Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2017 R10316

Verkenning Cybersecurity Informatiedeling binnen de Topsectoren

Datum 7 maart 2017

Auteur(s) A.W. Huistra
T.H.E.E.A. Krabbendam-Hersman

Samenvatting

De topsectoren zijn negen gebieden waar het Nederlandse bedrijfsleven en onderzoekscentra wereldwijd uitblinken. Bedrijven, onderzoeksinstellingen en de overheid werken in deze topsectoren samen aan kennis en innovatie om de internationale toppositie te behouden. Net als de rest van de samenleving zijn de bedrijven in de topsectoren sterk gedigitaliseerd. Nederland is een digitale koploper in de wereld en één van de '*most connected countries in the world*'.
De digitalisering brengt economische kansen met zich mee, maar vraagt ook om het verhogen van de weerbaarheid tegen cyberdreigingen. Door digitalisering zijn de bedrijven in de topsectoren in toenemende mate afhankelijk van informatie- en communicatietechnologie en daarmee kwetsbaar voor zowel discontinuïteit als diefstal van intellectueel eigendom. Inlichtingendiensten hebben digitale spionage waargenomen op bedrijven, overheden en organisaties binnen de topsectoren.

Binnen het TNO Vraaggestuurd Programma Cyber Risk Management and System Resilience is een verkenning uitgevoerd naar de behoefte en de noodzaak voor het delen en analyseren van informatie over cyberdreigingen binnen de topsectoren. Onderdeel daarvan was een quick scan naar bestaande buitenlandse good practices.

Uitkomst van de verkenning is dat binnen de structuur van de topsectoren cybersecurity op dit moment geen prominent onderwerp is. Cybersecurity informatiedeling vindt niet of slechts in beperkte mate plaats. Voor de sectoren Agri & Food, Creatieve Industrie, Life Sciences & Health en Tuinbouw & Uitgangsmaterialen is aangegeven dat cybersecurity op dit moment niet standaard wordt meegenomen bij het ontwikkelen van nieuwe innovaties. Binnen de topsector High Tech Systemen & Materialen (HTSM) is cybersecurity een onderwerp dat onder andere door de brancheverenigingen FME wordt opgepakt. Binnen deze topsector vindt binnen de Roadmap Security tevens kennisopbouw ten aanzien van cybersecurity plaats. De volgende stap, namelijk het verkrijgen van dreigingsinformatie en het bieden van handelingsperspectieven aan bedrijven die deel uit maken van deze topsector is nog niet sectoraal gezet. Binnen de (top)sectoren Chemie, Energie, Logistiek (Schiphol en de Rotterdamse Haven) en Water (Drinkwater en Keren en Beheren Oppervlaktewater) bestaan Information Sharing and Analysis Centres (ISAC's), waar cybersecurity informatiedeling plaatsvindt. De deelnemers in de ISAC's zijn veelal (chief) information security officers van hiervoor geselecteerde bedrijven. Deze ISAC's zijn echter niet opgezet vanuit het perspectief van de topsector, maar in verband met het vitale karakter van de sector. Niet alle organisaties uit de sector zijn betrokken in een ISAC. Dit geldt voor de niet als vitaal aangemerkte organisaties (de meerderheid). Daarbij ligt de nadruk in de ISAC's meer op de business continuïteit en minder op innovatie.

Op basis van het onderzoek kan worden geconcludeerd dat de topsectoren extra aandacht moeten gaan geven aan cybersecurity en de mogelijke impact die digitale dreigingen kunnen hebben op hun business. Hiervoor is het belangrijk dat het onderwerp niet alleen op de agenda staat van de information security officers, maar ook van de innovatiemanagers en het senior management van bedrijven en onderzoeksinstellingen uit de topsectoren.

Om de cybersecurity uitdagingen van onze digitale samenleving het hoofd te kunnen bieden, is inzicht in kwetsbaarheden en dreigingen cruciaal. Op basis van voldoende actuele en juist informatie en gedegen analyse kunnen publieke en private organisaties de juiste maatregelen treffen om zich efficiënt en effectief te beschermen. Dit geldt niet alleen voor vitale sectoren maar ook voor niet-vitale sectoren. Daarbij zijn de topsectoren slechts één manier om deze grote groep bedrijven te categoriseren en dekt dit lang niet de hele niet-vitale groep bedrijven. Er zijn namelijk ook andere manieren om die grote groep private organisaties te clusteren, zoals per branche, per geografisch gebied, per keten of naar grootte van de organisatie. Daarom wordt er een aanpak voorgesteld die toepasbaar is op een topsector, maar die net zo goed op elk ander soort samenwerkingsverband kan worden toegepast. Slechts op die manier kan Nederland komen tot een dekkend netwerk van organisaties die informatie over cybersecurity dreigingen en oplossingen kan uitwisselen. Hiermee zal Nederland weerbaarder worden tegen digitale dreigingen.

Het onderzoek toont de nut en noodzaak aan voor het ontwikkelen en opbouwen van een cybersecurity informatie-uitwisselingsinfrastructuur ten behoeve van de bedrijven en onderzoeksinstellingen in de topsectoren. Belangrijk hierbij is dat deze infrastructuur niet alleen de bedrijven in de topsectoren zelf ten goede komt, maar tevens de ketenpartners en toeleveranciers van die bedrijven, aangezien de bedrijven voor het digitale weerbaarheid daarvan afhankelijk zijn. Ook belangrijk is dat deze infrastructuur goed aansluit bij de huidige structuren zoals die bestaan voor de overheid en de vitale infrastructuren om een goede sluitende aanpak voor Nederland te krijgen. In de uitwerking van dit Nederlandse model zijn met name de Verenigde Staten, het Verenigd Koninkrijk en Duitsland goede voorbeelden.

Inhoudsopgave

1 Inleiding

De topsectoren zijn negen sectoren waarin Nederland wereldwijd toonaangevend is. Binnen de topsectoren werken bedrijven, onderzoeksinstellingen en de overheid samen aan kennis en innovatie om de internationale toppositie te behouden.
Net als de rest van de samenleving zijn ook de topsectoren sterk gedigitaliseerd. Deze digitalisering biedt enorme kansen voor efficiëntie en verbetering, maar vraagt ook om het verhogen van de weerbaarheid tegen cyberdreigingen. Nederland is als een van de meest ICT-intensieve economieën ter wereld, een aantrekkelijk doelwit voor cybercriminelen, cyberspionnen en hackers.[1] Het verhogen van de weerbaarheid van de topsectoren tegen cyberdreigingen bevordert het vestigingsklimaat, de duurzame economische groei en cybersecurity als export product. Het beschermen van intellectueel eigendom, het voorkomen van discontinuïteit in digitale systemen en het behoud van een goede internationale reputatie zijn van groot belang voor de topsectoren.

Om de uitdagingen van het digitale domein het hoofd te kunnen bieden, hebben organisaties inzicht nodig in kwetsbaarheden en dreigingen die voor hen relevant zijn. Op basis van voldoende informatie en gedegen analyse kunnen deze organisaties de juiste maatregelen treffen voor een efficiënte en effectieve bescherming. Dit geldt niet alleen voor de vitale sectoren[2], maar ook voor partijen die deel uit maken van de topsectoren.

Binnen de vitale sectoren wordt informatie over cyberdreigingen uitgewisseld binnen zogenaamde Information Sharing en Analysis Centres (ISAC's).
Hierin nemen zowel private als publieke organisaties deel. De publieke partijen zijn onder andere het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Team High Tech Crime van de politie. De organisaties in de vitale sectoren gebruiken de gedeelde informatie om hun eigen risicoanalyse te maken. Op basis hiervan nemen bedrijven in de vitale sectoren passende maatregelen.

Binnen het TNO Vraaggestuurd Programma Cyber Risk Management en System Resilience is de verkenning uitgevoerd naar de behoefte en de noodzaak voor het delen en analyseren van informatie over cyberdreigingen binnen de topsectoren. Het onderzoek maakt onderdeel uit van de programmalijn Cyber Threat Intelligence Sharing waarin methoden voor het delen van cybersecurity informatie worden onderzocht.

De centrale onderzoeksvragen van de verkenning zijn:
- Is er behoefte en noodzaak voor het oprichten van een infrastructuur voor het delen van cybersecurity informatie voor de topsectoren in Nederland?
- Zo ja, is de bestaande topsectoren structuur een organisatievorm om dit op te pakken of zijn er andere organisatievormen om cybersecurity in de topsectoren op een hoger peil te brengen?

---

1 https://www.aivd.nl/actueel/nieuws/2017/03/02/rapport-rathenau-overheid-en-bedrijven-onvoldoende-beschermd-tegen-cyberdreigingen

2 https://www.nctv.nl/binaries/18.factsheet-vitale-infrastructuur_tcm31-32336.pdf

- Is het ISAC model dat voor overheid en vitale infrastructuur wordt gebruikt een model dat hiervoor gebruikt kan worden of zijn er andere modellen meer geschikt?
- Welke good practices zijn er te vinden in het buitenland die passen op de Nederlandse situatie en hoe zouden deze op de Nederlandse situatie toegepast kunnen worden?

