vervolgonderzoek nodig is. Dit houdt in dat het model zou moeten functioneren als beschreven in hoofdstuk 6, waar alle stakeholders betrokken zijn en het een verbeterde informatiepositie oplevert voor het mkb.

BELANGRIJKE INFORMATIE

De in hoofdstuk 8 beschreven vervolgonderzoeken zijn niet uitputtend. De vervolgonderzoeken geven slechts een indicatie van de barrières met betrekking tot het informatie-uitwisselingsvraagstuk.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel onderzoeksrapport voortgezet. In het voorgaande hoofdstuk zijn de onderdelen verificatie en onderzoeksrapport beschreven. In het komende hoofdstuk wordt het onderdeel onderzoeksrapport voortgezet. De fase rapporteren wordt hiermee voortgezet.

Afbeelding 10: Voortgang onderzoek

8 DISCUSSIE

In de voorgaande hoofdstukken is beschreven: het kader waarbinnen dit onderzoek is verricht, de onderzoeksopzet, het literatuuronderzoek, de interviews, de resultaten, de optimalisatie van de informatie-uitwisseling en de conclusie en aanbevelingen van dit onderzoek. In dit hoofdstuk wordt de discussie beschreven. Het doel van dit hoofdstuk is het vinden van een verklaring voor het al dan niet uitkomen van de hypothese.

Met dit hoofdstuk wordt de fase rapporten voortgezet. Onderzoeksrapport is een onderdeel van de fase rapporteren.

8.1 HYPOTHESE

De hypothese is verworpen zoals in hoofdstuk 5 is te lezen. De verklaring voor het verwerpen van de hypothese is dat dit onderzoek is bijgesteld, waardoor de hypothese in een eerder stadium binnen dit onderzoek al is verworpen. Het model is ontwikkeld om de publiek-private samenwerking tussen organisaties, instrumenten en initiatieven te optimaliseren en te faciliteren.

In het model zijn er posities weggelegd voor de ISAC's en brancheverenigingen. Daarentegen zijn de veiligheidsregio's en de Kamer van Koophandel niet opgenomen. Vervolgonderzoek is nodig om uit te wijze of het verstandig is deze organisaties op te nemen. Momenteel zijn er niet veel aanwijzingen die aangeven dat het thema cybersecurity leeft. Op termijn kunnen de veiligheidsregio's een positie nemen als zij bijvoorbeeld een gedeelde dienstverlening, in de vorm van een SOC en/of CERT functionaliteit, voor de veiligheidsregio gaan inrichten. Ook het oprichten van een ISAC functionaliteit moet niet worden uitgesloten.

8.2 BEPERKINGEN

Dit onderzoek is binnen een tijdsbestek van 17 kalenderweken uitgevoerd zoals in hoofdstuk 2 is te lezen. Als gevolg van deze tijdsbeperking kon tijdens het uitvoeren van dit onderzoek niet op alle aspecten even diepgaand worden ingegaan.

Tijdens het schrijven van dit onderzoeksrapport zijn er nog verschillende onderzoeksrapporten gepubliceerd. Deze rapporten zijn uiteindelijk niet verwerkt in dit onderzoeksrapport. Het rapport[7] *"The Netherlands Cyber readiness at a Glance"* benadrukt dat de informatie-uitwisseling met de private sector meer mag worden gestimuleerd (Spidalieri & Hathaway, 2017).

[7] The Netherlands Cyber Readiness at a Glance – *Cyber Readiness Index 2.0*, Melissa Hathaway en Francesca Spidalieri, Potomac Institute for Policy Studies (mei 2017)

Het rapport[8] *"Verkenning Cybersecurity Informatiedeling binnen de Topsectoren"* benadrukt dat de topsectoren extra aandacht moeten gaan geven aan cybersecurity en de mogelijke impact die digitale dreigingen kunnen hebben op hun business (Huistra & Krabbendam-Hersman, 2017).

Het rapport[9] *"Challenges around Measuring Cybersecurity Threats in the Netherlands"* benadrukt dat een goede informatie-uitwisseling Nederland kan helpen om de weerbaarheid van de digitale ketens te verhogen en benoemen barrières die informatie-uitwisseling (negatief) beïnvloeden (Cornelisse, Bargh, & Choenni, verwachting 2017).