2 Verantwoording aanpak

In dit onderzoek zijn vertegenwoordigers vanuit de topsectoren geïnterviewd, alsmede diverse vertegenwoordigers vanuit brancheverenigingen. Dit geldt eveneens voor relevante stakeholders vanuit de overheid, zoals ministerie van Economische Zaken, ministerie van Veiligheid en Justitie, VNO NCW en uitvoeringsdiensten.[3]

Daarnaast is een quick scan gedaan waarbij diverse good practices uit landen, die een voortrekkerspositie op gebied van cybersecurity hebben, zijn bestudeerd zoals:

- Cyber-Security Information Sharing Platform (CiSP) in het Verenigd Koninkrijk[4]
- Information Exchanges van CPNI in het Verenigd Koninkrijk
- Information Sharing and Analysis Centres (ISAC) in Nederland
- Information Sharing and Analysis Centers (ISAC) in de Verenigde Staten[5]
- Information Sharing and Analysis Organizations (ISAO) in de Verenigde Staten[6]
- Reporting and Analysis Centre for Information Assurance MELANI in Zwitserland[7]
- Umsetzungsplan KRITIS (UP-Kritis) in Duitsland[8]
- Alliance for Cybersecurity in Duitsland[9]
- Cooperation Group for Information Security (SAMFI) in Zweden[10]
- National Emergency Supply Agency (NESA) in Finland[11]
- ENISA onderzoek 'Incentives and Challenges to Information Sharing[12]
- TNO Publicatie ten behoeve van GCCS2015 'Sharing Cyber Security Information'[13]

---

3 Zie het totaal overzicht in bijlage A.
4 https://www.ncsc.gov.uk/cisp
5 https://www.nationalisacs.org/
6 https://www.isao.org/
7 https://www.melani.admin.ch/melani/en/home.html
8 http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html
9 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
10 https://rib.msb.se/Filer/pdf/26177.pdf
11 https://tapahtumat.tekes.fi/uploads/3ef8185/savisalo_security_of_supply-1506.pdf
12 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
13 https://www.tno.nl/en/focus-areas/defence-safety-security/cyber-security-resilience/sharing-cyber-security-information/

3 Cybersecurity informatiedeling

3.1 Voordelen van het delen van Cybersecurity informatie

Alvorens in te gaan op de vraag wat volgens de betrokken partijen uit de topsectoren de meerwaarde zou kunnen zijn van het delen van cybersecurity informatie is het van belang om dit allereerst vanuit het maatschappelijke perspectief te bekijken. Nederland is een digitale koploper in de wereld en één van de '*most connected countries in the world*'[14]. De digitalisering brengt grote economische en maatschappelijke kansen met zich mee. Om die kansen te kunnen blijven benutten, is het noodzakelijk dat we vertrouwen hebben in de digitale wereld en ons er veilig kunnen bewegen. Dit wordt aangehaald in het rapport "De economische en maatschappelijke noodzaak voor meer Cyber Security: Nederland Digitaal Droge Voeten"[15]. Herna Verhagen CEO van PostNL heeft dit rapport opgesteld op verzoek van de Cyber Security Raad. Het rapport omschrijft de noodzaak voor versterking van publiek-private samenwerking en het delen van informatie op het gebied van cybersecurity:

"Samenwerking tussen bedrijven en overheid op het gebied van cybersecurity moet worden verstevigd en geïnstitutionaliseerd. Informatie-uitwisseling op het gebied van ongeoorloofd gebruik, kwetsbaarheden in systemen, criminaliteit of spionage in de digitale wereld moet worden bevorderd. Veiligheid borgen begint bij het monitoren van dreigingen en risico's, vervolgens voorkomen en eindigt bij het opsporen van criminele actoren en vervolging van criminelen. Een essentiële eerste stap voor snelle, adequate reacties op misstanden of aanvallen (respons) en preventieve maatregelen is daarom detectie en onderzoek naar cyberaanvallen te intensiveren.
Nederland moet in staat zijn snelle en accurate impactanalyses te maken om schade te beperken en succesvol attributie-onderzoek uit te voeren om daders te identificeren. Die […] samenwerking is te bewerkstelligen door uitbreiding van de eerder genoemde structuur van ISAC's naar andere delen van de economie, met name naar de kennisintensieve bedrijven."

Zowel de vitale infrastructuren als ook de niet vitale infrastructuren zijn in toenemende mate afhankelijk van informatie- en communicatietechnologie (ICT) of, in het kort, cyber. Cyberveiligheid en veerkracht worden gezien als steeds belangrijkere onderwerpen voor het bestuur. Het is een van de belangrijkste uitdagingen voor de samenleving van vandaag. Daarbij verandert het dreigingslandschap voortdurend. Informatie-uitwisseling tussen organisaties - in een vitale sector, cross-sector, nationaal en internationaal - wordt over het algemeen gezien als een effectieve maatregel om de digitale weerbaarheid van organisaties, sectoren en de samenleving te verhogen.

Het delen van informatie is echter niet een eenvoudig onderwerp. Het komt met vele facetten. Het delen van informatie:

- raakt het strategisch, tactisch, operationeel en technisch niveau;
- omvat alle fasen van de cyber incident response-cyclus (proactie, preventie, preparatie, incident response, herstel, nazorg / follow-up);

---

[14] Digital globalization: the new era of global flows: McKinsey Institute: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows
[15] Nederland Digitaal Droge Voeten – adviesrapport cyber security https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf

- is zeer dynamisch;
- overstijgt de grens van publieke en private domein;
- heeft een dilemma in zich, aangezien het veelal gaat over gevoelige informatie, die schadelijk kan zijn voor een organisatie, terwijl ze zeer nuttig zijn voor anderen.

3.2 Information Sharing & Analysis Centres

Om een gepaste oplossing te formuleren voor de aanpak van cyberdreigingen en kwetsbaarheden, zijn in Nederland voor de vitale sectoren Information Sharing and Analysis Centres (ISAC's) opgericht. ISAC's zijn publiek-private samenwerkingsverbanden en zijn per sector georganiseerd. De ISAC's worden gefaciliteerd door het Nationaal Cyber Security Centrum[16]. 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. Het delen van informatie vindt plaats onder een strikte set van spelregels. De kruisbestuiving tussen publieke en private sector levert toegevoegde waarde voor alle deelnemers. Een belangrijke meerwaarde voor alle deelnemers is het opbouwen van een permanent netwerk. Ook buiten de ISAC-bijeenkomsten weten de deelnemers elkaar te vinden voor informeel overleg en uitwisseling van kennis en intelligence. Met behulp van deze 'extra' informatie zijn de deelnemende organisaties beter in staat om hun eigen risicoanalyse uit te voeren en passende maatregelen te treffen.

3.3 Buitenlandse good practices

In het buitenland zijn diverse modellen ontwikkeld voor de uitwisseling van informatie op het gebied van cyber security ook richting het niet-vitale deel van de samenleving. In het kader van dit onderzoek is een scan gemaakt van initiatieven voor informatiedeling op het gebied van cybersecurity. Daarbij is zowel naar modellen gekeken die gericht zijn op vitale sectoren als ook die gericht zijn op het niet-vitale deel van de samenleving. In de analyse zijn de cybersecurity informatiedelingsmodellen uit de volgende landen bestudeerd: Verenigd Koninkrijk, Verenigde Staten, Finland, Zweden, Zwitserland, Duitsland en Oostenrijk. Per land is gekeken naar de verschillende modellen initiatieven en in hoeverre deze als voorbeeld voor Nederland kunnen dienen. Zie in bijlage C de uitgebreide versie van de uitkomsten van deze analyse. De Nederlandse situatie vindt het meest aansluiting bij de modellen uit de Verenigde Staten, het Verenigd Koninkrijk en Duitsland.

In het verleden is het Nederlandse ISAC model ontwikkeld op basis van de ervaringen en richtlijnen van soortgelijke initiatieven in de Verenigde Staten (ISAC's) en het Verenigd Koninkrijk (Information Exchanges binnen CPNI). Duitsland heeft in een later stadium het UP KRITIS model ontwikkeld. Al deze initiatieven waren gericht op de vitale infrastructuren.

De laatste tijd hebben deze drie landen daar informatiedelingsmodellen naast gezet die gericht zijn op niet-vitale onderdelen van de maatschappij.

[16] https://www.ncsc.nl/samenwerking/isacs.html

Zo is in de Verenigde Staten het ISAO-model ontwikkeld voor het niet-vitale deel van de samenleving. Hierbij delen groepen organisaties die iets gemeen hebben (sector, keten, regio) informatie over cyberdreigingen. Een centrale cyber fusion cel speelt daarbij een belangrijke rol om de informatie specifiek en actionable te maken voor de organisaties in de ISAO. De Amerikaanse overheid voedt deze ISAO's met informatie, maar faciliteert ze niet zelf. Het ISAO model sluit daarbij aan op de ISAC structuur dat al langer in de VS bestaat en in het verleden ook inspiratie is geweest voor de Nederlandse ISAC structuur. Zoals beschreven kent het Verenigd Koninkrijk al lange tijd het stelsel van Information Exchanges voor de vitale sectoren. Deze zijn opgegaan in het CiSP (als onderdeel van het National Cyber Security Centre). Vanuit het CiSP wordt ook een platform aangeboden voor niet vitale organisaties om informatie onderling en met de overheid te delen.
Duitsland kent naast UP KRITIS een Alliance for Cybersecurity die zich richt op de brede gemeenschap. Deze drie landen horen tot de koplopers op het terrein van cyber security. De gehanteerde modellen dienen als input voor de ontwikkeling van een Nederlandse cybersecurity informatie-uitwisselingsmodel.

Overigens zijn er in Nederland ook al verschillende initiatieven om het niet-vitale deel van de Nederlandse samenleving digitaal weerbaar te maken en te houden. Deze zijn voornamelijk gericht op het delen van kennis (bijv. good practices) en het creëren van awareness. De focus ligt niet of nauwelijks op informatiedeling op het gebied van bijvoorbeeld incidenten en kwetsbaarheden.

In onderstaande tabel is de globale indeling weergegeven van de cybersecurity informatiedeling initiatieven in de Verenigde Staten, het Verenigd Koninkrijk, Duitsland en Nederland:

Land	**Vitaal**	**Niet-vitaal**
Verenigde Staten	ISAC's	ISAO
Verenigd Koninkrijk	Information Exchanges	CiSP
Duitsland	UP KRITIS	Alliance for Cybersecurity
Nederland	ISAC's	Diverse initiatieven op gebied van kennisdeling en awareness zoals: • Alert Online campagne • veiliginternetten.nl • veiligbankieren.nl • veiligzakelijkinternetten.nl

4 Topsectoren en cybersecurity

4.1 Topsectoren

Nederland staat op het gebied van handel en industrie aan de wereldtop.
We verdienen veel van ons geld in het buitenland, maar onze toppositie is niet vanzelfsprekend. We zullen concurrerend moeten blijven. Alleen dan is duurzame economische groei mogelijk. Dat doen we door te investeren in de negen sectoren waarin we wereldwijd toonaangevend zijn: de topsectoren.

Zoals in hoofdstuk 1 reeds genoemd zijn de topsectoren negen sectoren waarin Nederland wereldwijd toonaangevend is. De digitalisering biedt enorme kansen voor efficiëntie en verbetering. Het verhogen van de weerbaarheid van de topsectoren tegen cyberdreigingen bevordert het vestigingsklimaat, de duurzame economische groei en cybersecurity als export product. Het beschermen van intellectueel eigendom, het voorkomen van discontinuïteit in digitale systemen en het behoud van een goede internationale reputatie zijn van groot belang voor de topsectoren.

De kracht van de topsectorenaanpak zit niet alleen in de samenwerking tussen ondernemers, onderzoekers en overheden binnen de verschillende topsectoren. Ook de kruisbestuivingen tussen topsectoren hebben aantoonbaar meerwaarde. Zo wordt er samengewerkt om de beste producten en diensten te realiseren (innovatie), talenten aan te trekken (human capital) en de sectoren goed internationaal te positioneren (Holland trade).

De negen topsectoren zijn:
- Agri & Food
- Chemie
- Creatieve industrie
- Energie
- High Tech Systemen & Materialen
- Life Sciences & Health
- Logistiek
- Tuinbouw & Uitgangsmaterialen
- Water

Zie in bijlage B een korte omschrijving per topsector.

4.2 Cyberdreigingen voor topsectoren

Nederland is kwetsbaar voor digitale dreigingen en dat geldt niet alleen voor vitale sectoren, maar zeker ook voor de topsectoren. Zo geeft de AIVD in haar reactie[17] op de publicatie van het Cyber Security Beeld Nederland 2016 aan dat digitale spionage het afgelopen jaar weer is toegenomen.

"Deze spionage is gericht op politieke en economische informatie. Dit vormt een belangrijke bedreiging voor de nationale veiligheid en concurrentiepositie van Nederland […] De Nederlandse topsectoren zijn in het afgelopen jaar meermaals het doelwit geweest van digitale spionage. Statelijke actoren blijken grote belangstelling te hebben voor de innovatieve of specialistische technologie waar Nederland bekend om staat. Door deze digitale economische spionage door buitenlandse inlichtingendiensten komt de concurrentiepositie van Nederland onder druk te staan."

Het Cyber Security Beeld Nederland[18] vermeldt dat digitale spionage "vanuit historisch perspectief ongeëvenaard succesvol is geweest en een significante bedreiging voor de nationale veiligheid vormt".

"Volgens de AIVD en MIVD zijn de waargenomen aanvallen slechts het topje van de ijsberg. Het totale aantal gevallen van digitale spionage is vele malen groter. In het afgelopen jaar hebben de inlichtingendiensten veel digitale spionage waargenomen op Nederlandse bedrijven binnen de defensie-industrie en topsectoren als high-tech, chemie, energie, life sciences & health en de watersector. Hierbij is vastgesteld dat de aanvallers op zoek waren naar zeer specialistische technologie en soms zelfs experimentele technologie die zijn marktwaarde nog moet bewijzen. Dit getuigt van structurele en gedetailleerde aandacht voor innovatie-initiatieven in Nederland. Deze technologieën zijn essentieel voor het huidige en toekomstige verdienmodel van de getroffen bedrijven. Dit illustreert de structurele en omvangrijke digitale spionagedreiging tegen het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven. Nederlandse inspanningen op het gebied van onderzoek en ontwikkeling zijn een gewild doelwit voor digitale spionage door statelijke actoren. Hiermee kunnen zij hun economieën draaiende houden, maar ook de krijgsmacht versneld moderniseren. De omvang van de economische schade door digitale spionage op de Nederlandse bedrijven is moeilijk vast te stellen. Ook blijkt dat circa twee derde van de getroffen bedrijven, tot het moment van notificatie door inlichtingendiensten, niet op de hoogte was van deze aanvallen."

4.3 Stand van zaken en behoefte topsectoren

De topsectoren aanpak is gericht op het stimuleren van innovatie en de kansen die het biedt voor de Nederlandse economie. Digitalisering staat hierbij centraal. Denk bijvoorbeeld aan het makkelijker kunnen delen van data binnen een keten, waarmee bijvoorbeeld transporten sneller en efficiënter plaatsvinden. De keerzijde van digitalisering, namelijk de kwetsbaarheid die hierdoor toeneemt, is niet het eerste waar binnen de topsector aandacht aan wordt besteed. De kansen en mogelijkheden staan centraal. Wel worden er vragen gesteld als: 'wie is eigenaar van de data?' en 'wie kan er allemaal bij?'.

De topsectoren aanpak bevordert innovatie. Cybersecurity zou volgens de respondenten een aandachtspunt moeten zijn bij innovatie. Dit is op dit moment nog niet zo georganiseerd. Cybersecurity is op dit moment niet een agendapunt van

[17] https://www.aivd.nl/actueel/nieuws/2016/09/06/csbn-2016-toenemende-digitale-spionage
[18] https://www.nctv.nl/actueel/nieuws/2016/Beroepscriminelen-steeds-groter-gevaar-voor-digitale-veiligheid.aspx

de topteams binnen de topsectoren. Uit gesprekken met betrokkenen komt naar voren dat de sectoren zich (nog) niet voldoende bewust zijn van de risico's die de digitalisering met zich meebrengt. Risicoanalyses voor de sector hebben niet plaatsgevonden. Sectorale risicoanalyses zijn nodig om inzicht te krijgen in de digitale kwetsbaarheden in sector. Tevens geeft dit input voor de te nemen noodzakelijke maatregelen.

De topsectoren HTSM, Water, Energie, Logistiek en Chemie raken aan de vitale sectoren, waar cybersecurity en nationale veiligheid reeds aandacht heeft. Met andere woorden: de bescherming van de vitale infrastructuur heeft aandacht. De bescherming van innovaties (economische veiligheid) heeft (nog) niet de aandacht, die het zou moeten hebben.

De respondenten zijn het allemaal eens dat cybersecurity geagendeerd moet worden bij bedrijven die binnen de topsectoren actief zijn. Dit kan via de topsectorenaanpak, waarbij cybersecurity als randvoorwaarde moet worden meegegeven. Dit kan ook via de brancheverenigingen. De brancheverenigingen zien hier een rol in voor zichzelf richting hun leden. Hiermee worden ook de kleinere bedrijven bereikt. De kleinere bedrijven hebben vaak geen ICT-medewerkers in dienst en zijn volledig afhankelijk van hun ICT-leverancier. Voor deze bedrijven is het belangrijk dat specifiek wordt gemaakt welke risico's ze lopen en welke maatregelen daartegen te nemen zijn. Wij zien de meerwaarde ervan om de agendering van cybersecurity zowel via de brancheverenigingen als via de topsectoren te organiseren. Per (top)sector zal afgewogen moeten worden welke vorm het beste werkt.