Bij de verificatie en validatie van de optimalisatie van de informatie-uitwisseling is door een beperkt aantal experts op het terrein van cybersecurity feedback geleverd. Dit heeft geresulteerd in een groeimodel waarin organisaties, instrumenten, initiatieven kunnen worden toegevoegd. Het model is niet volledig uitgekristalliseerd. In de optimalisatie is alleen cybersecurity gerelateerde informatie-uitwisseling opgenomen. Cybercriminaliteit is buiten beschouwen gelaten, maar is een waardevolle toevoeging aan het model.

Het Landelijk Servicecentrum E-crime (werktitel) kan mogelijk worden aangesloten, waardoor het bedrijfsleven melding en/of aangifte kan doen. Het inzicht dat wordt verkregen uit de meldingen en/of aangifte is belangrijk voor de opsporing en vervolging vanuit de Nationale Politie en het Openbaar Ministerie. De Nationale Politie en het Openbaar Ministerie zouden als organisaties aan het model kunnen worden toegevoegd.

Als de doelgroepen dreigingsinformatie en handelingsperspectieven ontvangen moet daar opvolging aan kunnen worden gegeven. Het bedrijfsleven, met name het mkb, heeft in veel gevallen niet de beschikking over gekwalificeerd personeel met betrekking tot cybersecurity. In dit onderzoek is dit aspect nauwelijks aan bod gekomen.

Ook moet aandacht worden besteed aan of de huidige selectie van initiatieven wel het volledige Nederlandse bedrijfsleven omvat. Door het selecteren van de topsectoren zijn in ieder geval de kennisintensieve bedrijven betrokken. Meerdere bronnen geven aan dat eerst de prioriteit moet liggen bij het verbeteren van de informatiepositie van de topsectoren. Door het selecteren van de brancheverenigingen is een groot deel van het Nederlandse bedrijfsleven betrokken. Echter, omvat dit niet het volledige Nederlandse bedrijfsleven, omdat er ook bedrijven zijn die geen lid zijn van een branchevereniging en niet behoren tot een topsector.

[8] TNO-rapport – *Verkenning Cybersecurity Informatiedeling binnen de topsectoren*, Auke Huistra en Tjarda Krabbendam-Hersman, TNO (mei 2017)

[9] WODC-rapport – *Challenges around Measuring Cybersecurity Threats in the Netherlands*, Rémon Cornelisse, Mortaza S. Bargh en Sunil Choenni, WODC (verwachting 2017)

De verantwoordelijkheid voor cybersecurity ligt ondanks de komst van een DTC bij de bedrijven zelf. Het aangesloten zijn op een cybersecurity gerelateerde informatie-uitwisseling ontneemt niet de verantwoordelijk van cybersecurity voor het bedrijfsleven. Elk individueel bedrijf is juridisch gezien aansprakelijk en verantwoordelijk voor cybersecurity.

8.3 AANBEVELINGEN

Dit onderzoek geeft een aantal aanbevelingen voor vervolgonderzoek. Deze aanbevelingen zijn gebaseerd op inzichten die zijn verkregen tijdens dit onderzoek, maar konden vanwege de beperkingen van dit onderzoek niet worden meegenomen.

8.3.1 VEILIGHEIDSREGIO´S

Op termijn kunnen de veiligheidsregio's een positie in het model innemen. Vervolgonderzoek moet uitwijzen welke functionaliteit past binnen de taken van de veiligheidsregio. Het staat vast dat de veiligheidsregio's zich moeten verdiepen in het thema cybersecurity. Een functie waaraan kan worden gedacht is een gedeelde SOC en/of CERT, die ondersteuning biedt aan de regionale initiatieven. Ook een ISAC functionaliteit moet worden verkend, daar zal wel afstemming moeten plaatsvinden met de regionale initiatieven

8.3.2 EIGEN VERANTWOORDELIJKHEID

Het bedrijfsleven moet bewust worden van de eigen verantwoordelijkheid die cybersecurity met zich meebrengt. Het is van belang dat op een positieve manier de aandacht van het bedrijfsleven wordt gewonnen. Een negatieve benadering kan een tegeneffect bewerkstelligen, zoals de respondenten hebben aangegeven. Vervolgonderzoek moet uitwijzen op welke wijze het bedrijfsleven benaderd kan worden om het awareness niveau met betrekking tot cybersecurity te kunnen verhogen.

8.3.3 FISCALE VOORDELEN

Om het bedrijfsleven te laten aansluiten bij het DTC is het belangrijk dat er een hele lage tot aan nihile instap barrière wordt gevormd. Het bedrijfsleven moet de toegevoegde waarde van cybersecurity inzien alvorens het wil aansluiten. Het aanbieden van fiscale voordelen kunnen een stimulerende werking hebben. Aangezien ieder bedrijf verantwoordelijk is voor zijn eigen cybersecurity moet er een juiste balans worden gevonden tussen fiscale voordelen en de eigen verantwoordelijkheid van het bedrijf. Het rapport *"Nederland digitaal droge voeten"* adviseert om 10% van het IT-budget als maatstaf te nemen. Vervolgonderzoek moet uitwijzen of in bepaalde gevallen en onder bepaalde voorwaarden fiscale voordelen te geven aan het bedrijfsleven. Voor de overheid is dit het overwegen waard in het kader van de stabiliteit van het economisch en maatschappelijk belang. Hierbij kan worden gedacht aan fiscale voordelen via het belastingstelsel te denken valt aan het verlagen van het BTW tarief van 21% naar 6% voor veiligheidsverhogende investeringen, subsidie, medefinanciering en/of een financiële impuls voor brancheorganisaties.

8.3.4 CERTIFICEREN VAN DIENSTVERLENERS

Steeds meer ICT-toepassingen zullen met elkaar worden verbonden. Hierdoor is geen enkele organisatie meer in staat om alle taken zelf uit te voeren. Een consequentie hiervan is dat de afhankelijkheid van andere bedrijven en dienstverleners toeneemt, zoals eerder te lezen is in hoofdstuk 3. Het bedrijfsleven is hierdoor grotendeels afhankelijk van dienstverleners. Het certificeren van dienstverleners kan leiden tot een hogere mate van digitale weerbaarheid bij het bedrijfsleven. Vervolgonderzoek moet uitwijzen op welke wijze of het noodzakelijk is om dienstverleners te certificeren. En zo ja, op welke wijze certificering mogelijk moet worden gemaakt.

8.3.5 EVALUATIE VEILIGINTERNETTEN.NL

Tijdens dit onderzoek is steeds duidelijker geworden dat de website veiliginternetten.nl een voorloper is van het DTC. Veilig internetten is een website waar burgers en het bedrijfsleven tips, tricks en praktische stap voor stap uitleg kunnen vinden over wat zij kunnen doen en laten om veilig te internetten. Vervolgonderzoek moet uitwijzen of de website veiliginternetten.nl door het bedrijfsleven veelvuldig wordt gebruikt. En zo ja, dan moet worden onderzocht op welke wijze de website kan bijdrage aan het DTC en/of de website hier kan worden ondergebracht.

VOORTGANG ONDERZOEK

Met de afsluiting van dit hoofdstuk is het onderdeel onderzoeksrapport en de fase rapporteren afgerond. In het voorgaande hoofdstuk is het onderdeel onderzoeksrapport voortgezet. Alle fasen en onderdelen van de onderzoeksopzet zijn doorlopen.

Afbeelding 11: Voortgang onderzoek

LITERATUURLIJST

ACM. (2017, 04 12). *Concurrentie door overheden*. Opgeroepen op 04 12, 2017, van Autoriteit Consument & Markt: https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concurrentie-door-overheden/als-overheden-concurreren/

Baloo, J. (2017, 02 10). *Vergroot je cyberweerbaarheid*. Opgeroepen op 04 22, 2017, van KPN Security: https://www.kpn.com/zakelijk/blog/vergroot-je-cyberweerbaarheid.htm

BIG6. (2017, 02 09). *What is the Big6?* Opgehaald van BIG6: http://big6.com/pages/about.php

Bruijn, J. d., Kickert, W., & Koppenjan, J. (1993). *Netwerkmanagement in het openbaar bestuur, over de mogelijkheden van overheidssturing in beleidsnetwerken.* Den Haag: VUGA Uitgeverij.