De respondenten binnen de sectoren Agri & Food, Creatieve Industrie, Life Sciences & Health en Tuinbouw & Uitgangsmaterialen geven aan dat cybersecurity voor de topsector en de brancheverenigingen een nieuw onderwerp is. Cybersecurity is (nog) niet structureel een aandachtspunt bij het ontwikkelen van nieuwe technologieën. Bij de groeiende onderzoeksgebieden van bijvoorbeeld Smart Agri & Food, BIO Tech en de ontwikkeling van Smart Dairy Farming zou cybersecurity een aandachtspunt moeten zijn. In de creatieve industrie is het beschermen van intellectueel eigendom voor het verdienvermogen van groot belang. Creatieve producten en diensten worden vaak in digitale vorm (liedjes, films, foto's, games, ontwerpen et cetera) gecreëerd en verhandeld.

Informatiedeling over cyberdreigingen vindt in deze vier sectoren niet plaats, sectorale risicoanalyses zijn niet gemaakt. Voor de kleinere spelers is het handzaam om informatie op maat te organiseren. De brancheverenigingen van deze sectoren zijn een goed kanaal om dit verder te organiseren. Op deze manier worden de grote en kleine bedrijven bereikt, ook de bedrijven die niet betrokken zijn bij initiatieven uit de topsectorenaanpak. De creatieve industrie bestaat bijvoorbeeld uit veelal kleine bedrijven, die niet allemaal zijn aangesloten bij de topsectorenaanpak, maar vaak wel bij één van de brancheverenigingen. Volgens de respondenten zou een awareness programma vanuit de brancheverenigingen naar haar leden een eerste stap zijn. Binnen de topsector Life Sciences & Health is LSH Alliance, waarin negen brancheverenigingen uit de sector verenigd zijn, een ingang om cybersecurity op de agenda te krijgen. In de sector Tuinbouw en Uitgangsmaterialen is in 2015 een cybersecurity middag georganiseerd en is een contactgroep onder de leden van de branchevereniging

opgezet. Voor het zetten van een volgende stap, zoals structurele informatiedeling, is hulp nodig.

De topsector High Tech Systemen & Materialen is een topsector die overlapt met andere topsectoren. Een bedrijf in deze topsector kan ook actief zijn in een andere topsector. Denk bijvoorbeeld aan high tech bedrijven in de energiesector. Cybersecurity is een onderwerp dat o.a. door de brancheverenigingen FME wordt opgepakt. De digitalisering van de industrie vraagt om meer aandacht voor cybersecurity. Individuele bedrijven, waaronder vitale bedrijven, pakken cybersecurity op, maar een sectorbrede aanpak ontbreekt. Bovendien hebben bedrijven in de industrie veel vragen over cybersecurity. Met name de kleine bedrijven zijn vaak onvoldoende op de hoogte en weten niet waar ze moeten beginnen. Het verzamelen en analyseren van dreigingsinformatie en het bieden van handelingsperspectieven vindt sectoraal niet plaats. De topsector HTSM biedt een netwerk van relevante bedrijven, maar is niet de plek waar op dit moment cybersecurity op de agenda staat, met uitzondering van de cybersecurity kennisopbouw die plaatsvindt onder de Roadmap Security.

Binnen de (top)sectoren Chemie, Energie, Logistiek en Water bestaan ISAC's, waar structurele cybersecurity informatiedeling plaatsvindt. De deelnemers in de ISAC's zijn veelal (chief) information security officers van hiervoor geselecteerde bedrijven. Voorbeelden van deze ISAC's zijn de Chemie-ISAC, Energy-ISAC, Water-ISAC, Keren en Beheren ISAC, Airport-ISAC (Schiphol) en Haven-ISAC (Rotterdam). Deze ISAC's zijn opgezet in verband met het vitale karakter van de sector.
Lang niet alle organisaties uit zo'n (top)sector zijn betrokken in een ISAC. De niet als vitaal aangemerkte organisaties (de meerderheid) zijn niet betrokken bij de genoemde ISAC. Wat opgemerkt wordt is dat door de toenemende afhankelijkheid van ICT voor cybersecurity en security by design blijvend aandacht gevraagd moet worden. De grote spelers hebben de aandacht voor dit vraagstuk, maar het staat nog lang niet op de agenda van alle spelers. Ook wordt cybersecurity nog onvoldoende intersectoraal aangevlogen.

Om cybersecurity bij meer bedrijven onder de aandacht te brengen is in de sector Logistiek de publicatie 'Cybersecurity voor de logistieke dienstverleners' verspreid. Deze publicatie informeert logistieke dienstverleners over de impact van nieuwe digitale dreigingen.[19]

Door de respondenten is uitgesproken dat het wenselijk is dat (brancheverenigingen en bedrijven binnen) de topsectoren extra aandacht gaan geven aan cybersecurity en de mogelijke impact die digitale dreigingen kunnen hebben op hun business. Hiervoor is het belangrijk dat het onderwerp niet alleen op de agenda staat van de information security officers maar ook op de agenda van de innovatiemanagers en het senior management. De topteams van topsectoren en de brancheverenigingen hebben hierbij behoefte aan een gefaciliteerde aanpak en kennis over cybersecurity, omdat deze veelal niet of onvoldoende aanwezig is.

[19] ABN AMRO, AON, TLN (2016). Cybersecurity voor logistieke dienstverleners.

5 Concept informatiedeling topsectoren

5.1 Uitdagingen

Om de uitdagingen van het digitale domein het hoofd te kunnen bieden, hebben zowel de bedrijven als de overheid inzicht nodig in kwetsbaarheden en dreigingen. Op basis van voldoende informatie en gedegen analyse kunnen organisaties de juiste maatregelen treffen om zich efficiënt en effectief te beschermen. Dit geldt niet alleen voor vitale sectoren, die voor hun informatie-uitwisseling worden gefaciliteerd door het NCSC middels de ISAC's. Ook het deel dat als niet-vitaal is aangemerkt, heeft deze informatie nodig. De bedrijven in de topsectoren vallen voor het grootste deel onder de niet-vitale categorie. Enkele topsectoren overlappen met vitale sectoren, zoals energie en chemie.

Dit onderzoek heeft als eerste focus informatiedeling op het gebied van cybersecurity binnen de topsectoren. Het onderzoek maakt duidelijk dat de bedrijven uit de topsectoren via meerdere routes digitaal weerbaar gemaakt kunnen worden. Naast de topsector als organisatievorm zijn structuren als brancheorganisaties, ketens en regionale of thematische samenwerkingsverbanden geschikt. Op die manier kan Nederland komen tot een dekkend netwerk van organisaties die informatie over cybersecurity dreigingen en oplossingen kan uitwisselen. Hiermee zal Nederland weerbaarder worden tegen digitale dreigingen.

5.2 Succesfactoren

Bij de uitwerking van een Nederlands cybersecurity informatie-uitwisselingsmodel, om de bedrijven uit de topsectoren digitaal weerbaarder te maken, kan worden geleerd van de succesfactoren voor het opbouwen van een ISAC structuur in Nederland. Het is belangrijk om daar te beginnen waar al energie aanwezig is. En bij bijvoorbeeld het kiezen van pilots hier rekening mee te houden. Bij het opstarten van de ISAC's werd de aanpak 'Learning by doing' gevolgd. Door te experimenteren en aan de slag te gaan werd geleerd, zowel van de successen als hetgene dat niet lukt. De leerpunten werden vervolgens weer toegepast. De ISAC's hebben ook geleerd dat er twee kernwoorden zijn voor succesvolle informatie-uitwisseling: Vertrouwen en Waarde[20]. Immers informatie wordt alleen gedeeld met partijen of personen die worden vertrouwd. Partijen nemen alleen deel aan een informatie-uitwisselingsinitiatief als ze er zelf meerwaarde uit halen. Anders neemt de animo snel af. Commitment en continuïteit van de deelnemers draagt bij aan het opbouwen van vertrouwen.

Belangrijk voor het slagen van de ISAC's is de aanwezigheid van een permanent vliegwiel geweest. Aanvankelijk waren dit het programma Nationale Infrastructuur tegen Cyber Crime (NICC) en in een later stadium Centre for the Protection of National Infrastructure (CPNI.NL). Beide initiatieven werden gefinancierd door het ministerie van Economische Zaken. Sinds haar oprichting op 1 januari 2012 is het Nationaal Cyber Security Centrum (ministerie van Veiligheid en Justitie) de facilitator van de ISAC structuur. Een stelsel van informatie-uitwisselingsorganisaties voor de niet-vitale sectoren in Nederland heeft een

[20] Publiek-private samenwerking in het Informatieknooppunt Cybercrime, NICC,2008.

dergelijk vliegwiel ook nodig. De overheid dient hier zeker in de beginfase een stevige rol in te nemen door enerzijds de opstart te faciliteren en anderzijds ook dreigingsinformatie en good practices beschikbaar te stellen. De ervaringen van bijvoorbeeld het NCSC zijn belangrijk bij het inrichten van een fusion center dat de informatiedeling op gang moet brengen en houden door actionable intelligence beschikbaar te stellen.