CBS. (2016). *ICT, kennis en economie 2016.* Den Haag: Centraal Bureau voor de Statistiek.

Cornelisse, R., Bargh, M., & Choenni, S. (verwachting 2017). *Challenges around Measuring Cybersecurity Threats in the Netherlands.* Den Haag: WODC.

Cropper, S. (1996). *'Collaborative working and the issue of sustainability' In: Creating Collaborative Advantage.* Londen: Sage Publications.

CSR. (2016, 07 11). Digitale ketenveiligheid krijgt veel te weinig aandacht. Den Haag.

Deloitte. (2016). *Digital Infrastructure in the Netherlands - Driver for the Online Ecosystem.* Amsterdam: Deloitte.

DHPA, DDA, ISPConnect en theMETISfiles. (2017). *Fundament van onze digitale economie.* DHPA, DDA, ISPConnect en theMETISfiles.

Europese Commissie. (2003, 05 06). Aanbeveling van de commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen. Brussel, België.

F4analyse. (2017, 04 22). *F4analyse*. Opgeroepen op 04 22, 2017, van https://www.audiotranskription.de/f4-analyse

F5transkript. (2017, 02 09). *f4 & f5transkript*. Opgehaald van Audiotranskription.de: https://www.audiotranskription.de/english/f4.htm

Gartner. (2017, 04 12). *Adaptive Security Architecture*. Opgeroepen op 04 12, 2017, van Gartner: https://www.gartner.com/doc/reprints?id=1-279SLRJ&ct=150109&st=sb

Glaser, B., & Strauss, A. (1999). *The Discovery of Grounded Theory.* Transaction Publishers.

Huistra, A., & Krabbendam-Hersman, T. (2017). *TNO-rapport Verkenning Cybersecurity Informatiedeling binnen de topsectoren.* Den Haag: TNO.

Huxham, C. (1996). *Creating Collaborative Advantage.* Londen: Sage Publications.

Kaarts, E., & Opheij, W. (2012). *Leren samenwerken tussen organisaties.* Deventer: Kluwer.

Koppenjan, J., & Klijn, E. (2004). *Managing Uncertainsties in Networks.* Londen: Routledge.

kst-34300-XIII-45. (2015, 10 15). Tweede Kamer der Staten-Generaal, Motie van het lid Verhoeven. *Vaststelling van de begrotingsstaten van het Ministerie van Economische Zaken (XIII) en het Diergezondheidsfonds (F) voor het jaar 2016*. Den Haag.

McGuire, M. (2006). *Collaborative Public Management: Assessing What We Know and How We Know It.* Bloomington: Indiana University.

Ministerie van Justitie. (2017, 04 22). *Wet veiligheidsregio's*. Opgeroepen op 04 22, 2017, van Overheid.nl: http://wetten.overheid.nl/BWBR0027466/2017-01-01

MKB-Nederland. (2017, 03 02). *Wat houdt ketenverantwoordelijkheid in?* Opgeroepen op 03 02, 2017, van MKB Servicedesk: http://www.mkbservicedesk.nl/4020/wat-houdt-ketenverantwoordelijkheid.htm

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid.* Den Haag: Rathenau Instituut.

NCSC. (2017, 04 22). *Deelname aan een ISAC*. Opgeroepen op 04 22, 2017, van Nationaal Cyber Security Centrum: https://www.ncsc.nl/samenwerking/deelname-aan-een-isac.html

NCSC. (2017, 01 19). *Wat is het NCSC?* Opgeroepen op 01 19, 2017, van Nationaal Cyber Security Centrum: https://www.ncsc.nl/organisatie

Nederlands Comité voor Ondernemerschap en Financiering. (2016). *Staat van het MKB: Jaarbericht 2016.* Den Haag: Ministerie van Economische Zaken.

Rijksoverheid. (2011). *Staatblad, nr. 162.* Den Haag: De Tweede Kamer der State Generaal.

Rijksoverheid. (2012, 01 12). *Nationaal Cyber Security Centrum (NCSC) bundelt kennis en expertise.* Opgeroepen op 01 19, 2017, van http://www.rijksoverheid.nl: https://www.rijksoverheid.nl/actueel/nieuws/2012/01/12/nationaal-cyber-security-centrum-ncsc-bundelt-kennis-en-expertise

Rijksoverheid. (2016). *Beleidsreactie Staatssecretaris Dijkhoff op Cyber Security Beeld Nederland 2016.* Den Haag: NCTV.

RUG. (2017, 02 09). *Bronnen voor literatuuronderzoek*. Opgehaald van Bron- en literatuurgebruik: http://www.rug.nl/society-business/language-centre/academische-communicatievaardigheden/hacv/schriftelijke-vaardigheden/voor-studenten/bronnen-literatuur/literatuur-onderzoek

Security.nl. (2017, 04 22). *Kabinet trekt 55 miljoen uit voor Nationaal Detectie Netwerk*. Opgeroepen op 04 22, 2017, van Security.nl: https://www.security.nl/posting/494352/Kabinet+trekt+55+miljoen+uit+voor+Nationaal+Detectie+Netwerk

Spidalieri, F., & Hathaway, M. (2017). *The Netherlands Cyber Readiness at a Glance.* Arlington: Potomac Insitute for Policy Studies.

Spoelstra, F. (2013). *Integrale aanpak hennepkwekerijen Den Haag - Over het creëren van meerwaarde in interorganisationele samenwerking.* Rotterdam: Flori Spoelstra.

Vangen, S., & Huxham, C. (2003). *Nurturing Collaborative Relations: Building Trust in Interorganizational Collaboration.* Sage Publications.

Vangen, S.; Huxham, C. (2005). *Managing to Collaborate: The theory and practice of collaborative advantage.* Londen: Routledge.

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity.* Den Haag: H.W.P.M.A. (Herna) Verhagen, op verzoek van de Cyber Security Raad.

Verhoeven, N. (2014). *Wat is onderzoek? Praktijkboek voor methoden en technieken.* Amsterdam: Boom Lemma Uitgevers.