Het opzetten van de ISAC's heeft uitgewezen dat het hebben van experimenteerruimte en een flexibel onderzoeksbudget belangrijke succesvoorwaarden zijn. Vooraf is namelijk niet altijd precies te bedenken hoe zo'n stelsel het meest effectief opereert. Daarom zijn experimenten nodig. Bij succes kunnen de uitkomsten worden geïmplementeerd, indien niet succesvol worden ze gestopt. Het onderzoeksbudget is bij de ISAC's belangrijk geweest om relevante content en kennis te genereren voor specifieke ISAC's. Voorbeelden hiervan zijn benchmarks in de energie- en drinkwatersector.

Als gevolg van de oprichting van de ISAC's is een publiek-privaat netwerk van professionals ontstaan, die elkaar weten te vinden als het nodig is. Bijvoorbeeld bij incidenten of het doen van aangiftes.

5.3 Oplossingsrichting

In het onderzoek zijn verschillende informatie-uitwisselingsmodellen bekeken in landen als de Verenigde Staten, het Verenigd Koninkrijk, Duitsland, Zwitserland en Zweden. Op basis van die informatie wordt voorgesteld om het Nederlandse stelsel voor cybersecurity informatiedeling voor niet-vitale organisaties te ontwikkelen met behulp van de methodologie en richtlijnen van de Information Sharing and Analysis Organization Standards Organization[21] uit de Verenigde Staten. Andere belangrijke referenties zijn het CiSP model uit het Verenigd Koninkrijk en het Alliance for Cybersecurity uit Duitsland.

Het onderzoek maakt duidelijk dat het belangrijk is het model toepasbaar te maken op de Nederlandse situatie. Daarbij kunnen de ervaringen van het opbouwen van de Nederlandse ISAC structuur alsmede de uitkomsten van een recent gehouden 'Next Generation ISAC' onderzoek worden meegenomen.

Op basis van een aantal criteria lijkt het Amerikaanse ISAO model het best als basis te kunnen fungeren voor de uitwerking van een Nederlands model.
Deze criteria zijn:

- Flexibiliteit en schaalbaarheid: Het ISAO model is flexibel toe te passen op verschillende manieren van clustering. Zowel per topsector, branche, regio, keten als thema. Het model is goed schaalbaar en flexibel in de inrichting. De fusion centers die een belangrijk onderdeel vormen van een ISAO kunnen zowel centraal (binnen de overheid, dan wel privaat) als decentraal worden ingericht.
- Passend bij ISAC's: het ISAO model sluit goed aan op het ISAC model.
- Actionable maken van intelligence: Het ISAO model biedt de beste mogelijkheid om actionable intelligence te genereren en daar te krijgen waar het nodig is, namelijk in de organisaties die de maatregelen moeten treffen. Informatiedeling

[21] ISAO Standards Organization: https://www.isao.org

binnen een relevante clustering van organisaties, biedt hiervoor betere mogelijkheden dan meer generieke informatiedeling naar alle sectoren tegelijk.
- Aansluiting op het NCSC: het fusion center dat in het hart van een ISAO actief is, kan relatief eenvoudig aansluiten op de informatievoorziening van het NCSC. Dit is vergelijkbaar met het model waarop de Informatiebeveiligingsdienst (IBD) is aangesloten op het NCSC.

Zoals gezegd kunnen hierbij in de uitwerking van het Nederlandse model elementen vanuit de modellen van het Verenigd Koninkrijk en/of Duitsland worden toegevoegd.

Information Sharing and Analysis Organisation (ISAO)
In de Verenigde Staten kent men eveneens een stelsel van ISAC's voor de vitale infrastructuren, maar wordt de facilitering niet per definitie gedaan door de Amerikaanse overheid. De meeste ISAC's zijn commerciële initiatieven waarvoor de deelnemers een jaarlijkse bijdrage betalen. Wel vindt er tussen de ISAC's en de Amerikaanse overheid informatie-uitwisseling plaats.

In de Verenigde Staten ontstond echter ook het besef dat het merendeel van de organisaties in de overheid en het bedrijfsleven geen onderdeel uitmaken van een vitale infrastructuur en derhalve ook niet onderdeel waren van een ISAC. Dit leidde ertoe dat het Witte Huis in februari 2015 Executive Order (EO) 13691[22], "*Promoting Private Sector Cybersecurity Information Sharing*" uitvaardigde waarin de secretaris van het Department of Homeland Security (DHS) werd opgeroepen de ontwikkeling en de vorming van *Information Sharing Analyse Organisations* (ISAO's) voortvarend aan te jagen. Deze Executive Order erkende dat een bredere uitwisseling van informatie (buiten vitale infrastructuren) nodig is om de Verenigde Staten beter te beschermen tegen cyber incidenten. Daarbij werd het volgende meegegeven:
- ISAO's kunnen worden georganiseerd per sector, sub-sector, regio of elke andere vorm van clustering. Ze kunnen publiek, privaat of publiek-privaat zijn en kunnen zowel not-for-profit als ook profit organisaties zijn.
- Het National Cybersecurity and Communications Integration Center (NCCIC) moet een actieve rol spelen.
- Er moet een 'non-governmental' ISAO Standards Organization worden opgericht.

Deze ISAO Standards Organization[23] (ISAO SO) is opgericht op 1 oktober 2015, en wordt geleid door de Universiteit van Texas in San Antonio (UTSA) met steun van LMI Government Consulting en Retail Cyber Intelligence Sharing Center (R-CISC). De ISAO SO heeft een gemeenschappelijke set van vrijwillige normen en richtlijnen opgesteld voor de oprichting en de werking van ISAO's. Dit in samenwerking met de bestaande informatie-uitwisseling organisaties, eigenaren en exploitanten van vitale infrastructuur, betrokken instanties en andere belanghebbenden binnen de publieke en private sector. Deze normen richten zich bijvoorbeeld op het maken van contractuele afspraken, de interne bedrijfsprocessen van een ISAO, operationele procedures, technische specificaties en privacybescherming. Daarnaast adviseert en ondersteunt de ISAO SO organisaties over de oprichting en de werking van ISAO's.

---

22 https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

23 https://www.isao.org/

Nederlands model

Bij de uitwerking van een cybersecurity informatie-uitwisselingsmodel voor de bedrijven in de topsectoren zijn er nog diverse punten die uitgewerkt dienen te worden voor de Nederlandse situatie:

- Er dient een passende Nederlandse naamgeving te worden bedacht die aanspreekt. In de rest van dit document wordt als werktitel over Nederlandse ISAO's gesproken.
- Het Nederlandse ISAO model dient toegespitst te worden op de Nederlandse situatie.
- Het aansluitmodel van ISAO's op het NCSC en de inrichting van de fusion centers moet worden uitgewerkt. Hierbij kunnen nog verschillende keuzes worden gemaakt over de wijze waarop dit gebeurt qua organisatie, type informatie et cetera.

Uitgaande van het feit dat de Nederlandse ISAO's op den duur zelfstandig moeten kunnen functioneren zijn enkele uitgangspunten van belang bij de inrichting van het ISAO stelsel Nederlandse stijl:

- De facilitering van de ISAO's is in eerste instantie de verantwoordelijkheid van de deelnemers zelf, maar in de opstartfase speelt de overheid een belangrijke rol door (tijdelijk) zelf het vliegwiel te zijn, dan wel dit in de vorm van een programma te organiseren.
- Het NCSC stelt relevante dreigingsinformatie beschikbaar aan ISAO's (via een fusion center) die aan nader op te stellen voorwaarden voldoen.
- De organisaties die deel uitmaken van de ISAO's zijn zelf verantwoordelijk voor het nemen van passende maatregelen in hun eigen organisaties, net als het geval is binnen de ISAC's. Zij doen dit op basis van hun eigen risicoanalyse. Hierbij dienen zij rekening te houden met wettelijke verplichtingen en de facto standaarden in de markt.

Om het ISAO stelsel in de implementatiefase aan te jagen is het wenselijk dat de faciliterende partij in deze initiële fase ook een ondersteunende rol richting de ISAO's kan vervullen door bijvoorbeeld:

- Een fusion center in te richten dat informatie uit verschillende bronnen (open bronnen, commerciële bronnen, overheidsbronnen) bij elkaar brengt, analyseert en in de vorm van actionable intelligence deelt met de aangesloten partijen.
- Een platform te bieden waarin op een vertrouwde manier informatie kan worden gedeeld tussen ISAO deelnemers onderling.
- Good Practices te ontwikkelen en te verspreiden.

In de uitwerking van het implementatieplan dient duidelijk te worden wat het benodigde programmabudget (incl. personeelskosten, materiële kosten, communicatie, reiskosten etc.) is en wie zorg draagt voor de financiering van het centrale deel van een ISAO. Het meest voor de hand liggend daarbij is dat de overheid de initiële programmakosten voor haar rekening neemt en dat als onderdeel van het programma een onderzoek wordt gegaan wat een toekomstbestendig financieringsmodel is, publiek-privaat, privaat of publiek.

6 Conclusie

De verkenning heeft zich gericht op de volgende centrale onderzoeksvragen:

- Is er behoefte en noodzaak voor het oprichten van een infrastructuur voor het delen van cybersecurity informatie voor de topsectoren in Nederland?
- Zo ja, is de bestaande topsectoren structuur een organisatievorm om dit op te pakken of zijn andere organisatievormen om cybersecurity in de topsectoren op een hoger peil te brengen?
- Is het ISAC model dat voor overheid en vitale infrastructuur wordt gebruikt een model dat hiervoor gebruikt kan worden of zijn er andere modellen meer geschikt?
- Welke good practices zijn er te vinden in het buitenland die passen op de Nederlandse situatie en hoe zouden deze op de Nederlandse situatie toegepast kunnen worden?

Er is behoefte en noodzaak om cybersecurity informatie te delen binnen de topsectoren in Nederland. Om wereldwijd toonaangevend op innovatie te blijven is het van groot belang om in digitale veiligheid te investeren. Niet alleen wordt intellectueel eigendom gestolen, ook de continuïteit van onze digitale samenleving wordt bedreigd en daarmee de economische kansen voor de toekomst. Op dit moment is cybersecurity nog onvoldoende belegd in de topsectoren.

Het onderzoek maakt duidelijk dat de bedrijven uit de topsectoren via meerdere routes digitaal weerbaar gemaakt kunnen worden. Naast de topsector als organisatievorm zijn structuren als brancheorganisaties, ketens en regionale of thematische samenwerkingsverbanden hiervoor geschikt. Op die manier kan Nederland komen tot een dekkend netwerk van organisaties die informatie over cybersecurity dreigingen en oplossingen kan uitwisselen. Hiermee zal Nederland weerbaarder worden tegen digitale dreigingen.

Deze infrastructuur voor het niet-vitale deel van het bedrijfsleven, dat zo belangrijk is voor de verdere economische groei van Nederland, moet aansluiten op de bestaande ISAC infrastructuur voor overheid en vitale sectoren waarin cybersecurity informatie publiek-privaat wordt gedeeld ten behoeve van de nationale veiligheid en de continuïteit van deze sectoren.

Het voordeel van het opzetten van een structuur die breder is dan alleen de topsectoren is dat alle aspecten van digitale weerbaarheid kunnen worden geadresseerd. Naast het beschermen van het innovatieve vermogen is ook het verzekeren van de business continuïteit van belang. Daarbij kennen de bedrijven uit de topsectoren ook vele toeleveranciers en ketenpartners die op deze wijze ook onderdeel maken van de gezamenlijke infrastructuur.

Deze grote en diverse groep van organisaties kan op meerdere manier worden ingedeeld (topsector, branche, regionaal, keten). De op te bouwen infrastructuur moet flexibel genoeg zijn om deze verschillende samenwerkingsverbanden te kunnen bedienen. Bij de ontwikkeling van een Nederlands model kan gebruik worden gemaakt van good practices uit het buitenland. Met name de modellen in de Verenigde Staten (ISAO), het Verenigd Koninkrijk (CiSP) en Duitsland (Alliance for Cybersecurity) passen goed op de bestaande Nederlandse situatie.

A Respondenten

Sector	**Organisatie**
Agri & Food	LTO
	FNLI
Chemie	VNCI
Creatieve Industrie	EZ
	Topteam / Info.nl
	NVA
Energie	EZ
	TKI Urban Energy
	Commit 2 Data
HTSM	EZ
	FME
Life Sciences & Health	EZ
	LSH Alliance
Logistiek	TLN
	NLIP
Tuinbouw & Uitgangsmaterialen	GroentenFruit Huis
	Plantum
Water	EZ
Overig	**Organisatie**
	EZ
	VNO NCW
	VenJ NCSC
	VenJ DCS
	VU

B Achtergrondinformatie topsectoren

Algemeen – waarom topsectoren?
Nederland moet concurrerend blijven om onze internationale toppositie te behouden. Tegelijk vragen maatschappelijke vraagstukken, zoals de toenemende vergrijzing en de overgang naar schone energie en duurzaam voedsel, vragen om creatieve oplossingen. Daarvoor heeft Nederland nieuwe producten, slimme productketens en nieuwe vaardigheden nodig. In negen topsectoren werken bedrijven, onderzoekers, overheden en maatschappelijke organisaties aan een gemeenschappelijk doel om te blijven innoveren met goed opgeleide mensen.
Dit doen zij vanuit hun talent, expertise en belang. De kracht van de topsectorenaanpak zit niet alleen in de samenwerking tussen ondernemers, onderzoekers en overheden binnen de verschillende topsectoren. Ook de kruisbestuivingen tussen topsectoren hebben aantoonbaar meerwaarde. Zo wordt er samengewerkt om de beste producten en diensten te realiseren (innovatie), talenten aan te trekken (human capital) en de sectoren goed internationaal te positioneren (Holland trade).

Op www.topsectoren.nl is een overzicht te vinden van de 9 topsectoren, met daarin verwijzingen naar de websites per topsector.

Topsector Agri & Food

De topsector Agri & Food omvat alles rond voedsel, zowel de primaire productie als het bewerken, verwerken, vermarkten en de distributie ervan. Om zowel maatschappelijke als economische kansen te benutten, stimuleert de topsector Agri & Food de ontwikkeling van nieuwe kennis en innovaties. De Nederlandse Agri & Foodsector blinkt uit in innovaties en productiviteit. Van de 40 belangrijkste voedsel- en drankbedrijven ter wereld hebben 12 bedrijven R&D-activiteiten of een vestiging in Nederland. De sector wil deze leidende positie vasthouden en uitbouwen.
Het gaat niet alleen om productie van duurzame en hoogwaardige voeding, maar ook om duurzame voedselketens waarin mens dier en natuur centraal staan.

Topsector Chemie

Nederland heeft een sterke chemische sector en wil een leidende rol spelen in de overgang naar groene en duurzame chemie. De chemische industrie maakt en bewerkt producten door de chemische samenstelling van bestaande stoffen te veranderen. Net als andere sectoren heeft de chemische industrie te maken met schaarsheid van grondstoffen: ze raken op of zijn niet eenvoudig beschikbaar.
Dit probleem biedt voor de topsector Chemie ook mogelijkheden. Bijvoorbeeld door duurzame en milieuvriendelijke grondstoffen te gebruiken voor slimme materialen en oplossingen, die worden toegepast in de gezondheidszorg, voedingsindustrie, energie- en transportsector en hergebruik van grondstoffen in de chemische sector.

Topsector Creatieve Industrie

De topsector Creatieve Industrie is de meest dynamische topsector van de Nederlandse economie. De creatieve sectoren architectuur, mode, gaming, design, en media en entertainment zijn een aanjager van innovatie in andere sectoren. Ook leveren ze creatieve oplossingen voor maatschappelijke uitdagingen op gebieden als zorg, veiligheid en energie. De Nederlandse creatieve industrie is internationaal een top 10-speler. Bedrijven die internationale bekendheid genieten zijn bijvoorbeeld Endemol, G-star, Guerilla Games en Droog Design. Het Topteam Creatieve Industrie heeft de ambitie dat Nederland in 2020 de meest creatieve economie van Europa is. De topsector Creatieve Industrie heeft drie websites: CLICKNL.nl (de TKI; over kennis & innovatie), CreativeHolland.com (over internationalisering) en de website van het Topteam en de Dutch Creative Council.

Topsector Energie

De topsector Energie is de drijvende kracht achter innovaties die nodig zijn voor de transitie naar een betaalbaar, betrouwbaar en duurzaam energiesysteem. Internationalisering van de energiemarkt en CO2-reductie zijn belangrijke thema's. Doelstellingen zijn het verlagen van de kosten van de CO2-uitstoot, het ontwikkelen van hernieuwbare energiebronnen en het slimmer benutten daarvan. De vraag naar (duurzame) energie groeit en biedt kansen voor bijvoorbeeld opwekking en transport van en handel in energie. Nederland heeft een goede uitgangspositie om hiervan te profiteren, door de gunstige ligging aan zee, de stevige positie van de zeehavens, de aanwezigheid van gas en een gasinfrastructuur. Hierdoor kan Nederland uitgroeien tot het energieknooppunt van Europa.

Topsector High Tech Systemen en Materialen (HTSM)

De Nederlandse hightechsector is een sterk internationaal georiënteerde, kennisintensieve sector, waar veel onderzoek plaatsvindt en hoogwaardige producten en diensten worden ontwikkeld. Daarnaast zit in bijna alle producten van tegenwoordig een stukje technologie, wat de impact van de sector nog groter maakt.