BIJLAGEN

BIJLAGE I – KENMERKEN SAMENWERKINGSVERBANDEN

BIJLAGE II – TOPICLIST INTERVIEWS

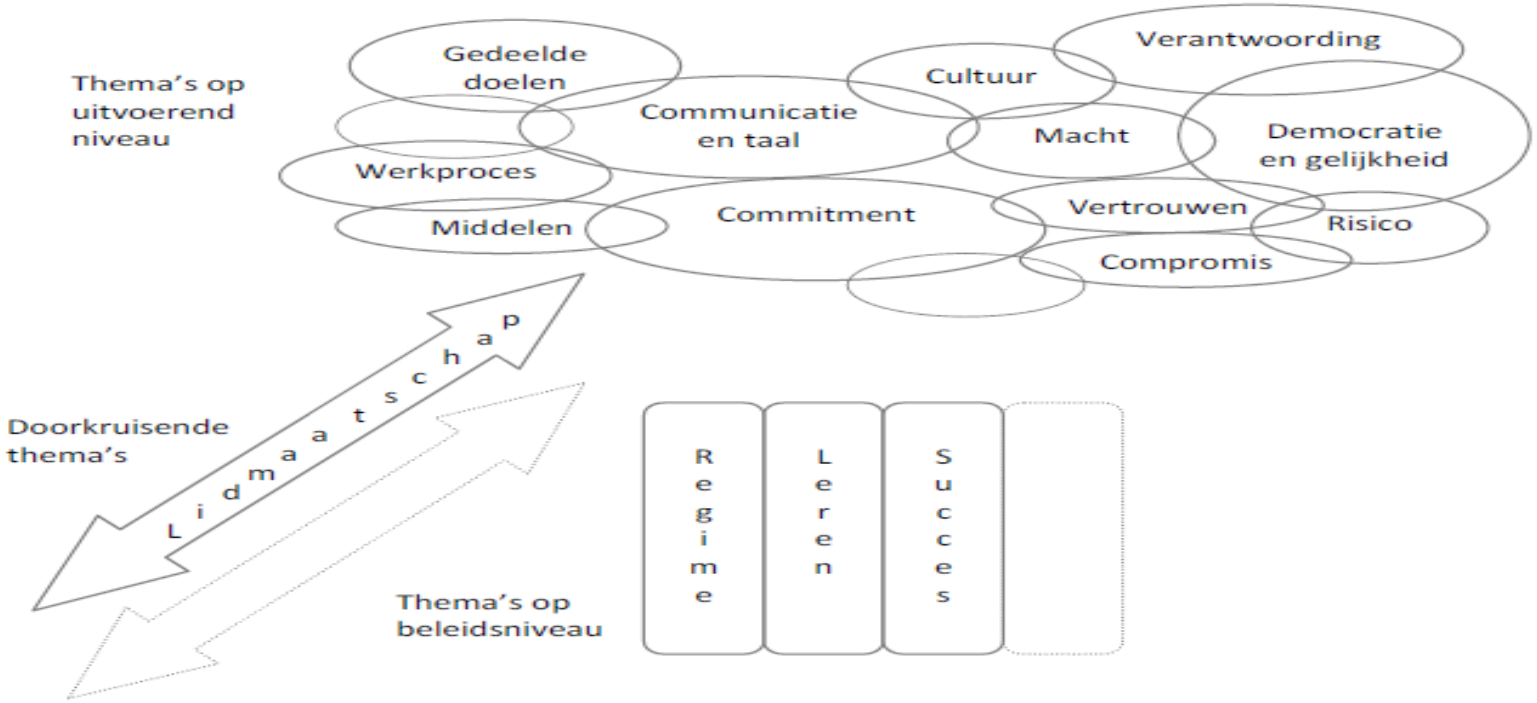
BIJLAGE III – PUBLIEKE RESPONDENTEN

BIJLAGE IV – CAMISO

BIJLAGE I – KERNMERKEN SAMENWERKINGSVERBANDEN

Onderstaand zijn de kenmerken van samenwerkingsverbanden (Spoelstra, 2013) bijgevoegd.

Deze bijlage behoort toe aan paragraaf 3.2 van dit document.



BIJLAGE II – TOPICLIST

Onderstaand is een voorbeeld topiclist bijgevoegd. De onderzoeker heeft binnen elk thema de vragen afgestemd op de specifieke situatie van de respondent.

Deze bijlage behoort toe aan paragraaf 4.2 van dit document.

INTRODUCEREN

- Kennismaking/introduceren
- Toestemming voor opname interview
- Onderzoek en onderwerp inleiden
- Doelstelling en structuur interview
- Informeren over de dataverwerking

DIGITALISERING

- Welke kansen biedt digitalisering Nederland?
- Welke bedreigingen ziet u voor de digitalisering?
- Welke acties zouden ondernomen moeten worden?

UW MODEL

- Welke gedachte lag aan uw model ten grondslag?
- Waarom heeft u voor deze inrichting gekozen en waren er alternatieve beschikbaar?
- Welke randvoorwaarden heeft u destijds gesteld om het vertrouwen te waarborgen?
- Wat moet volgens u de volgende stap zijn om Nederland weerbaarder te maken?

MIJN MODEL

- Welke partijen zouden bij deze aanpak moeten worden betrokken?
- Wat zijn uw ideeën en opvattingen over de inrichting van het model?

AFSLUITEN

- Bedanken voor tijd en informatie
- Toestemming voor contact bij aanvullende vragen

BIJLAGE III – PUBLIEKE RESPONDENTEN

Onderstaand is de lijst van publieke respondenten bijgevoegd.

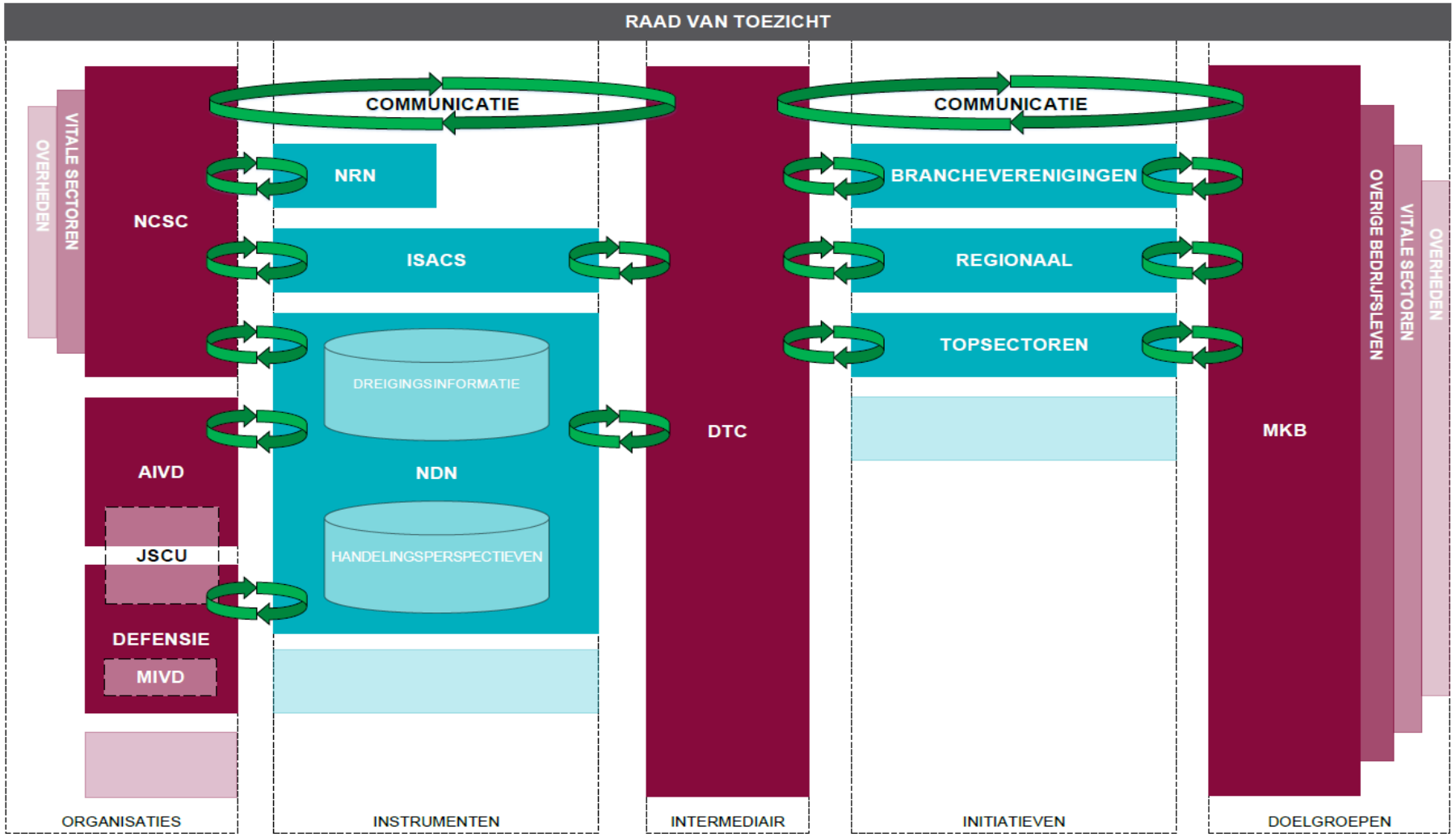
Deze bijlage behoort toe aan paragraaf 4.2 van dit document.

NAAM	ORGANISATIE
Stijn Grove	Dutch Datacenter Association
Auke Huistra	TNO
Tjarda Krabbendam-Hersman	TNO
Piet Bel	Eindhoven Cyber Security Group
Sarah Olierook	Port of Rotterdam

BIJLAGE IV – CAMISO

Onderstaand is het Collaboration Architecture Model of Information Sharing Organizations (CAMISO) bijgevoegd.

Deze bijlage behoort toe aan paragraaf 6.2 van dit document.



DISCLAIMER:

Dit onderzoek is uitgevoerd in opdracht van mw. drs. E.C. van den Heuvel, Secretaris Cyber Security Raad, namens Bureau Secretaris van de Cyber Security Raad. De uitkomsten van dit onderzoek staan los van meningen, opvattingen en/of adviezen van de Cyber Security Raad.

Dit onderzoek is uitgevoerd op persoonlijke titel van de auteur.