De sector speelt een essentiële rol in het bedenken en realiseren van oplossingen voor wereldwijde maatschappelijke uitdagingen op het gebied van mobiliteit, gezondheid, duurzame energie, veiligheid en klimaatverandering, met technologieën die in Nederland stevig geworteld zijn: micro-/nano-elektronica, nanotechnologie, fotonica, geavanceerde materialen en productie, en halfgeleiders.

De markt voor Nederlandse hightechproducten en -diensten ligt voor het grootste deel in het buitenland. Dit is een groeimarkt, vooral op wereldschaal. Kernambitie van Holland High Tech is om Nederland door innovatie en exportgroei internationaal tot de top te laten blijven behoren, en wereldwijd een cruciale bijdrage te leveren aan het oplossen van maatschappelijke uitdagingen. De Nederlandse hightechsector heeft de ambitie de export te verhogen tot 74,6 miljard euro in 2025, en de productie tot 182 miljard euro.

Topsector Logistiek

Nederland leeft van oudsher van de internationale handel en is hierdoor een belangrijke speler in de wereldeconomie. De topsector Logistiek staat voor de uitdaging om de verwachte groei van goederenstromen duurzaam in te richten. Logistiek wil bijdragen aan een betere bereikbaarheid en minder uitstoot van CO2. De focus van het topteam Logistiek ligt op de internationale concurrentiepositie van Nederland en daarmee op internationale logistiek, supply chain-regie en de bijdrage van logistiek aan het vestigingsklimaat voor internationale bedrijven. Van grote invloed is de internationale bereikbaarheid via de belangrijkste mainports van ons land: Schiphol en de Rotterdamse haven.

Topsector Life Sciences & Health

De topsector Life Sciences & Health omvat het brede terrein van medische technologie, (bio)farmacie, regeneratieve geneeskunde en gezondheidsinfrastructuur. De sector draagt bij aan de kwaliteit van gezondheid van mens en dier en zoekt oplossingen voor maatschappelijke vraagstukken, zoals de vergrijzing. De grootste uitdaging van de topsector Life Sciences & Health is om de kwaliteit van leven te vergroten en te zorgen voor toegankelijke, betaalbare zorg. Nederlandse bedrijven ontwikkelen baanbrekende innovaties voor de snelgroeiende internationale markt van de gezondheidszorg. Het biomedische onderzoek bij de Nederlandse universitair medische centra en universiteiten staat in de internationale ranglijsten zeer hoog genoteerd.

Topsector Tuinbouw & Uitgangsmaterialen

De topsector Tuinbouw & Uitgangsmaterialen omvat alle plantaardige ketens in het tuinbouwcomplex. De topsector is een brede sector met deelsectoren die lopen van groenten, fruit en bomen tot aan bloemen en bollen. Uitgangsmaterialen zijn producten, zoals pootgoed, plantgoed en zaaizaad. Daaronder vallen bedrijven in verwerking, toelevering, handel en distributie. De wereldbevolking blijft groeien, waardoor duurzame oplossingen steeds belangrijker worden. De Tuinbouw & Uitgangsmaterialensector loopt voorop in de ontwikkeling van gewassen die bijvoorbeeld minder gevoelig zijn voor de weersomstandigheden of die minder gewasbeschermingsmiddelen nodig hebben. Nederland kent zes Greenportclusters, waar teeltbedrijven, veilingen, afzetorganisaties, handelsbedrijven, exporteurs en tuinbouwtoeleveranciers geconcentreerd zijn.

Topsector Water

De topsector Water telt drie clusters: Water-, Delta- en Maritieme technologie. De sector houdt zich bezig met onder meer de bescherming van land, het halen van energie uit water en technologieën voor waterhergebruik. De sector richt zich ook op technologische ontwikkelingen in de scheepvaart en zorgt voor innovatie en veiligheid in de maritieme sector. Wereldwijd staat Nederland bekend om haar uitgebreide kennis op het gebied van water en watermanagement. Indrukwekkende voorbeelden zijn de Deltawerken en de tweede Maasvlakte in de Rotterdamse haven, die veel belangstelling krijgen vanuit het buitenland. Ook de kennis die

Nederland in huis heeft over bescherming van land tegen extreem hoogwater, zorgt voor internationale belangstelling. Zo was Nederland betrokken bij de bouw van een stormvloedkering in St. Petersburg en werd Nederland om advies gevraagd na de orkaan ‘Sandy’ in New York en de overstroming in Groot-Brittannië.

C Buitenlandse voorbeelden cybersecurity informatiedeling

	Achtergrondinformatie	**Flexibiliteit van het model (top down en horizontaal delen) *Informatie disseminatie mogelijkheden***	**Aansluiting (ISAC/NCSC) structuur Nederland**	**Actionable maken van informatie**	**Wie draagt de kosten?**	**Toepasbaarheid op grotere schaal? Wie is de informatieverstrekker, efficiëntie?**
Verenigd Koninkrijk	Cyber Security Information Sharing Partnership (CiSP). **Doelgroep**: Organisaties, individuen en vitale infrastructuur die middels een online portaal (technische) informatie delen. Beheerd door CERT-UK welke onder het Nationaal Cyber Security Centre in het Verenigd Koninkrijk valt. De Information Exchanges waarin vitale structuren en de overheid informatie delen zijn recent ook hier onder gebracht (in plaats van onder CPNI).	Bottom-up en top-down totstandkoming van kennis en informatie.	Het model van Information Exchanges is vergelijkbaar met het Nederlandse model van ISAC's.	Binnen de IE's wordt sectorspecifieke informatie besproken en gedeeld.	Overheid.	Twee lagen van informatiedeling. Generiek via een geautomatiseerd platform en specifiek via de Information Exchanges.
Verenigde Staten	Cyber Information Sharing and Collaboration Program (CISCP). **Doelgroep**: Department of Homeland Security en vitale infrastructuur. **Doel**: Deelnemers voegen informatie toe die gedeeld wordt met alle andere deelnemers (indicatoren van cyber threat activiteit). Voornamelijk een machine-to-machine platform voor delen van technische informatie waarna analytische capaciteit van de deelnemers ingezet kan worden om tekstuele producten op te leveren om de	Informatie is niet sector specifiek. Cross-sectorale informatiedeling en samenwerken aan analyses, factsheets en oplossingen. Bottom-up en top-down totstandkoming van kennis en informatie.	In Nederland zou het CISCP een combinatie zijn van een aantal CERT (machine-to-machine) taken en activiteiten zoals uitgevoerd binnen de ISAC's (analyses en ervaringen).	Informatie is direct inzetbaar voor meerdere sectoren tegelijkertijd, met waarborging van privacy.	Amerikaanse overheid.	Informatiedeling in twee richtingen waarbij deelnemers informatie vanuit de overheid en vanuit de vitale operatoren ontvangen in een gestructureerde manier. Schaalbaar.

	gezamenlijke weerbaarheid te verhogen.					
	Cyber Fed Model (CFM). **Doelgroep**: Overheid en de energiesector. **Doel**: Automatisch machine-to-machine distributienetwerk voor cyber threat intelligence.	Sectoraal-specifieke tooling. Bottom-up en top-down totstandkoming van kennis en informatie.	In Nederland zou het CFM overeenkomen met systemen zoals die nu actief zijn in de CERT van het Nederlandse Nationaal Cyber Security Centrum.	Informatie is direct inzetbaar in de eigen omgeving.	Amerikaanse overheid.	Informatiedeling in twee richtingen waarbij deelnemers informatie vanuit de overheid en vanuit de sector ontvangen in een gestructureerde manier. Schaalbaar.
	Cybersecurity Risk Information Sharing Program (CRISP) **Doelgroep**: Overheid, energieleveranciers en cybersecurity bedrijven op vrijwillige basis. **Doel**: Detectienetwerk met sensoren. Op de informatie die gedeeld wordt vindt een verificatie en valorisatieslag plaats, persoonsgegevens gestript worden waarna de verrijkte informatie verspreid wordt door het netwerk ten behoeve van alle deelnemers.	Informatie is sector specifiek. Sectorale informatiedeling (sensoren/tooling) en samenwerking aan analyses, factsheets en oplossingen. Bottom-up en top-down totstandkoming van kennis en informatie.	In Nederland zou een dergelijk programma een pilot zijn die binnen een ISAC opgezet zou worden met samenwerking van het NCSC, waarbij het sensorennetwerk overeenkomsten toont met het Nationaal Detectie Netwerk.	Informatie is direct inzetbaar binnen de eigen sector.	Onbekend.	Lastiger. Men beoogd tweerichtingsverkeer en dat is eenvoudiger met een homogene set aan deelnemers wat bij CRISP het geval is.
	Information sharing and analysis organizations (ISAO). **Doelgroep**: Publieke en private zelforganiserende groepen. **Doel:** Online en in persoon cyber security informatie delen die niet per se in dezelfde sectoren opereren. ISAO's hebben verschillende doelstellingen en	Delen van operationele, tactische en strategische informatie. Bottom-up totstandkoming van kennis en informatie.		Afhankelijk van de doelstellingen en mate van vertrouwen in een ISAO.	Onbekend.	DHS verspreid informatie.

	de overeenstemming met de verschillende ISAO's is dat de ISAO regels en standaarden nageleefd worden. Samenwerking met DHS.					
	Information Sharing and Analysis Center (ISACs). **Doelgroep**: sectoren specifiek. ISACS zijn een manifestatie van ISAO's. Koepelorganisatie is de National Council of ISACS (NCI). NCI draagt zorg voor de cross-sectorale informatiedeling.	Bottom-up totstandkoming van kennis en informatie.	De Amerikaanse ISAC structuur is een voorbeeld van en voor de Nederlandse ISAC structuur.		Kosten lidmaatschap voor deelnemende organisaties. Overheid draagt bij met kennis en informatie.	Schaalbaar.
Finland	National Emergency Supply Agency (NESA). Zeven clusters. **Doelgroep**: e.g. Food Supply Cluster, Energy Cluster, Finance Cluster, Industry Cluster etc.) met daarin 23 Industry Pools (e.g. water supply pool, maritime Transport Pool, etc.).	Onbekend.	Onbekend.	Onbekend.	Onbekend.	Onbekend.
Zweden	Cooperation Group for Information Security (SAMFI). **Doelgroep**: overheid. **Doel**: uitwisselen van operationele, strategische en tactische informatie op het gebied van informatiebeveiliging.	Niet van toepassing.	Vergelijkbaar met de Nederlandse Rijks-ISAC.	Onbekend.	De overheidsorganisatie MSB faciliteert.	Onbekend.
	Forum for information sharing (FIDI). **Doelgroep** e.g. FIDI-SCADA, FIDI-Healthcare, FIDI-Finance, FIDI-Telekom, FIDI-CERT, Gebaseerd op de richtlijnen van CPNI UK.	Onbekend.	Onbekend.	Onbekend.	Onbekend.	Onbekend.

	National Telecommunications Coordination Group (NTSG). **Doelgroep**: Post and Telecom Agency. Doel: kennisuitwisseling, met name op fysieke veiligheid.	Onbekend.	Onbekend.	Onbekend.	Onbekend.	Onbekend.
Zwitserland	MELANI (Reporting and Analysis Centre for Information Assurance). **Doel:** Dreigingsanalyses, situational reports, statistieken, factsheets en achtergrondinformatie, indicators of compromise via een online platform. **Doelgroep**: Closed Customer Base (CCB) geselecteerde bedrijven en nationale vitale infrastructuur. **Doelgroep**: Open Customer Base (OCB) MKB en burgers.	Informatiedeling richting: Gerichte en generieke informatiedeling.	Samenwerken aan dreigingen en ontwikkelingen en uitwisseling van ervaringen en duidelijk verschil tussen de govCERT.CH en de PPP overlegorganen.	Informatie toegespitst op sectoren en informatie generiek.	Overheid.	Uitermate schaalbaar voor veel deelnemers. De overheid heeft hier een rol als facilitator, kennisontwikkeling en kennisverspreider.
Duitsland	Alliance for Cyber Security. **Doelgroep:** Deelnemers: Overheid, instituten, vitale infrastructuur, niet vitale infrastructuur. **Doel**: kennisopbouw en kennisinstituut, delen en uitwisselen van informatie en ervaringen. Delen van gerubriceerde informatie en ontvangen hiervan van organisaties en bedrijven. Gericht en generiek. Factsheets, white papers maar ook strategisch-tactisch voor het bedrijfsleven.	Informatiedeling richting: Gerichte en generieke informatiedeling.	Kennisomgeving vanuit het ministerie met directe contacten naar sectoren en overheid. Samenwerken aan dreigingen en ontwikkelingen en uitwisseling van ervaringen.	Informatie toegespitst op sectoren en informatie generiek.	Overheid.	Uitermate schaalbaar voor veel deelnemers. De overheid heeft hier een rol als facilitator, kennisontwikkeling en kennisverspreider.
	UP KRITIS (Platform Critical Infrastructure Protection). **Doelgroep** vitale infrastructuur.	Informatiedeling richting: Iedere werkgroep heeft een eigen beveiligde infrastructuur. Hiërarchie: Single Point of Contact (SPOC) per sector. SPOC communiceert naar het BSI.	Single Point of Contact is uitgesprokener op papier in Duitsland dan in Nederland. BAK is vergelijkbaar, waarbij de TAK een gestructureerde benadering geeft voor cross-sectorale	Informatiedeling gericht op zowel de sector specifiek en andere sectoren.	Overheid.	Overheid speelt een faciliterende en informerende rol en is een gelijkwaardige partner. Bottom-up informatiedeling.

	Vorm van samenkomen: Sectoral working groups (BAK) en Thematic working Groups (TAK). Ook een "Plenum" waar cross-sectoraal informatie gedeeld wordt (combineert de informatie uit de BAK en TAK).	TAK's werken aan cross-sectoraal onderwerpen.	informatiedeling en kennisontwikkeling.			
	Thema's: operationeel-technisch en tactisch-strategisch.					
	Deelnemers: Per sector een werkgroep waar een vertegenwoordiger van een bedrijf in de desbetreffende sector in deel kan nemen. Eerst is men participant, daarna een partner. Centrale Informatieknooppunt is het Situation Centre bij het ministerie (BSI). Mogelijkheid tot gebruik technisch platform voor het delen van informatie voor werkgroepen en landelijke bijeenkomsten.					
Oostenrijk	Austrian Trust Circle (ATC).	Informatiedeling richting: Gerichte en generieke informatiedeling. Zowel bottom-up als top-down.	Veel gelijkenissen met de Nederlandse ISAC's. Geen informatie over de mate van technische informatie-uitwisseling.	Onbekend.	Overheid.	Schaalbaar.
	Deelnemers: vertegenwoordigers uit de zes vitale sectoren. Sectoren komen vier keer per jaar bij elkaar en één keer per jaar om cross-sectoraal informatie te delen.					
	Doel: informatiedeling en het maken van risk management plannen, oefeningen. Voor specifieke onderwerpen worden werkgroepen gevormd. Naast vergaderingen is er ook een online omgeving waar informatie gedeeld kan worden. Samenwerking en facilitering door de Oostenrijkse CERT genaamd CERT.AT en het Cyber Security Platform.					

D Referentielijst

ABN AMRO, AON, TLN (2016). Cybersecurity voor logistieke dienstverleners.

AIVD. Toenemende digitale spionage. Online: https://www.aivd.nl/actueel/nieuws/2016/09/06/csbn-2016-toenemende-digitale-spionage

McKinsey Institute. Digital globalization: the new era of global flows. Online: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

NCTV. Factsheet Vitale Infrastructuur. Online: https://www.nctv.nl/binaries/18.factsheet-vitale-infrastructuur_tcm31-32336.pdf

NCTV. Nieuws. Online: https://www.nctv.nl/actueel/nieuws/2016/Beroepscriminelen-steeds-groter-gevaar-voor-digitale-veiligheid.aspx

NICC. Publiek-private samenwerking in het Informatieknooppunt Cybercrime, NICC,2008.

Rathenau Instituut. Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid. 2017. https://www.aivd.nl/publicaties/rapporten/2017/03/02/rapport-rathenau-overheid-en-bedrijven-onvoldoende-beschermd-tegen-cyberdreigingen

TNO. Sharing cybersecurity information. Online: https://www.tno.nl/en/focus-areas/defence-safety-security/cyber-security-resilience/sharing-cyber-security-information/

Verhagen. Nederland Digitaal Droge Voeten – adviesrapport cyber security. Online: https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf

Internationale Cybersecurity Informatiedelingsmodellen

Duitsland
http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/leitfaden.pdf?__blob=publicationFile&v=4

Finland
https://tapahtumat.tekes.fi/uploads/3ef8185/savisalo_security_of_supply-1506.pdf

Nederland
https://www.ncsc.nl/samenwerking/ISAC's.htm

Oostenrijk
https://publicwiki-01.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy#Austria

Verenigd Koninkrijk
https://www.ncsc.gov.uk/cisp

Verenigde Staten
https://www.nationalisacs.org/
https://www.isao.org/
https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing
https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ciscp_one_pager.pdf

https://cfm.gss.anl.gov/about-cfm/

Zweden
https://rib.msb.se/Filer/pdf/26177.pdf
https://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Information%20Security%20in%20Sweden.pdf -
http://www.pts.se/upload/Faktablad/En/facts-about-ntsg.pdf

Zwitserland
https://www.melani.admin.ch/melani/en/home.html
Dunn Cavelty, Myriam. 2014. Cybersecurity in Switzerland. http://dx.doi.org/10.1007/978-3-319-10620-5

ENISA
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing