CYBERGEREEDHEID ECONOMIE PROVINCIE ZUID-HOLLAND

Een strategische luchtfoto en handelingsperspectief

Koen Gijsbers

Cyber4Board
Oktober 2020

CYBERGEREEDHEID ECONOMIE
Provincie ZUID-HOLLAND

Een strategische luchtfoto en handelingsperspectief

Inhoudsopgave:

Opgesteld in opdracht van Provincie Zuid-Holland en *Task Force Digital Economy* van de *Economic Board* Zuid-Holland door Koen Gijsbers – Cyber4Board.

INTRODUCTIE

Digitale transformatie versnelt, en daarmee de maatschappelijke en economische afhankelijkheid van digitale netwerken en diensten. Tegelijkertijd neemt het aantal cybersecurity incidenten dagelijks toe. Intellectueel eigendom en persoonsgegevens worden illegaal gekopieerd en misbruikt; cyberaanvallen leggen bedrijven, universiteiten en ziekenhuizen plat uit financieel gewin, om de maatschappij te ontwrichten, of als neven schade van intra statelijke conflicten waarbij die organisaties niet eens een gericht aanvalsdoel waren. Er is toenemende uitval van vitale systemen en diensten. Goed georganiseerde kwaadaardige cybercriminelen zijn actief in netwerken van overheden en bedrijven, vaak gedurende langere tijd voordat een daadwerkelijke aanval zichtbaar wordt. Bijna elke dag lezen we wel over een succesvolle cyberaanval.[i]

Dit is een punt van zorg van provincie en regio's. De maatschappelijke en economische impact van onvoldoende beschermde en weerbare netwerken en ICT-systemen wordt helderder en daarmee de bereidheid tot het nemen van maatregelen en doen van investeringen. Het bestuur van de Provincie Zuid-Holland, geadviseerd door de Economic Board Zuid-Holland en haar Taskforce Digitale Economie toont haar betrokkenheid om de digitale weerbaarheid en veerkracht te vergroten, wil een aanzet geven voor regionale programmering om cybersecurity (verder) in de economie in te bedden. Daartoe is opdracht gegeven voor een **Road Map Digitaal Weerbare Economie** als basis voor effectieve maatregelen, beleid, en verbeterde processen om het geïdentificeerde risico te beheersen.

Overigens zijn er naast zorgen ook kansen. Immers digitaal weerbaarheid van de economie is een goed uithangbord voor het aantrekken van nieuwe bedrijven. Een robuuste en veilige ICT- infrastructuur, goede dienstverlening om cyber incidenten te voorkomen en te verhelpen, een hoge mate van cyber awareness bij het MKB waarvan grotere bedrijven afhankelijk zijn en een *cyber-ready workforce* nemen zorgen weg en dragen bij aan een goed vestigingsklimaat.

Ook zijn er goede kansen voor cyberinnovatie en voor cybersecurityondernemingen in de regio. Er is immers al een goede basis rondom The Hague Security Delta. Binnen de ICT is cybersecurity de snelst groeiende sector, naast toepassing van *Artificial Intelligency* (AI) en *blockchain*. Hoe beter ondernemingen samen voor de regionale economie relevante cyberproducten ontwikkelen en hoe meer deze regionaal verkocht worden, hoe meer groei van deze cybersecuritybedrijven zal worden gerealiseerd, terwijl de regionale economische sectoren ook nog eens beter zijn voorbereid op cyberaanvallen. Samenwerking met academische instelling, R&D-organisaties, volwassen ICT-dienstverleners en de overheid als klant versterkt zo'n cluster verder.

Deze regionale analyse is gebaseerd op een methodologie voor evaluatie van cyber gereedheid[ii] en CRI 2.0[iii] van Potomac Institute uit Arlington, VA, USA en beschrijft een achttal aspecten van cybersecurity gereedheid als basis voor de roadmap. Ze koppelt de ambitie aan kwalitatieve normen en aantoonbare initiatieven op het gebied van organisatie, beschikbare middelen en feitelijke realisatie. Het kan zijn dat bepaalde aspecten afhankelijk zijn van landelijke initiatieven, bijvoorbeeld op het gebied van cyberinlichtingen, diplomatie, defensie of nationale politie. Samenhang met activiteiten in de provincie en regio moet echter worden geborgd. Voor elk aspect wordt vastgesteld wat dit voor de provincie betekent en wat we eraan kunnen doen. De synthese van die separate adviezen vormt de basis voor het actieplan ter verbeteren van de weerbaarheid.

Deze analyse richt zich niet op de rijksoverheid of de nationaal vitale infrastructuur en diensten. Dat is een nationale verantwoordelijkheid, waarbij het Nationale Cybersecurity Centrum (NCSC) van het Ministerie van Justitie en Veiligheid een belangrijke rol speelt. Wel kijkt deze analyse naar infrastructuur en diensten die vitaal zijn voor de regio, maar niet formeel deel uitmaakt van vitale nationale infrastructuur. Daarnaast stimuleert de regio cyberweerbaarheid van de economie, natuurlijk de grotere nationaal en internationaal opererende bedrijven, maar vooral dat deel van de economie die gedragen wordt door het Midden- en Klein Bedrijf (MKB). De provincie of regio heeft een rol bij het verbeteren van weerbaarheid van belangrijke maatschappelijke diensten zoals het onderwijs, ziekenhuizen en natuurlijk bij het helpen de inwoners beter te beschermen tegen kwaadaardige cyberactiviteiten.

De provincie Zuid-Holland heeft ingezet op een goed vestigingsklimaat voor ondernemingen. In dat kader is een actieplan ingezet voor versterking van de digitale infrastructuur versnelde uitrol van 5G communicatie en glasvezel, moderne datacenters en aandacht voor cybersecurity om deze diensten te borgen. Ook werkt de provincie aan een Human Capital Agenda als voorwaarde om bedrijven aan te trekken.

Zuid-Holland heeft een sterke economie die steeds meer digitaal wordt. Vrijwel alle topsectoren van de nationale economie zijn aanwezig in de provincie. Zonder andere tekort te doen, spelen de volgende sectoren een belangrijke rol in de verdere versterking van de digitale economie:

- De haven Rotterdam en de maritieme delta die reikt van de Tweede Maasvlakte tot Gorinchem. Verschillende grote bedrijven in de haven vallen onder nationaal aangewezen essentiële diensten.
- Het Westland en de horticultuur bedrijven door de provincie heen, productie en distributie van groente, fruit en bloemen wereldwijd.
- De High Tech Systems en Materialen (HTSM) industrie die componenten en meet- en regelsystemen maakt vooral voor industriële toepassingen.
- Het ruimte- en luchtvaartcluster onder meer rondom het Europese Space Agency, maar ook verder door de provincie.
- De Medical Delta en de biotech industrie met een belangrijke concentratie rondom het Leiden BioScience Park, maar ook in Rotterdam (Erasmus)
- Industrie voor defensie en veiligheid, waaronder maritiem, luchtvaart en beveiligde ICT-systemen (o.a. crypto). Defensie, de veiligheidsdiensten, NAVO en politie zijn belangrijke opdrachtgevers en klanten in deze provincie.
- Natuurlijk de digitale infrastructuur: vaste en mobiele netwerken (telecom), datacenters die de drager zijn van de verdere digitalisering van de regio. Overigens heeft de cyberveiligheid van de digitale infrastructuur als essentiële dienst nationale aandacht.

Al deze sectoren worden economisch gestimuleerd door verdere digitalisering, maar hebben tegelijkertijd te maken met nieuwe dreigingen die continuïteit en winstgevendheid onder druk kunnen zetten.

Deze analyse richt zich met name op bovengenoemde sectoren, zonder daarbij afbreuk te doen aan het belang van andere. Generieke lessen uit deze sectoren zullen zeker een bijdrage leveren aan de rest van de Zuid-Hollandse economie, die voor een belangrijk deel gedragen wordt door zo'n 300.000 MKB-bedrijven.

REGIONALE STRATEGIE

De provincie Zuid-Holland draagt met een Bruto Regionaal Product van ong. Mld€157 voor ongeveer een vijfde deel bij aan de economie van Nederland. Zuid-Holland wil haar internationale positie als economisch centrum verder versterken door een van de meest digitale economieën te worden en heeft daartoe in 2017 een Roadmap Digital Economy opgesteld. Er is een *Economic Board* Zuid Holland (EBZ) met participatie van zowel overheden, kennisinstituten als het bedrijfsleven om implementatie van deze strategie te stimuleren. De provincie, gemeenten en EBZ worden geadviseerd door een publiek/private Task Force Digitale Economie, die dit onderzoek naar verbeterde digitale weerbaarheid laat uitvoeren. Men onderkent dat de digitale weerbaarheid en cybersecurity meer aandacht moet krijgen als waarborg voor maatschappelijke en economische veiligheid, zeker in combinatie met verdere digitalisering. De implementatie van nieuwe technologie brengt immers ook nieuwe risico's met zich mee.

Provincie. De provincie Zuid-Holland heeft geen eigen regionale cybersecuritystrategie; overigens geldt dit voor alle provincies in Nederland. De rol van de provincie bij het verbeteren van digitale weerbaarheid is niet helder vastgelegd. De provincie functioneert binnen de nationale kaders voor cybergereedheid en stimuleert verschillende activiteiten op het gebied van verbeterde digitale weerbaarheid, innovaties, kennisontwikkeling (*Human Capital Agenda*) en het verbeteren van awareness voor overheden en het bedrijfsleven, met name MKB. Ze werkt daarbij samen met de gemeenten, met name Den Haag en Rotterdam, met de regionale ontwikkelingsmaatschappij InnovationQuarter (IQ), met het veiligheidscluster The Hague Security Delta (HSD) en met verschillende andere organisaties in de provincie. Voor deze activiteiten heeft de provincie een beperkt budget beschikbaar van enige tonnen per jaar. Ook zijn fondsen opgenomen in budgetten om digitalisering te stimuleren.

In de begroting van de provincie Zuid-Holland wordt het stimuleren van digitale weerbaarheid of cybersecurity niet direct benoemd. Er zijn geen geoormerkte bedragen voor deze onderwerpen geïdentificeerd waarover moet worden gerapporteerd.[iv]

Tot op heden is het geen *common practice* op het provinciale niveau een enkelvoudige autoriteit te benoemd voor het stimuleren van digitale weerbaarheid of cybersecurity[v] binnen de provincie. Ook Zuid-Holland heeft dat niet gedaan. De taken zijn verdeeld. Taken op het gebied van maatschappelijke veiligheid liggen bij de Commissaris van de Koning in zijn rol als ambassadeur voor cyberweerbaarheid en als toezichthouder op de veiligheidsregio's; daar is ook crisismanagement belegd. De gedeputeerde economie en innovatie heeft de digitalisering van de economie in haar portefeuille, en ook de digitale weerbaarheid en cyberveiligheid ervan. De *Human Capital Agenda*, ook relevant voor cybersecurity ligt bij een andere gedelegeerde.

In het kader van het Besluit Risico Zware Ongevallen onderzoekt de provincie of zij een rol heeft in het controleren van cybersecuritymaatregelen bij BRZO-bedrijven [vi], omdat cyberincidenten van operationele technologie ongevallen bij deze bedrijven kunnen veroorzaken. Tot slot pakt de provincie (Dienst Beheer Infrastructuur) de cyberweerbaarheid van haar infrastructuur voortvarend op. Dit betreft provinciale wegen, vaarwegen, sluizen en bruggen.

Provincie handelt binnen nationale kaders. Omdat de provincie handelt in het kader van wettelijke regelgeving en nationale strategieën op het gebied van digitale weerbaarheid en cyberveiligheid, is het goed de belangrijkste te beschouwen. Daaruit blijkt welke aspecten die voor de provincie belangrijk zijn

elders worden geregeld en welke lacunes er wellicht zijn. In bijlage B worden de belangrijkste nationale kaders uitgewerkt.

Wat betekenen de nationale kaders (wet- en regelgeving en rijksbeleid) voor de provincie en grote steden? Helder is dat nationaal de aandacht voor cybersecurity de laatste jaren fors is toegenomen. Wel moeten we vaststellen dat de nationale aandacht en financiering zich vooral richt op rijksoverheid, haar dienstverlenende organisaties, zoals Rijks Waterstaat of de Belastingdienst en nationaal vitale infrastructuur en diensten, waaronder de belangrijke ICT-infrastructuur.

- Alleen de nationale aanbieders essentiële diensten (AED's) en digitale diensten in de provincie kennen meld- en zorgplicht en worden ondersteund door het Nationaal Cybersecurity Center (NCSC); het gros van de economie van Zuid-Holland, het bedrijfsleven dat niet tot de categorie AED behoort en de burger wordt maar beperkt ondersteund vanuit nationaal perspectief.
- Het gros van de grotere bedrijven en het MKB heeft geen wettelijk vastgelegde meld- en zorgplicht. Het nemen van cybersecuritymaatregelen is een bedrijfseconomische keus. De ondernemingen worden niet met zekerheid ondersteund bij cybercalamiteiten vanuit het NCSC. Het centrum zal zich inspannen, maar heeft geen leverplicht.
- Het Digital Trust Center van het Ministerie van Economische Zaken en Klimaat is namens het Rijk verantwoordelijk voor het verbeteren van cyberweerbaarheid van dat deel van de economie dat niet is aangewezen als essentiële dienst. Het DTC ontwikkelt een netwerk van cyberweerbaarheidscentra door het land. We moeten echter vaststellen dat in de provincie Zuid-Holland deze vooralsnog maar een klein deel van het MKB bereiken en nauwelijks de burger.[vii] Het gros van het MKB krijgt geen dreigingsinformatie of cybersecurityadvies, tenzij ze deel uitmaakt van een regionale of sectorale organisatie die daartoe is geautoriseerd. Wel is generieke informatie via de website beschikbaar.
- Overheidsorganisaties zijn voor cybersecurity gereguleerd; het bedrijfsleven slechts in bepaalde gevallen. Dit betreft vooral AED-bedrijven (deze hebben zorgplicht, maar deze niet helder genormeerd), financiële instellingen (o.a. vanuit de Nederlandse Bank), telecom en andere digitale dienstverleners en beursgenoteerde bedrijven. Gereguleerde bedrijven moeten bepaalde cybersecuritymaatregelen nemen en worden daarop meestal ge-audit. Deze bedrijven hebben daardoor vaak een hogere mate van cybergereedheid.
- Bedrijven die producten of diensten leveren aan de overheid, moeten in veel gevallen aan specifieke cybersecurity eisen voldoen. Dit geldt met name voor leveranciers van defensie, NATO of als hogere beveiligingsniveaus worden vereist (ABDO-regeling). Hoe meer regionale bedrijven voorbereid zijn om aan die aanbestedingen deel te nemen, hoe meer kans er is dat werk regionaal wordt gegund.
- De nationale aandacht voor weerbare digitale diensten (netwerken, ICT-infrastructuur) ondersteunt zeker ook de provincie en haar digitaliseringsinitiatieven.
- Aangezien de politie en het OM nationaal is opgehangen profiteert de provincie en regio mee met de extra investeringen van het Rijk in de aanpak van cybercrime.
- Dit geldt ook voor de landelijke ambities op het gebied van cybersecurity kennisontwikkeling. Juist omdat veel activiteiten in Zuid-Holland plaatsvinden (Dcypher, HSD, Universiteiten) profiteert Zuid-Holland en met name de Haagse regio wellicht extra.
- Zuid-Holland profiteert van de landelijke digitaliseringsstrategie door aanwezigheid van veel initiatieven in de provincie.

- Dutch Digital Delta (DDD) helpt de nieuwe nationale Topsector ICT te stimuleren en is gevestigd in de Haagse regio. De provincie kan profiteren van het stimuleren van cybersecurity als sleuteltechnologie en het opleiden van nieuw cybersecuritytalent.

Grote steden. De grote steden, met name Den Haag en Rotterdam hebben ook een belangrijke rol in digitale weerbaarheid van hun economieën. Daarbij zijn de burgemeesters belangrijke spelers in de veiligheidsdriehoek.

- **Den Haag.** Hoewel niet zo benoemd, heeft de stad wel een cybersecuritystrategie. Als stad van Vrede, Recht en Veiligheid is deze stad expliciet over het verbeteren van digitale weerbaarheid. De Staat van de Stad 2020 beschrijft de lokale betekenis van cybercriminaliteit en digitale dreiging. Er is een sterke groei van cybercriminaliteit onder de bevolking en bedrijven. Over de cyberdreiging voor de burgen heeft men goede cijfers; cijfers over slachtofferschap onder bedrijven in de stad Den Haag ontbreken. Aangiftebereidheid onder MKB in Den Haag ligt zeer laag: enkele tientallen op jaarbasis.
  Ook maakt men zich zorgen over de onveiligheid van Operationele Technologie (OT) en de *Internet of Things* (IoT).[viii] De stad Den Haag heeft een expliciete cybersecuritystrategie gericht op de organisatie van de gemeente. [ix] Ook is er een generiek Resilience Strategie Den Haag vastgesteld in 2019 en heet de stad een *Chief Resilience Officer* aangewezen. In haar pakket zit ook het verbeteren van cyberweerbaarheid, met name gericht op de kwetsbare groepen zoals burgers en MKB; ook is er een *Cyber Resilience Community Platform* Den Haag opgericht. [x]
  Tot slot kent Den Haag een Integraal Veiligheidsplan 2019-2022. Speerpunt 1 van dit plan is de versterking van de weerbaarheid van de stad, waaronder ook aanpakken van cybercriminaliteit. Naast het verbeteren van awareness door informatie-uitwisseling wil met kennisontwikkeling en publiek-private innovatiesamenwerking op het gebeid van cybersecurity verder versterken.[xi]
- **Rotterdam.** Rotterdam kent geen expliciete cyberstrategie, maar wel de nodige activiteiten op het gebied van cybersecurity. De Rotterdamse haven vormt het zwaartepunt rond deze inspanningen. Er is hechte samenwerking tussen de gemeente Rotterdam en het Havenbedrijf en Rotterdam heeft een Port Cyber Resilience Officer aangewezen. Er is een actieplan en een weerbaarheidscentrum (FERM) voor de haven opgericht. Maar ook doet Rotterdam het nodige voor MKB'ers. Samen met een verzekeringsbedrijf heeft de Maasstad met zestig MKB-bedrijven een cybersecuritystartpakket uitgerold. Sinds 2019 zet de gemeente zich actief in om de digitale weerbaarheid van Rotterdamse burgers en ondernemers te vergroten; voor het eerst zijn cyber-gerelateerde vragen in de Veiligheidsmonitor opgenomen.[xii]

Regionale economische strategie.
Zuid-Holland kent een unieke samenwerking tussen overheid (provincie en gemeenten), kennisinstellingen en het bedrijfsleven in de *Economic Board Zuid-Holland* (EBZ). [xiii] EBZ zet met de belangrijkste spelers in Zuid-Holland een economische strategie uit voor de toekomstige economie. Dat is van wezenlijk belang, omdat Zuid-Holland een van de grootste motoren is van de Nederlandse economie, bijna een kwart van het bruto nationaal product wordt in de provincie verdiend. Zuid-Holland wil een sleutelrol spelen in de grote transities waar de samenleving voor staat: digitalisering, energietransitie en de overhang naar een circulaire economie. De economische strategie loopt langs twee paden: het vernieuwen van de economie en het creëren van een excellent vestigingsklimaat met een goede fysieke en digitale infrastructuur, een wendbare arbeidsmarkt, goede bereikbaarheid en een goed ondernemersklimaat.
De digitaliseringsstrategie werkt toe naar een betrouwbaar digitaal vestigingsklimaat, naadloos verbonden en met een veilige open-access structuur, waarin wordt samengewerkt aan innovatie in

technologie en de toepassing ervan. Binnen de strategie wordt gewerkt aan connectiviteit, innovatie, kennis en vaardigheden en cyberveiligheid. Dit onderzoek draagt bij aan de cyberaanpak binnen de digitaliseringsstrategie.

Conclusie regionale strategie. Door steeds verdergaande digitalisering en toenemende onveiligheid [xiv], neemt het cyberrisico van de provincie/regio toe, zonder dat dit vanuit strategisch perspectief voldoende en samenhangende aandacht krijgt. Nationaal beleid, wetgeving, strategieën en strategische initiatieven dekken vooral nationale belangen af, maar laten lacunes achter voor digitale weerbaarheid van veel provinciale maatschappelijke en economische belangen. De Provincie heeft aandacht voor het overwerp cyberveiligheid, maar is niet expliciet in het benoemen van haar cybersecurity ambities en de middelen die nodig zijn om die ambitie te realiseren. Bij gemeenten is er niet altijd structureel voldoende aandacht voor het onderwerp. Men onderkent de groei van cybercriminaliteit en de kwetsbaarheid van de burger en het MKB, maar slechts weinig steden hebben een consistent actieplan om deze kwetsbaarheden weg te nemen. Den Haag is een positief voorbeeld als het gaat om expliciet maken van de aandacht voor een integrale cybersecuritybenadering. De aandacht in Rotterdam richt zich vooral op de haven en kan als voorbeeld dienen voor de versterking van weerbaarheid van de economie.
Als het gaat om de digitale economie heeft de EBZ een ambitieus plan op zich genomen om de economie te vernieuwen en het vestigingsklimaat te verbeteren. Daarbij wordt cyberveiligheid als een van de pijlers meegenomen.

Wat kan er verbeteren?

- Een digitaal weerbaarder economie stimuleren is een ingewikkelde uitdaging. Gebrek aan gevoel van urgentie en geen expliciete kennis van de schade die cyberonveiligheid aan de economie berokkent, maken het lastig om aandacht voor het onderwerp vast te houden, een actieplan uit te voeren en tijd en middelen te reserveren. Om die reden is het aan te bevelen dat organisaties of verbanden expliciet zijn in hun cyberambitie en ook één persoon de motor van succes maken, en net als de Rotterdamse haven een Cyber Resilience Officer aanwijzen. Namens de EBZ zou dit een bestuurslid of de voorzitter TF digitale economie kunnen zijn. Aangezien cyberveiligheid complex een publiek-privaat vraagstuk is, lijkt de EBZ het beste gepositioneerd om maximaal succes te realiseren.
- Ook overheden kunnen helpen bij het agenderen van cyberweerbaarheid en het ondersteunen van actieplannen ter vermindering van risico's. Daarom is het aan te bevelen dat de provincie, maar ook grote steden, in navolging van het Rijk en de gemeente Den Haag een bondige cybersecuritystrategie opstellen en formeel vaststellen. Die strategie is daarmee onderdeel van politieke evaluatie. Zo'n integrale strategie is breder dan alleen de weerbare economie en moet zich ook richten op maatschappelijke veiligheid en de burger. Ook helpt het aanstellen van een 'cyber resilience officer' om cybersecurity een gezicht en de noodzakelijke leiding te geven.
- Het bedrijfsleven moet ook zijn deel nemen. Het verdient ook aanbeveling dat samenwerkingsverbanden van economische sectoren net als de Rotterdamse haven (HI, Greenport, BioTech Science, NIDV en andere) cybersecurity expliciet maken en een rol spelen bij en/of verantwoordelijk zijn voor de implementatie van een deel van een regionale strategie. Ook voor de economische sectoren geldt dat het benoemen van een *Cyber Resilience Officer* de aandacht voor het onderwerp zal versterken en de volwassenheid zal vergroten.
- De middelen voor de uitvoering van cybersecuritystrategieën van overheden moeten expliciet gemaakt worden in begrotingen. Daarmee wordt actie van de overheid transparant en kan verantwoording worden afgelegd. Overigens zouden ook private economische sectoren zoals

Greenport of Holland Instrumentation transparant middelen moeten alloceren omdat de verbetering van de weerbaarheid van de economie een gezamenlijke verantwoordelijkheid is.

- Er is onvoldoende zicht op de impact van het digitaal risico als percentage van het regionale bruto binnenlands product (value at risk) dat mogelijk wordt gewonnen of verloren door de strategie te implementeren. We weten niet wat digitale onveiligheid ons kost. Dat geldt voor de economie als geheel, maar ook is er onvoldoende beeld bij de impact voor sectoren van de economie. Het is van belang om vast te stellen hoe kwetsbaar de regio is en welke prioriteit dit onderwerp moet krijgen. Wellicht kan een LDE-universiteit of een Hogeschool bij dit onderzoek een rol spelen.
- Deze regionale cybergereedheidsanalyse is een eerste stap om te komen tot een beoordeling van het digitale risico van de provincie/regio, maar beschouwt maar een deel van de economie. Logistiek/distributie, *retail* en andere voor de regio belangrijke sectoren worden niet behandeld.
- ER komt een goed en actueel overzicht van nationaal essentiële diensten (AED's) die in de regio zijn gehuisvest en heeft vastgesteld of borging van de regionale economische belangen aanvullende AED's vergen? Daarbij stelt men vast of de cyberweerbaarheid van die regionale AED's moet worden verbeterd en wie daarvoor verantwoordelijk is.
- EZB borgt dat er voldoende samenhang en afstemming is van de verschillende cybersecuritystrategieën en -beleid van verschillende sectoren van de regionale economie: industrie, landbouw, vervoer en handel. Er worden *metrics* vastgesteld en een *dashboard* ingericht om vast te stellen of digitale weerbaarheid van die sectoren voldoende aandacht krijgt van de verschillende belangrijke organisaties en hun besturen de bereidheid tonen deze aan te pakken. Net als bij de Human Capital Agenda kan HSD hier als expert partner helpen.
- Het leiderschap van organisaties die verenigd zijn in de EBZ voert een actieve communicatiecampagne uit om het publieke risicobewustzijn van cyberveiligheid te vergroten via het stimuleren van onderwijs, training, en de ontwikkeling van kennis en vaardigheden. Via die communicatie wordt ook de burger verleidt deel uit te maken van de oplossing om samen een sterke cyberveiligheidscultuur op te bouwen om de digitale weerbaarheid van de economie te borgen en het gevoel van veiligheid te versterken.

INCIDENT RESPONSE

Onder Incident Response verstaan wij een georganiseerd proces voor cyber security van een organisatie, bestaande uit: identificeren van cybersecurity risico's; beschermen van de belangrijkste digitale dienstverlening; detecteren van een cybersecurity incident; het nemen van acties om de impact van dat incident te stoppen en te beperken; en het herstellen van de impact van het incident en terugveren naar de normale situatie van de digitale dienstverlening.[xv] Het reageren op cyberincidenten is in eerste instantie een verantwoordelijkheid van organisaties en bedrijven zelf. Dit geldt ook voor het nemen van preventieve maatregelen om incidenten te voorkomen.

Grofweg onderkennen we de volgende categorieën ondernemingen en organisaties met verschillende volwassenheid voor cybersecurity:

- **Multinationals en beursgenoteerde bedrijven**. Deze bedrijven hebben veelal voldoende aandacht voor cyber security en incident response. Toch komen er geregeld succesvolle cyberaanvallen bij dergelijke bedrijven in het nieuws, vaak met een financiële impact van enkele tot honderden miljoenen euro's. Er is bij deze ondernemingen een Chief Information Security Officer (CISO) die namens het bestuur de digitale weerbaarheid en informatiebeveiliging helpt waarborgen met veelal een eigen *Security Operations Center* (SOC) en een *Cyber Security Incident of Emergency Response Team* (CSIRT/CERT). Vaak rapporteren lokale vestigingen in de regio naar het hoofdkantoor in Nederland of in het buitenland. Voor buitenlandse bedrijven is het daarom lastiger om in de regio op het gebied van cybersecurity samen te werken. Publiek verhandelde beursgenoteerde bedrijven zijn gereguleerd en moeten incidenten melden aan de beursautoriteiten en aandeelhouders.
- **Bedrijven en organisaties behorende tot AED (aangewezen essentiële diensten) en ICT-dienstverleners** (nationaal vitale infrastructuur en diensten). Deze bedrijven hebben een wettelijk opgelegde zorgplicht om cybersecuritymaatregelen te nemen, maar helaas is nog niet helder vastgesteld wat die zorgplicht inhoudt. De bedrijven en organisaties hebben veelal voldoende aandacht voor cybersecurity en incident response; ook hier geldt, niet altijd een garantie voor succes. Er is een CISO die namens het bestuur de digitale weerbaarheid en informatiebeveiliging helpt waarborgen met een eigen CSIRT/CERT. Deze bedrijven zijn gereguleerd, hebben wettelijke zorgplicht om voldoende cyberweerbaarheidsmaatregelen te nemen en hebben meldplicht naar het NCSC. Zij krijgen gedetailleerde informatie over dreigingen en ook ondersteuning bij de afhandeling van incidenten. Bedrijven in sommige sectoren kennen meer verplichtingen, zoals bijvoorbeeld financiële instellingen. Veel AED-bedrijven worden ook uitgenodigd deel te nemen aan nationale en internationale cyberoefeningen, zoals ISIDOOR.[xvi]
- **Grotere bedrijven en organisaties met eigen IT afdelingen en een CIO/CISO**. Deze groep organisaties is vaak niet gereguleerd voor cybersecurity, anders dan net als elke organisatie of onderneming door de Algemene Verordening Gegevensbescherming (AVG).[xvii]. De mate van aandacht voor digitale weerbaarheid en cybersecurity is een bedrijfseconomische keus. Het feit dat een CISO is aangesteld helpt bij het agenderen van het onderwerp op de bestuurstafel. Het digitale risicomanagement en haar impact op de bedrijfsvoering is niet altijd even volwassen. Er liggen vaak wel basisplannen voor incident response, maar vaak niet voor incidenten met een digitale oorzaak.
- **MKB met een eigen IT afdeling**. Deze groep bedrijven en organisaties zijn meestal niet gereguleerd voor cybersecurity, behoudens AVG. De mate van aandacht voor digitale weerbaarheid en cybersecurity is een bedrijfseconomische keus. Digitaal risico wordt meestal

niet bewust gemanaged. Vaak wordt IT als een kostenpost gezien en cybersecurity als een 'noodzakelijk kwaad'. De leiding kijkt vaak onvoldoende naar digitale weerbaarheid en cybersecurity als een waarborg voor digitalisering en groei. Er is een grote (culturele) afstand tussen het management en de IT-afdeling, waardoor bedrijfseconomische afwegingen van digitaal risicomanagement vaak onder de tram komen. Incident response is meestal *ad hoc* geregeld.

- **Overig MKB**. Dit is zeker in aantallen maar ook in economische omvang de grootste groep ondernemingen. In veel gevallen betreft het kleinere bedrijven en organisaties die niet veel aandacht hebben voor informatietechnologie en onwetend en onbekwaam zijn aangaande cybersecurity. Het is immers niet hun *core business*. Diensten worden veelal uitbesteed en cybersecurity afwegingen maken zelden deel uit van bedrijfsvoeringbeslissingen. Bij incidenten valt men terug op de leveranciers van ICT-diensten.[xviii]

Sectoren Zuid-Hollandse economie. In verschillende sectoren van de Zuid-Hollandse economie zijn bepaalde activiteiten van incident response gebundeld om de organisaties en bedrijven te helpen de impact van cyberincidenten te beperken. Het is daarom goed om de verschillende sectoren die onderwerp zijn van dit onderzoek te beschouwen. We beperken ons hier tot zeven sectoren die een belangrijke bijdrage leveren aan de regionale economie. Een meer uitgebreide analyse per economische sector vinden we in bijlage.

- **Haven Rotterdam en de maritieme delta**. De haven van Rotterdam heeft incident response goed georganiseerd, na de *wake-up call* van 2017 (Not-Petya aanval op APM-terminals). In de haven zijn veel bedrijven aangemerkt als AED. Deze hebben meld- en zorgplicht. Ze moeten incidentresponse plannen hebben en beoefenen. Bij incidenten worden ze ondersteund vanuit het CSIRT van het NCSC. De overige bedrijven kunnen gebruik maken van de diensten van FERM. FERM bouwt zich uit als een volwassen CyberWeerbaarheidscentrum, die niet alleen informatie deelt en awareness programma's verzorgt, maar ook gezamenlijke diensten voor incidentafhandeling opzet.
- **Horticultuur bedrijven/Greenport**. Bij de meeste bedrijven is incident response ad hoc geregeld. In veel gevallen wordt teruggevallen op leveranciers van de technologie. Als er al incidentresponse plannen zijn, zijn die vaak gericht op fysieke incidenten. Sommige telersverenigingen denken na over digitale weerbaarheid om incidenten te voorkomen, zoals goede back-up voorzieningen en fail-over systemen. Samenwerking in ketens of met stakeholders staat nog in de kinderschoenen. De zaadveredelaars hebben een meer volwassen system van incident response, ook omdat ze een complexe wereldwijde infrastructuur hebben, en waardevol IP.
- **High Tech Systemen en Materialen (HTSM) industrie**. Er zijn een aantal grotere bedrijven met een gemonitoorde ICT-dienstverleningen hebben en die incident response redelijk onder de knie heeft. Plannen voor de impact van cyberincidenten op de bedrijfsvoering zijn niet altijd even volwassen. Bij de meeste MKB-bedrijven is incident response ad hoc geregeld. In veel gevallen wordt teruggevallen op leveranciers van de technologie. Als er al incidentresponse plannen zijn, zijn die vaak gericht op fysieke incidenten. Samenwerking in ketens of met stakeholders staat nog in de kinderschoenen.
- **Ruimte- en luchtvaartcluster**. Deze sector hoort bij de meer volwassen sectoren voor cyber incident response. Dit heeft ook te maken met de eisen die klanten stellen en de waarde van het *intellectual property*. De meeste grotere bedrijven hebben een SOC en monitoren cybersecurity

continue. Er is ervaring met incident response en men werkt samen met overheid of gelijksoortige bedrijven.

- **De Medical Delta en de biotech industrie**. De sector kent een grote mate van verscheidenheid. Iedereen heeft te maken met persoonlijke data en patiëntengegevens die vallen onder AVG. Het besef dat cyber incident goed geregeld moet zijn, is er zeker. Multinationals rapporteren aan vaak buitenlandse hoofdkantoren en zijn gesloten over hun maatregelen en volwassenheid. Maar omdat er grote belangen zijn en deze beursgenoteerde ondernemingen onder toezicht staan, kan worden aangenomen dat incident respons volwassen is. Voor de grote (academische) ziekenhuizen geldt dat ze veel aandacht hebben voor de impact van IT uitval op hun medische zorgverlening. Incident responseplannen zijn doordacht en uitgewerkt. Niet altijd zijn plannen voor incidenten veroorzaakt door cyberuitval goed beoefend met alle stakeholders, inbegrepen de veiligheidsregio. De grote groep MKB in deze sector baart meer zorg. Ze staan er vaak alleen voor, hebben maar beperkte kennis en hebben ondersteuning nodig.
- **Industrie voor defensie en veiligheid**. Als bedrijven in de sector de zaak niet op orde zou hebben, wint men geen contracten. De klant vereist een hoge beveiligingsstandaard, via de ABDO-regeling (Algemene Beveiligingseisen voor Defensie Opdrachten). Dat betekent overigens niet dat in alle gevallen incident response op orde is. Bij de grotere bedrijven wel.
- **Telecom en digitale dienstverlening**. Deze sector is voor cyberincident response sterk gereguleerd door de overheid, niet alleen via de Wbni, maar ook via de Telecomwet. De Digitale Service Providers (DSP) monitoren hun dienstverlening en werken nauw samen met CSIRT/NCSC en CSIRT-DSP van het Ministerie van Economische Zaken.

Conclusie incident response. Vrijwel alle besproken economische sectoren van de provincie Zuid-Holland kennen een hoge mate van digitalisering en zijn kwetsbaar voor cyberaanvallen. De mate waarin ondernemingen of organisaties volwassen zijn op het gebied van cyberweerbaarheid en eventuele cyberincidenten adequaat afhandelen varieert sterk. De mate waarin een onderneming of organisatie het onderwerp op orde heeft is in grote mate afhankelijk van de aandacht die het bestuur of de Raad van Commissarissen aan cybersecurity geeft.
Gereguleerde ondernemingen zijn over het algemeen beter voorbereid op cyberincidenten dan ondernemingen die niet aan specifieke cybersecurityregels moeten voldoen. Behoudens bij een aantal specifieke sectoren die een wettelijke verplichting hebben (defensie-industrie, AED-ondernemingen en organisaties, telecom en ICT-dienstverleners) is het managen van digitaal risico en incident response bij veel bedrijven voor verbetering vatbaar.
Het is op de bestuurstafel niet altijd gemeengoed om af te wegen om wel of geen technische cybermaatregelen te nemen op basis van risicoanalyse, om zich te verzekeren, om tijd in te ruimen voor cybercrisisoefeningen of extern Boardadvies in te winnen.
De AED-bedrijven in de regio krijgen gegarandeerde ondersteuning uit het nationale CSIRT bij een cyber incident en handelen dit af, vaak met externe consultancy steun. Bij het MKB ligt dit anders: een grote groep MKB-bedrijven hebben wel incident response plannen, maar vaak niet aangepast voor digitale incidenten; zelden worden deze plannen regelmatig beoefend en up-to-date gehouden.

Wanneer een cyberaanval grote maatschappelijke impact heeft zal naast het NCSC of een ander CSIRT ook de regionale driehoek een rol gaan spelen bij incident response. Regionale of sectorale cyberoefeningen om incident response te testen zijn niet structureel geregeld, anders dan deelname van regionale overheid en AED-bedrijven bij de landelijke cyberoefeningen van het NCTV. Die oefeningen hebben lage frequentie en bereiken een belangrijke, maar slechts kleine groep ondernemingen.

Wat kunnen we eraan doen?

- **Organiseren van Cyber-brandweer**. *Cyber Security Incident Response Teams* (CSIRT) of *Cyber Emergency Response Teams* (CERT) zijn de brandweer voor cybersecurity incidenten. Er is een landelijk CSIRT bij het NCSC dat leverplicht heeft aan AED-bedrijven en organisaties, maar niet aan andere organisaties in Zuid-Holland. CSIRTs helpen om de impact van een cyberincident te beperken en zo snel mogelijk weer de effecten van de aanval teniet te doen. Er bestaan voor een aantal sectoren *Cyber Emergency Response Teams* (CERT), onder andere voor de zorg en voor universiteiten en hogescholen. Deze CERTs hebben een vergelijkbare functie als de CSIRT. Gezien het grote aantal ondernemingen en organisaties in de provincie die geen gegarandeerde steun krijgen bij cyberaanvallen, is er behoefte aan een Cybersecurity Incident Response Team (CSIRT) of een netwerk van CSIRTs om incidenten te helpen managen en om een grote groep ICT-gebruikers ten dienste te staan, zoals MKB.
  Een regionaal dekkend CSIRT op provincie/regio niveau is een goede 'eerste hulp bij cyberincidenten'-functie om bedrijven en organisaties te helpen wanneer er geen steun beschikbaar is van het landelijke CSIRT, maar het is ook een forse investering. Voordeel is dat alle economische sectoren worden bediend; nadeel is dat wellicht kennis bestaat van specifieke aanvallen op een bepaalde economische sector. Een CSIRT/CERT is geen goedkope functie; het vergt een 24/7 helpdesk en een cyberexpertteam met verschillende hoogwaardige expertises en apparatuur om snel IT-systemen van slachtoffer-bedrijven te kunnen onderzoeken.
- Een belangrijke vraag is of een CSIRT een overheidstaak is, vergelijkbaar met de rol van de brandweer en die van het nationale CSIRT, of een taak te organiseren door het bedrijfsleven gezamenlijk. Ook kan incident response puur een commerciële dienstverlening zijn die ad hoc wordt ingehuurd; ondernemingen zoals Fox-IT leveren dergelijke diensten bij cyber incidenten. Er is een studie nodig naar dit vraagstuk. Als er besloten wordt tot een CSIRT te komen, moeten er structurele middelen worden gereserveerd (publiek of privaat) om deze CSIRTs operationeel te houden. Gezamenlijke inkoop door een economische sector of regio is zeker een optie.
- **Afstemmen incident response plannen**. Incident response is in eerste instantie een verantwoordelijkheid van bedrijven en organisaties zelf. In sommige gevallen kunnen incidenten maatschappelijke impact hebben, zoals bijvoorbeeld tijdens de NotPetya aanval in Rotterdam. Bij digitale ontwrichting van landelijke AED's worden *disaster recovery* mechanismen van vitale infrastructuren en diensten geborgd met steun van het NCSC. Incident response plannen van ondernemingen en organisaties die voor de provincie of regio belangrijk zijn vanwege maatschappelijke veiligheid of economische impact moeten op elkaar en met die van de overheid worden afgestemd. Ook moet er een oefen- en simulatieplan komen om te zorgen dat plannen getoetst worden op kwaliteit en up-to-date blijven.
- ***Situational awareness***. Momenteel is er in de regio geen goed beeld van de actuele cyberdreiging op de maatschappij en economie beschikbaar. Wel heeft de politie een dashboard, maar dat schetst niet de volledige situatie, namelijk vooral de incidenten waarvan aangifte is gedaan. Ook zijn er landelijk inzichten in de staat van cyberdreiging vanuit het CSIRT van het NCSC. Telecomdienstverleners kunnen vaststellen waar problemen bestaan in haar netwerken. Maar er is geen compleet beeld dat nodig is voor effectief incident- en crisismanagement. Er is behoefte aan een regionaal dashboard dat kijkt naar trends en soorten van cybersecurity incidenten in de regio, mogelijk per sector – met name incidenten die gelijksoortige aanvalsgroepen of tactieken, technieken en procedures gebruiken, met als doel bedrijven en organisaties tijdig te waarschuwen en maatregelen te nemen.

- **Incident communicatie**. Cyberincidenten ontwikkelen zich met lichtsnelheid. De impact van cyberincidenten gaan als een schok. Ineens staat alles stil, als een of meerdere belangrijke IT- of OT-systemen succesvol zijn aangevallen. Dit hoeven niet altijd gerichte aanvallen op een bedrijf te zijn. Onbekende computerkwetsbaarheden (*zero days*) of door te laat *patchen* van systemen kunnen meerdere bedrijven of organisaties tegelijk last krijgen van cyberaanvallen. Om goede incident communicatie te verzekeren is nodig:
    - Er komt een communicatieplan om beter aan bedrijven en organisaties uit te leggen wat men moet doen bij een cyberincident. Dit betreft het melden van incidenten, doen van aangifte bij cybercrime, inroepen van hulp bij CSIRTs en dienstverleners.
    - Er komt een overzicht van essentiële (ICT-) bedrijven die nodig zijn voor het in dienst houden en herstel van voor de regio vitale ICT-diensten en infrastructuren en hoe deze te bereiken is, ook buiten normale uren.
    - Probleem van een grotere cyberaanval is dat reguliere ICT-netwerken niet meer kunnen beschikbaar zijn. De provincie of veiligheidsregio's verzekeren dat een informatiesysteem in de regio beschikbaar is dat functioneert als de normale ICT-diensten niet meer voldoende werken. Het draagt er zorg voor dat activatie ervan is beoefend. Er zijn middelen beschikbaar om dit netwerk het in stand te houden en ermee te oefenen.
- **Regionale cyberoefeningen**. De provincie/veiligheidsregio's i.s.m. het bedrijfsleven implementeren een programma van regelmatige testen en cybersecurityoefeningen om de regionale cyberweerbaarheid te meten en verbeteren, in aanvulling op nationale programma's. In eerste instantie zullen de oefeningen zich richten op verbeteren van awareness, met name van leidinggevenden in bedrijven en organisaties. Deze simulaties zijn kort en krachtig en vooral ook enthousiasmerend. Later verschuift het accent naar incident response en crisismanagement en *lessons learned* programma's.

E-CRIME en WETSHANDHAVING

Opsporen en wetshandhaving van e-crime is in Nederland landelijk geregeld bij de Nationale Politie en het Openbaar Ministerie (OM). De provincie en de regio maakt gebruik van en werkt samen met deze organisaties in de regio. Gezien het feit dat e-crime geen grenzen kent, is dit een voorwaarde voor succes. De landelijke organisaties zijn weer internationaal verbonden met politieorganisaties van andere landen of via internationale organisaties, zoals Europol.

Nederland is internationaal toonaangevend in haar inzet om de samenleving tegen cybercrime te beschermen.[xix] Na twee versies van een cybersecuritystrategie en een actieplan, zijn er recent ook twee wetten ingevoerd die helpen tegen cybercrime op te treden. Het betreft de Wet beveiliging netwerken en informatiesystemen (Wbni), eerder besproken, en de Wet Computercriminaliteit III. Deze wet versterkt in het wetboek van Strafrecht (Sr) en het wetboek van Strafvordering (Sv) de opsporing en vervolging van computercriminaliteit. Hiermee wordt de wetgeving aangepast aan de technologische ontwikkelingen op internet en het gebruik van computers voor communicatie en de verwerking en opslag van gegevens. Ook worden burgers beter beschermd tegen bijvoorbeeld het verleiden van een minderjarige tot ontucht (*grooming*) of de verspreiding van kinderpornografie en ernstige computercriminaliteit. Met deze wet mogen politie en justitie heimelijk en op afstand (online) onderzoek doen in computers (pc, mobiele telefoon of server). Opsporingsambtenaren krijgen meer mogelijkheden om verschillende onderzoek handelingen toe te passen bij de opsporing van ernstige delicten. Zij kunnen bij een zeer ernstig misdrijf (mensenhandel of deelname aan een terroristische organisatie) gegevens ontoegankelijk maken of kopiëren en als het gaat om een ernstig misdrijf communicatie aftappen of observeren.

Voor de wetshandhaving heeft deze regering de capaciteiten van zowel de politie als het Openbaar Ministerie verder versterkt. De Politie is in staat verschillende vormen van cybercrime op te sporen en de criminelen voor het gerecht te brengen. Het landelijke Team High Tech Crime bestaat al sinds 2007 als onderdeel van de landelijke eenheid. Recent zijn er bij de 10 politieregio's cyber opsporingsteams toegevoegd. Bij de politie in Den Haag is een Expertise Centrum Cyber opgericht. In de Rotterdamse haven wordt cybercrime vooral door de zeehavenpolitie uitgevoerd. Ondanks extra budgetten en eenheden lijkt de groei van cybercrime sneller te gaan dan de groei van de digitale opsporingsdiensten. [xx]

Ook het Openbaar Ministerie ontwikkelt mee met de groeiende cybercriminaliteit en heeft inmiddels veel kennis opgebouwd. Bij elk parket is de cyberportefeuille ingericht. Cyberofficieren zijn daarbij de experts die cybercrimezaken aanjagen en vraagbaak zijn voor andere officieren. Bij het gerechtshof in Den Haag is het kenniscentrum Cybercrime opgericht. Dit kenniscentrum verschaft juridische en praktische kennis over cybercrime en basisinformatie over computertechnologie aan rechters, raadsheren en gerechtsambtenaren in Nederland.

Cybercrime wordt regionaal besproken in de driehoek (Gemeente, Politie, OM). Naast de traditionele driehoek waarin politie, Openbaar Ministerie en lokale overheid overleggen, is in Zuid-Holland ook een "cyberdriehoek" actief. In maart 2020 kwam de eerste cyberdriehoek, bestaande uit de burgemeester/regionaal portefeuillehouder cybercrime, de Haagse politiechef en de hoofdofficier van justitie voor het eerst bij elkaar. De cyberdriehoek is van plan om een breder bewustzijn rond virtuele en fysieke veiligheid te creëren, met name bij jongeren. Meerdere keren per jaar zal er in dit verband worden overlegd. [xxi]

Cybercrime komt veel voor, maar wordt zelden gemeld. Bureau Boekhorn heeft in 2019 onderzoek gedaan naar de regionale aanpak van cybercrime.[xxii] Zij stellen vast dat naast individuele digitale criminaliteit, ook bedrijven vaak slachtoffer zijn van cybercrime: uit CBS-onderzoek in 2017 blijkt dat ruim 20 procent van de bedrijven met minstens tien werkzame personen in 2016 te maken heeft gehad met de gevolgen van cyberaanvallen. Vooral bedrijven in de financiële sector en de energiesector hadden hier last van, maar ook bedrijven in de maakindustrie, transport/logistiek en feitelijk in elke sector in meer of mindere mate. Bij de helft van de getroffen bedrijven leidden deze aanvallen ook tot hoge kosten.

Van deze delicten wordt echter zelden bij de politie melding gemaakt of aangifte gedaan. Boekhoorn beschrijft dat van hacks bijvoorbeeld in minder dan 10% van de gevallen door slachtoffers aangifte wordt gedaan. Ook in andere onderzoeken wordt gewezen op lage aangiftepercentages bij zowel individuele slachtoffers (13%); als bij organisaties (13%). Bij het MKB doet maar 3,6% een aangifte bij de politie (2015). Uit de meest recente Veiligheidsmonitor komt naar voren dat in 2017 8% van de slachtoffers van cybercrime hiervan bij de politie aangifte deed, dit is vergelijkbaar met voorgaande jaren en zal niet veel verbeterd zijn.

Waarom is geen aangifte doen een probleem? Dergelijke cijfers zeggen niet veel over de feitelijke omvang van cybercriminaliteit, want er wordt een aanzienlijke hoeveelheid niet-geregistreerde cybercriminaliteit vermoed. Het belang van een aangifte is echter groot: het is het startpunt voor een opsporingsproces en het vergroot de kennis over het aantal en de aard van de delicten die worden gepleegd.
Niet aangeven en melden betekent ook dat in veel gevallen losgeld voor ransomware aanvallen wordt betaald en dus criminelen worden ondersteund. Dit is onwenselijk, omdat het tot meer en meer complexe aanvallen zal leiden, immers de criminele organisaties krijgen meer capaciteit en betere middelen om aanvallen uit te voeren.
Tenslotte leidt gebrek aan transparantie niet tot het leren van lessen om dergelijke aanvallen te voorkomen. Het is begrijpelijk dat een bedrijf of organisatie niet openlijk ‘met de billen bloot’ wil wanneer men onvoldoende maatregelen heeft genomen om een aanval te voorkomen en slachtoffer is geworden. Maar anderzijds is het noodzakelijk dat we goed begrijpen hoe aanvallen worden uitgevoerd, welke maatregelen nodig zijn om dergelijke aanvallen te voorkomen en hoe met die kennis de awareness van bestuurders en specialisten kan worden verhoogd en processen kunnen worden verbeterd. Complimenten zijn gepast voor de wijze waarop de Universiteit Maastricht zes weken na een serieuze cyber ransomware aanval (eind december 2019) volledige openheid van zaken heeft gegeven en een publiek lessons learned seminar heeft georganiseerd.

Wat kan er verbeteren?

- Kennelijk is er sprake van onvoldoende bekendheid, met name bij het MKB met de relevante wet- en regelgeving en de daaraan gerelateerde meld- en afhandelingsprocedures voor de ondernemingen en organisaties in de provincie/regio om zich te borgen voor cybercrime, onderbreking van belangrijke dienstverlening en verlies van data en infrastructuur. Er zou een stimuleringsprogramma moeten worden opgezet om de bekendheid van de cyber wet – en regelgeving te vergroten en hoe te handelen als slachtoffer van e-crime, met name voor MKB en organisaties.
- Ook is een goede analyse van sector gerelateerde wet- en regelgeving aan te bevelen, o.a. voor banken, beursgenoteerde bedrijven, bedrijven die AED of ICT/telecomdiensten leveren en

bedrijven die persoonsgegevens beheren. Dit brengt de problematiek dichter bij de verschillende economische sectoren in de provincie.

- Waar relevant zou in navolging van politieregio Den Haag via “cyberdriehoeken” naleving van deze wet- en regelgeving verder kunnen stimuleren.
- Er is geen helder beleid of richtlijn over het betalen van ransomware. Mag je (ter overleving van je onderneming) ransom betalen aan criminele organisaties? Ook als die op de internationale terroristenlijst staan? Helderheid borgt ook transparantie en zal tot meer aangiftes leiden.
- Het verdient aanbeveling een evaluatieprogramma in de regio op te zetten voor continue verbetering van de afhandeling van cybercrime incidenten.
- Awareness en bekendheid met de materie kan worden vergroot door cybercrime incidenten tijdens oefeningen en simulaties voor bedrijven en organisaties in de provincie/regio op te nemen en deze oefeningen toegankelijk te maken voor meer ondernemingen, met name het MKB, die niet worden uitgenodigd voor nationale oefeningen.
- De provincie/regio of economische sector kunnen beter begrip en handelingsperspectief voor e-crime stimuleren door lessons learned seminars te ondersteunen.

DELEN VAN INFORMATIE

Voor de veiligheid van Nederland en om de economie te beschermen tegen cyberaanvallen, is het van groot belang dat publieke en private partijen samenwerken en cybersecurityinformatie met elkaar delen. Het NCSC is het centrale aanspreekpunt in Nederland voor cybersecurity en verantwoordelijk voor incident response en het delen van informatie. In de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is geregeld hoe het NCSC voor een sector relevante informatie deelt tussen de overheid en het bedrijfsleven. Ook verwerkt zij de dreigingsinformatie om nieuwe strategieën en tactieken met de stakeholders te ontwikkelen en om adequaat te kunnen reageren op gemelde cyberincidenten. Het NCSC werkt samen met de veiligheidsdiensten om relevante cyberdreigingsinformatie te analyseren en gereed te maken voor praktisch gebruik voor bescherming van organisaties en diensten.

De Wbni regelt deze informatievoorziening met name ten behoeve van aangewezen vitale dienstverleners (AED) en digitale dienstverleners [xxiii]. Het CSIRT van het NCSC zal daarnaast informatie delen met aangewezen computercrisisteams (CERTs), zoals Z-CERT of SURF-CERT. Ter voorkoming van nadelige maatschappelijke gevolgen kan het NCSC ook informatie delen met andere organisaties, die objectief kenbaar tot taak hebben andere, dus derde organisaties of het publiek daarover te informeren. Voorwaarde is dat noodzakelijk wordt geacht en de informatie zorgvuldig wordt beheerd en gebruikt. Het NCSC zal dus geen informatie rechtstreeks aan bedrijven verstrekken, ook ter voorkoming van een oneerlijke concurrentiepositie.

Het Digital Trust Center [xxiv] speelt bij informatievoorziening aan het bedrijfsleven een belangrijke een rol. Het DTC helpt met veilig digitaal ondernemen. Het DTC deelt generieke informatie via haar website, toegespitst op het MKB. Ook levert ze tools, zoals een cyberweerbaarheidsbasisscan voor ondernemers. Het DTC zet faciliteert een netwerk van cyberweerbaarheidscentra en stimuleert het delen van *best practice*. Via het DTC kunnen sectoren, bijvoorbeeld via een cyberweerbaarheidscentrum van een industriesector worden geautoriseerd om onder voorwaarden ook gerubriceerde dreingingsinformatie te ontvangen.

Inmiddels is ook het Nationaal Detectie Netwerk (NDN) [xxv]uitgerold. In het NDN werken Rijksoverheidsorganisaties en vitale private organisaties (AED's en digitale dienstverleners) samen en delen onderling dreigingsinformatie om cybersecurity risico's en gevaren sneller waar te nemen. NCSC, de AIVD en de MIVD verzamelen informatie over cyberdreigingen en stellen die beschikbaar aan het NDN. Aangesloten organisaties nemen actief deel aan het NDN: zij moeten dreiging kunnen ontvangen, verwerken en delen. Dit betekent ook dat deelnemers hun monitoring en incident response proces op orde hebben, kunnen reageren op gevonden hits en zelf dreigingsinformatie kunnen aanleveren. Vitale partijen nemen kosteloos deel aan het NDN.

Het NCSC faciliteert verschillende *Information Sharing and Analysis Centers* (ISACs). Een ISAC is een sectoraal overleg over cybersecurity. In een ISAC creëert men een vertrouwde omgeving met organisaties uit dezelfde sector om gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity te delen. Die informatie bevat o.a. kwetsbaarheden in ICT-producten, vormen van cyberaanvallen, profielen van aanvallers. Er is een ISAC voor Energy; voor de financiële instituten; voor drinkwatervoorziening; voor de havens; voor chemie/olie; voor luchtvaart; voor de sector waterwerken: 'Keren en Beheren'; voor juridische ondernemingen en aspecten; voor nucleaire installaties; voor Pensioenfondsen; voor de Rijksoverheid;

voor de telecomsector en voor de gezondheidszorg. Het Ministerie van Defensie verzorgt een ISAC-functie voor de defensie-industrie. Het NCSC gebruikt in haar samenwerking met vitale diensten onder andere een digitaal platform, het *Malware Information Sharing Platform* (MISP) [xxvi]. Dit is een project dat binnen de NAVO is begonnen en inmiddels door de EU en landen verder is verbeterd en ook voor het internationaal delen van dreigingsdata wordt gebruikt. Digitale datacommunicatie is belangrijk, omdat snelheid van het uitwisselen van dreigingsinformatie essentieel is voor voorbereiding op een mogelijk op handen zijnde cyberaanval.

Landelijk dekkend netwerk van informatieknooppunten
Het NCSC streeft naar een landelijk dekkend netwerk van sectorale informatieknooppunten om cyberdreigingsinformatie te delen. Een sectorale aanpak is van belang omdat dit vaak georganiseerde samenwerkingsverbanden van bedrijven zijn die gelijksoortige digitaliseringsdreigingen en kwetsbaarheden hebben, maar ook vaak in ketens werken dus onderlinge afhankelijkheid. Er is natuurlijk ook concurrentie in economische sectoren, maar voor veel bedrijven geldt dat samenwerking op het gebied van cybersecurity boven bedrijfsbelangen gaat.

Sectoren die niet als essentieel voor nationaal belang zijn aangemerkt, kunnen zelf een ISAC-functie oprichten. Het DTC ondersteunt hen daarbij. [xxvii] Zo voorziet Z-CERT [xxviii] zorgverleners van informatie en SURFnet de universiteiten en hogescholen. Inmiddels zijn vier sectorale organisaties geaccrediteerd voor dit netwerk. [xxix] Onder voorwaarden kunnen dergelijke ISACs ook geaccrediteerd worden om gevoelige informatie van het NCSC te ontvangen. Inmiddels zijn er een aantal sectorale cyberweerbaarheidscentra bevoegd om als ISAC te functioneren, of zijn in het proces om die bevoegdheid te krijgen. Ook FERM in Rotterdam ontwikkelt zich in die richting.

Er zijn ook andere organisatievormen operationeel, zoals de stichting Connect2Trust (C2T) [xxx] die deze functie vervult. Connect2Trust is een cross-sectoraal samenwerkingsverband tussen (inter)nationale in Nederland actieve bedrijven. Het biedt deelnemende bedrijven een veilige en vertrouwde omgeving waarbinnen private partijen die onderdeel zijn van Connect2Trust, samen met de (cyber)security belaste overheidspartijen gevoelige en vertrouwelijke informatie over cyberdreigingen en *best practices* kunnen analyseren en uitwisselen. De bedrijven in Connect2 Trust, zoals Coolblue, PostNL, KLM, Centric, maar ook Rijk Zwaan en de Belastingdienst hebben vaak een eigen Security Operations Center (SOC) of maken gebruik van ingehuurde SOC-diensten en hebben dus zelf data om te delen. C2T heeft een kleine overhead; de bedrijven doen het meeste werk zelf. Ook C2T werkt aan accreditatie voor het Landelijk Dekkend Stelsel.

Helder is dat het Landelijk Dekkend Stelsel nog een lange weg te gaan heeft om landelijk dekkend te worden. Maar een klein deel van de economie wordt bediend.

MKB. Voor veel bedrijven in het MKB, die geen eigen Security Operations Center (SOC) of Computer Emergency Response Team (CERT) hebben, is deelname aan een ISAC te hoog gegrepen. Deze bedrijven, althans die hun IT en OT zelf in beheer hebben, behoeven informatie om hun ICT-infrastructuur en -diensten veilig te houden. Voor hen zijn '*threat alerts*' met een handelingsperspectief en actuele informatie over kwetsbaarheden in ICT-producten zeer relevant. Ook hebben die organisaties behoefte aan *best practices* om hun ICT zo veilig mogelijk te houden. Het NCSC publiceert dergelijke informatie regelmatig. Generieke informatie voor het MKB wordt door het DTC verstrekt.

Wat betekent dit voor de provincie/regio? De voor Nederland aangewezen essentiële diensten en digitale dienstverleners worden door het NCSC voorzien van actuele cybersecurity informatie. Belangrijke bedrijven in de provincie, zoals in de Rotterdamse haven, vliegveld Den Haag-Rotterdam, chemie en olie industrie zoals Shell, de banken en financiële instellingen en grotere bedrijven in de defensie-industrie worden voldoende voorzien van deze informatie. Veel van hen nemen ook deel aan het Nationaal Detectie Netwerk. Zorginstellingen hebben een voorziening via Z-Cert; universiteiten en hogescholen via SURF.nl. Een tiental grotere bedrijven in de regio die niet onder essentiële diensten vallen, heeft gezamenlijk zelf de *information sharing* functie opgericht, zoals in de stichting Connect2Trust. In de Rotterdamse haven vervult FERM deze rol.

Een belangrijk deel van de Zuid-Hollandse economie heeft echter geen toegang tot actuele cybersecurityinformatie. Het beoogde Landelijk Dekkend Netwerk van Informatieknooppunten is verre van dekkend in de Provincie Zuid-Holland. Wel kunnen bedrijven via publicaties door NCSC en DTC generieke alerts ontvangen. Er is geen voorziening voor sectorale informatie- en kennisdeling, behalve in de Rotterdamse haven via FERM, dat op weg is voor accreditatie voor het Landelijk Dekkend Netwerk. Dit is een omissie omdat sectoren zoals de glastuinbouw of hightech maakindustrie vaak specifieke ICT-diensten gebruiken, zoals meet- en regelapparatuur, met specifieke risico's en dreigingen. De generieke informatie van het DTC kan onvoldoende zijn om potentiële aanvallers telkens een stapje voor te zijn.

Wat kunnen we eraan doen?

- De overheden, ondernemersorganisatie en onderwijs/kennisinstellingen, verenigd in de EBZ zijn expliciet in het belang van uitwisseling van inlichtingen en informatie tussen overheden, overige maatschappelijke organisaties en industriesectoren en stimuleert de opzet van een netwerk van regionale en sectorale ISAC-functies gekoppeld aan het landelijke netwerk van het NCSC en het DTC.
- Het is gewenst dat economische sectoren, net zoals FERM voor de Rotterdamse haven, elk een ISAC-functie institutioneel organiseren voor hun sector, te beginnen met basale informatie-uitwisseling over cybersecurity. Als men niet kan aansluiten op een landelijke informatievoorzieningscapaciteit voor de economische sector, dan ligt het voor de hand regionaal in de sector te beginnen om de omissie weg te werken. Die sectorale ISAC-functie in de regio kan later uitgroeien tot landelijke informatievoorziening in de economische sector. Het DTC kan helpen bij het opzetten van de ISAC-functie. Dit past in de nationale strategie om een landelijk dekkend netwerk op te bouwen.
- Het DTC coördineert ook cross-sectoraal en met het Rijk. Nadere evaluatie moet duidelijk maken of landelijke samenwerking voldoende de behoeften in de regio afdekt. Met name geldt dit voor het MKB dat geen deel uitmaakt van een georganiseerde economische sector.
- Deze structuur verzekert dat er mechanismen bestaan (meldschema's, technologie, etc.) voor het uitwisselen van informatie tussen sectoren (tweerichtings), zowel voor operationele informatie (near-real-time) als voor forensische informatie (post facto) tussen alle relevante partijen in de provincie/regio, publiek en privaat.
- Sectorale ISACs moeten voldoende aandacht hebben om ook het MKB van relevante cyberinformatie en advies te voorzien, in aanvulling van wat het DTC verstrekt. Vertrouwen is daarbij belangrijk om dergelijke gevoelige informatie over de bedrijfsvoering te delen. Bekendheid met de sectorale bedrijfsvoering en fysieke nabijheid zijn belangrijk om dat vertrouwen te verzekeren. Natuurlijk moeten voldoende middelen worden begroot door zowel overheid als bedrijven om continuïteit te verzekeren.

- Het netwerk van ISACs in de provincie dragen elk bij aan het gezamenlijke cyber dashboard van de provincie voor het *verbeteren van situational awareness* rondom een incident en cross-sector en cross-stakeholder incident management.

COMPETENTE BEROEPSBEVOLKING

Elke organisatie is voor het bereiken van haar doelstellingen afhankelijk van kennis en ervaring van haar werknemers. Digitalisering en cybersecurity zijn geen onderwerpen waarmee het gros van de beroepsbevolking is opgegroeid. Vrijwel iedereen werkt momenteel digitaal en is voor het werk afhankelijk van informatietechnologie. Ouderen begrijpen vaak het belang van digitale veiligheid wel, maar vinden het lastig de juiste maatregelen te nemen. Voor de jeugd geldt dat zij zeer vaardig zijn in het gebruik van digitale middelen, maar vaak de risico's ervan onderschatten. Voor het merendeel van de beroepsbevolking ontbreekt kennis van basisvaardigheden om digitaal veilig te kunnen werken.

Het is zinvol om de cybergereedheid van de beroepsbevolking in Zuid-Holland te duiden in drie groepen: het bestuur en toezicht; de cyberspecialisten; de medewerkers. Overigens is cybersecurity een onderwerp met vele invalshoeken. Het vereist niet alleen technologiekennis, ook kennis van wet- en regelgeving, ethiek, gedrag van de digitale medewerker, privacyaspecten, risicomanagement en bedrijfsvoering, opleidingskunde, kortom: een breed scala aan aspecten.

Bestuur en toezicht. Elk volwassen management van een organisatie focust zich op het beheersen van risico's voor de bedrijfsvoering om de continuïteit van de bedrijfsvoering te borgen. Ook bij de overheid is risicomanagement gemeengoed. Het managen van *technisch risico* en digitale beveiliging van organisaties, publiek of privaat, is een volgende stap voor veel organisaties die in toenemende mate afhankelijk zijn van digitale processen om hun bedrijf te runnen. Het vertalen van dat technische risico naar bedrijfsvoeringsrisico en *value at risk* staat bij veel ondernemingen nog in de kinderschoenen. Een dergelijke benadering is van belang om onderbouwde keuzes te maken of er maatregelen worden genomen om het cyberrisico te beperken, of het risico bewust te accepteren of dat er gekozen wordt voor risico overdracht, bijvoorbeeld door cyberrisico te verzekeren.

Het management, vooral van niet-gereguleerde ondernemingen en MKB, is vaak niet bekend met methoden om digitale bedrijfsvoeringsrisico 's aan te pakken, ziet cybersecurity vaak als een kostenpost, en het onderwerp digitaal risicomanagement wordt niet regelmatig in de boardroom besproken. Het is voor hen lastig vast te stellen: hoeveel cyberveiligheid is genoeg? Is die extra investering wel nodig, of *nice-to-have*? Toezichthouders vinden het vaak lastig om de juiste vragen te stellen aan het management en dóór te vragen, omdat ze het gevoel hebben niet boven de stof te staan. De afstand tussen de ICT-afdeling en het bestuur is vaak groot, zeker wanneer er geen CISO is aangesteld. Voor bestuur is ICT vaak een black box, iets wat lastig te bevatten is als je er niet in bent opgeleid.

Voor de kleinere bedrijven is het onderwerp nog ingewikkelder. Daar zijn vaak alle diensten uitbesteedt en neemt de directeur zelf de beslissingen, zonder vaak zelf voldoende kennis te hebben. Voor de techniek kan hij terugvallen op de dienstverlener, maar over de consequenties voor zijn bedrijfsvoering bij uitval moet hij zelf beslissen.

Natuurlijk is er sprake van verscheidenheid in de mate waarin het onderwerp aandacht krijgt. Cybersecurity gereguleerde ondernemingen voeren risico audits uit die op boardniveau worden besproken. Er bestaat veel aandacht voor compliance met die wetten of regels.

Toch wordt het belang voor het bestuur steeds helderder: [xxxi]

- Voortdurende verliezen: organisaties zijn in toenemende mate afhankelijk van digitale processen om hun bedrijf te runnen en ondanks hun investeringen in beveiliging, blijven ze

grote servicestoringen en aansprakelijkheid gerelateerde verliezen lijden als gevolg van cyberaanvallen.

- Minimale beveiliging: de huidige beveiligingsprocessen en -technologieën zijn meestal gericht op *compliance*-vereisten, die cruciaal zijn bij het definiëren van minimale beveiligingsnormen, maar niet voldoende zijn om organisaties te beschermen tegen steeds veranderende cyberdreigingen.
- Toenemende onderlinge afhankelijkheden: operationele technologie, informatie technologie, het internet der dingen en fysieke beveiligingstechnologieën hebben een groeiende onderlinge afhankelijkheid die een op risico's gebaseerde benadering van bestuur en beheer vereist.
- Incongruente benaderingen: de meeste organisaties zijn niet toegerust voor een op risico gebaseerde benadering van digitale beveiliging, aangezien ze geen gemeenschappelijke methoden hebben om cyberbedrijfsrisico's bij de verschillende belanghebbenden (bestuur, leidinggevenden, operaties, IT) te kwantificeren en te beheren. Vaak leidt dit tot over- en vaker tot onder-investering.

Executive en management opleidingen en trainingen. Een quick scan door de curricula van de universiteiten verbonden aan Leiden, Delft en Erasmus en de Nationale Cybersecurity Education Agenda toont dat in management- en bedrijfsvoeringopleiding cybersecurity en het managen van digitaal risico beperkt aandacht krijgt. Methoden om cyberrisico integraal onderdeel te maken van de bedrijfsvoering en financieel te maken worden niet structureel onderzocht of onderwezen.[xxxii] Via de Cyber Security Academie wordt cyber voor executives onderwezen, een goede stap. De hogeschool van Den Haag besteedt aandacht aan safety & security-riskmanagement, waaronder cybersecurityrisico's. Ook een aantal MBO-opleidingen onderwijzen cybersecurity en de risico's die het met zich meebrengt, ook buiten ICT-opleidingen. Deze opleidingen richten zich op toekomstige MKB-ondernemers, bijvoorbeeld in de tuinbouw.

Commerciële aanbieders domineren cybersecuritytrainingen voor bestuur en management; dit zijn niet alleen de 'big four' accountancy firma's, maar tal van gespecialiseerde bedrijven. Bij commissarissenopleidingen wordt dit onderwerp soms ook meegenomen. Een effectieve methode om de leiding van bedrijven te trainen zijn cybersimulaties of *tabletop* oefeningen, die zowel incident- als crisismanagement kunnen omvatten. Tijd inruimen voor dergelijke simulaties is een aandachtspunt bij veel bedrijven. Vaak moet er eerst een serieuze aanval zijn geweest bij een bedrijf of organisatie zelf of in de sector voordat dergelijke trainingen voldoende aandacht krijgen. Bij een aantal gereguleerde ondernemingen, zoals financiële instellingen zijn dergelijke trainingen vast onderdeel van de bedrijfsvoering. Het percentage van bestuurders of toezichthouders dat deze beschikbare opleidingen en trainingen heeft gevolgd is niet bekend, maar is naar verwachting niet heel hoog.

Cyberspecialisten.
Er is een nijpend tekort aan cybersecurityspecialisten in Nederland. Professor Bibi van de Berg, hoogleraar cybersecurity governance van de Universiteit Leiden en Inge Bryan, cybersecurityadviseur van Deloitte vragen om een Deltaplan voor Cyber Security: *"…kennis en kunde op het terrein van cybersecurity blijven achter. Er is een schreeuwend tekort aan goed geschoolde professionals, zowel bij de overheid als in de wetenschap en in de private sector. Door tekorten aan mensen en middelen kan het hoger onderwijs onvoldoende studenten opleiden om de gaten te dichten…Tegelijkertijd ziet geschoold personeel op dit terrein, zowel binnen de universiteiten alsook binnen het bedrijfsleven, steeds vaker mogelijkheden om naar het buitenland te vertrekken, en is er dus sprake van een braindrain. Het Deltaplan ICT, dat gericht is op het creëren van meer werk in de ICT-sector noemt het thema cyber security slechts zes keer, en geeft dit domein geen prioriteit. … Het is tijd voor een Deltacommissaris die*

over alle beleidsterreinen een vorm van doorzettingsmacht heeft, die alle goede maar ontoereikende initiatieven samenbrengt en naar een hoger plan trekt. Die tegengestelde belangen oplost, richting geeft." [xxxiii]

CISO's van overheden en bedrijven die vitale diensten leveren en die vooral in het hogere risicodomein werken, bevestigen dit beeld. [xxxiv] Het is moeilijk om voldoende en goed gekwalificeerde mensen te vinden, zeker als het gaat om *hardcore* informatietechnologie. ICT-security specialisten op niveau 2 en 3 (HBO/WO) staan steevast in de top 3 van moeilijk te vullen vacatures. Een bijzonder lastige categorie zijn crypto-specialisten, die vaak uit het buitenland gehaald moeten worden. Dit maakt productontwikkeling en innovatie voor ondernemingen uitdagend. Ook maakt dit Nederland kwetsbaar en afhankelijk van buitenlands personeel en producten.

Een andere vaak genoemde tekortkoming is het tekort aan docenten op alle niveaus van; dit is een van de '*wicked problems*', een vicieuze cirkel. Er is enig beeld welke tekorten in welke expertisegebieden binnen cybersecurity er bestaan. Wel is helder dat bij verdere groei van digitalisering en toenemende cyberrisico's de onderwijsbehoefte zal toenemen. Daartoe zijn initiatieven genomen om meer docenten op te leiden, o.a. door de Cyber Security Academy, ROC Mondriaan en de Haagse Hogeschool. Ook wordt gewerkt aan "*The Hybrid Educator*", een concept om IT-professionals aangesteld bij HSD-partners tevens in het onderwijsveld te laten werken. [xxxv]

Inmiddels heeft Dcypher een Nationale Cyber Security Educatie Agenda (NCSEA) [xxxvi] uitgegeven om met name het (hoger) onderwijs te verbeteren, maar die ook ideeën oppert om de jeugd meer bij het onderwerp te betrekken. Het agendeert dit onderwerp met voorstel voor een meerjarig actieplan; uitvoering van die agenda is afhankelijk van vele partijen; middelen zijn niet gegarandeerd. Overigens geeft de agenda een overzicht van hoger cybersecurity master en bachelor onderwijs en initiatieven in de provincie:[xxxvii]

- TU Delft:
    - *Computer Science Master Special Program Cybersecurity*
    - *Delft Blockchain Certificate*
    - *Cybersecurity specialization – Masters System Engineering, Policy and Management*
- Cybersecurity Academy van Universiteit Leiden, TU Delft en Haagse Hogeschool:
    - Universiteit Leiden, Delft en de Haagse Hogeschool bieden gezamenlijk de *Executive Master Cyber Security*
    - De Haagse Hogeschool onderwijst de *Master Cyber Security Engineering*
    - TU Delft biedt de online cursus: *Cyber Security for Executives: Taking the Lead!* [xxxviii]
- Hogeschool Leiden: Forensisch ICT – bachelor; een master is in de maak
- Haagse Hogeschool:
    - Information Security Management – bachelor
    - Cyber Security Technology – bachelor
    - Cyber Security Engineering – master (via CSA)
- Hogeschool Rotterdam: Technische informatica – bachelor voltijd
- *National Cyber Security Summer School* – brede opleiding voor academici
- *International Cyber Security Summer School* – een samenwerking tussen HSD, Universiteit Leiden, NATO/NCI Agency, Europol en Dutch Innovation Factory. [xxxix]
- *Challenge the Cyber – capture the flag* competitie voor middelbare scholieren
- LDE is in voorbereiding voor een universitaire minor 'cybersecurity', als keuzevak voor alle studenten.

Verschillende MBO-opleidingen in de regio hebben cybersecurity beroepsopleidingen in hun programma. De NCSEA besteed hier geen aandacht aan. Er is wel een overzicht van opleiding te vinden op de door HSD opgezette website securitytalent.nl [xl]. Ook zijn in de agenda verschillende commerciële opleidingen niet opgenomen zoals die van de Leidse Onderwijs Instelling, InHolland, FoxIT, Security Academy en meer.

Vanuit de **Human Capital Agenda Topsectoren** werkt Dutch Digital Delta aan ICT. Nederland loopt internationaal voorop in innovatie met ICT. Deze groei gaat gepaard met een grote behoefte aan personeel met de juiste ICT-vaardigheden. Het onderwijs kan deze vraag van de arbeidsmarkt moeilijk bijbenen. Zowel bij bedrijven in de ICT-sector als daarbuiten loopt het aantal vacatures op. De nationale Human Capital Agenda (HCA) is een actieplan om aan de groeiende vraag naar ICT-professionals te voldoen. Men heeft drie actielijnen ontwikkeld: regionale samenwerking stimuleren; scholieren inspireren en informeren en bevorderen kennisoverdracht nieuwe technologieën. De aandacht voor digitale veiligheid kan sterker worden aangezet. Cybersecurity-activiteiten worden niet expliciet genoemd, maar maken onderdeel uit van deze ambitie. DDD werkt samen met Dcypher bij de implementatie van de cybersecurityprogramma's zoals verwoord in de NCSEA.

Vanuit de **Human Capital Agenda Zuid-Holland**, als onderdeel van het Human Capital Akkoord van de Economic Board Zuid-Holland [xli] is initiatief genomen om de tekorten aan cybersecuritypersoneel te verminderen. Cybersecurity is één van de focussectoren binnen de HCA-ZH. Dit komt momenteel op twee manieren terug:

- Deelproject **Stimuleren Bewustwording Cybersecurity**. Kort gezegd houdt dit project in dat bedrijven/werknemers in de sectoren hightech maakindustrie, tuinbouw en Life Sciences & Health getraind gaan worden in de bewustwording rondom de risico's rondom cybersecurity en uiteraard ook hoe te handelen. Dit vindt plaats in nauwe samenwerking met The Hague Security Delta en haar partners. De *Cybersecurity Experience* is erop gericht om 3,000 werknemers en flexwerkers een ontwikkelperspectief te bieden en 50 werkgevers te ondersteunen. Dit is een initiatief van overheden (gemeente Den Haag, PZH en UWV), onderwijsinstellingen (Haagse Hogeschool, ROC Mondriaan, NCIO, TU Delft, IT Campus Rotterdam, iFlow (Rijk)[xlii], organisaties (TNO, Havenbedrijf Rotterdam) en het bedrijfsleven (Fox-IT Academy, Fujitsa, KPN, Manpower Group, Siemens).
- **Digitaal platform**. HSD host een digitaal platform (www.securitytalent.nl) voor inzicht in vraag en aanbod van cybersecurityspecialisten van verschillende competenties in de regio; tevens stimuleert HSD betere afstemming tussen de vraag en het aanbod. Samen met InnovationQuarter werkt men aan het aantrekkelijk maken en houden van de regio voor cyberspecialisten uit andere regio's of het buitenland.

Meer Publiek Private Samenwerking (PPS) in de regio. Er zijn verschillende PPS-initiatieven in de regio, in verschillende fase van volwassenheid. Zonder volledig te willen zijn, aandacht voor de volgende stimulerende projecten.

- **Dutch Innovation Factory (DIF)** van de Haagse Hogeschool in Zoetermeer: Door ICT-onderwijs, onderzoek en bedrijven te verbinden in één gebouw ontstaat een broedplaats vol interactie en samenwerking. DIF creëert een innovatieve plek waar kennisdeling plaatsvindt, innovaties ontstaan en co-creaties geboren worden. Cybersecurity is een belangrijk onderwerp bij deze vorm van onderwijs en onderzoek.

- **Cyberwerf Den Haag** [xliii]is een initiatief om een omgeving te creëren waar opleidingen praktijkgericht en samen met het MKB inhoud kunnen krijgen, ROC Mondriaan speelt hierbij een belangrijke rol.
- **Lentiz Onderwijsgroep**. Vanuit een bijzondere samenwerking tussen bedrijfsleven, de opleiding Horti Technics & Management van Lentiz, MBO Westland en overheid (PZH gesteund door InnovationQuarter) zet de kerngroep zich in voor digitale veiligheid in tuinbouw. Deze samenwerking ontstond een jaar geleden in World Horti Center, de plek waar de glastuinbouw bij elkaar komt. Na diverse succesvolle bijeenkomsten om de sector bewust te maken van digitale gevaren, maakt de kerngroep de volgende stap. Hierbij gaan studenten – de ondernemers en medewerkers van de toekomst – tijdens hun stage aan de slag met digitale veiligheid.[xliv]
- **Cyber P@CT** (Partners in @ction for Cyber Talent) van ROC Mondriaan is begin 2020 succesvol afgerond. Het is een Publiek Private Samenwerking (PPS) in de Haagse regio voor cybersecurity en heeft werk gemaakt van de groeiende toestroom van studenten cybersecurity. Ook heeft het binnen andere mbo-opleidingen meer aandacht gegeven aan de impact van cybersecurity op het werkveld in alle sectoren. De PPS werkte samen met de partners aan een leven lang leren en het onderwijs op een vernieuwende manier ontwikkelen en uitvoeren.

Kansen voor cybersecurity-onderwijs in Den Haag. Ter versterking van de IT & Security campus in Den Haag is een initiatief in gang gezet om IT en cybersecurity-onderwijs te verbeteren. Het oogmerk is om een digitale leeromgeving uit te bouwen naar een online en fysiek platform met als werktitel *Digital Competence and Education Center* (DCEC). Oogmerk is dat er naast HBO-studenten en MBO-studenten, professionals en werkzoekenden worden opgeleid. Het DCEC is open toegankelijk. Er is ruimte voor experiment, innovatieve leermethoden en hybride leren. Naast opleiding zijn er *train-de-trainer* programma's om voldoende docenten op te leiden, vindt matching van talent met bedrijfsleven plaats om talent voor de regio te behouden, wordt Den Haag als aantrekkelijke Tech-stad om te leren en te werken geprofileerd en kunnen bedrijven innovatieprojecten rond digitalisering laten uitvoeren. Hiermee wordt meegewerkt aan verschillende sporen van de regionale Human Capital Agenda van de EBZ.
Met het DCEC wordt specifiek ingespeeld op relevante maatschappelijke uitdagingen waar wij in de Haagse regio op dit moment voor staan.

- Vergroten beschikbaar IT- en cybersecuritytalent voor de regio: door omscholing en uitbreiding van onderwijsaanbod: door uitbouw van bestaande curriculum/kennis naar nieuwe opleidingsprogramma's voor studenten en niet-studenten. Zoals bijvoorbeeld, maar niet definitief of uitputtend, kortlopende cursussen, open access webinars, bootcamps en leer-werk-trajecten.
- Up-to-date houden van skills en kennis voor digitale technologieën (AI, blockchain, software-ontwikkeling en cybersecurity): de snel veranderende digitale wereld vraagt om continue bijscholing en in veel gevallen een gepersonaliseerd leertraject.
- Gebruik maken van online leermethoden om een groter bereik te realiseren. De Haagse Hogeschool ontwikkelt een online leermodule cybersecurity om via dit platform te ontsluiten. Dit is zeer relevant gezien COVID-19.
- Het behouden van talent voor de regio: door te zorgen voor online en offline matching tussen talent en bedrijfsleven, van stageplaatsen, studieprojecten tot vacatures, wordt geborgd dat talent voor de regio behouden wordt.

- Focus op specifieke aansluiting en aandacht voor doelgroepen die het lastig hebben: door samenwerking met o.a. UWV en SZW, de actieve promotie van DCEC via netwerken, social media (van gemeente en partners) en de betrokken onderwijsinstellingen.

DCEC is een initiatief van de Haagse Hogeschool, het ROC Mondriaan, The Hague Security Delta, The Hague Tech en Yes! Delft, en wordt gesteund door de Metropool Rotterdam-Den Haag en de Gemeente Den Haag.

Certificering onderwijs en competenties. De Rijksoverheid heeft het *European Competence Framework* overgenomen en op basis daarvan heeft Platform voor Informatiebeveiliging en het programma *Qualification of Information Security* beroepsprofielen en competentieniveaus voor informatiebeveiliging beschreven. [xlv] Dit vormt een basis voor het regulier onderwijs. De betekenis van commerciële opleidingen vormt wel een uitdaging. Omdat cybersecurity een relatief jong gebied is, is commerciële certificering en kwaliteitsborging van opleidingen weinig transparant. Voor elke (commerciële) cursus die een expert doet, komt er weer een afkorting (certificaat) achter zijn naam, waarvan de betekenis niet altijd even helder is. Voor Human Resources afdelingen die personeel werven is de certificeringsjungle onwerkbaar. Het Verenigd Koninkrijk kent een systeem van certificering van cybersecurity-onderwijs en commerciële trainingen en beschrijft heldere competenties daarvoor. Dit wordt uitgevoerd door het National Cybersecurity Center, NCSC-UK. Deze certificering verzekert een standaard van cybersecurity kennis, ook voor gecertificeerde commerciële opleidingen. [xlvi] . Nederland kent niet zo'n certificering voor commerciële opleidingen, en dat vormt voor het werven van competent personeel een uitdaging. Ook zijn er geen eenvoudige methoden beschikbaar om de feitelijke kennis- en vaardigheden van technische sollicitanten te toetsen.

Cybersecurity voor onderwijs. Niet alleen moet het onderwijs voldoende cybersecurityspecialisten opleveren, ook moet het onderwijs en onderzoek zelf cyberveilig zijn. Van studenten en onderzoeker wordt verwacht dat zij van buiten vaste infrastructuur van onderwijsinstellingen inloggen om te kunnen deelnemen aan het onderwijs. De hack bij de universiteit van Maastricht [xlvii], december vorig jaar, toonde aan dat de malafide toegang tot de netwerken van de universiteit liepen via accounts van studenten en onderzoekers. Studenten hebben niet de neiging hun computers zorgvuldig te *patchen* voor veiligheid; wifi-netwerken van studentenhuizen of campussen zijn vaak open. *Access managemen*t van systemen van onderwijsinstellingen zijn veelal niet van *two-factor-authentication* voorzien. Verschillende onderwijsinstellingen hebben Eduroam, een beveiligd wifi-netwerk voor onderzoek en onderwijs uitgerold binnen de muren van de instellingen, maar vaak niet op campussen of studentenhuizen.

Hoewel onderwijs- en onderzoeksinstellingen een complexe IT-architectuur hebben, is het niet de norm om de IT-systemen continue, 24/7 te monitoren. Zeker voor universiteiten die exogeen gefinancierd onderzoek doen en waardevol *Intellectual Property* (IP) ontwikkelen is dit een kwetsbaarheid. Bij de hack van de Universiteit Maastricht waren de cybercriminelen drie maanden illegaal in de netwerken bezig zonder dat dat door het IT-team was ontdekt; er was geen continue monitoring. Een interessante noot is dat de ICT-faculteit van de Technische Universiteit Eindhoven een *Security Operations Center* (SOC) functie voor netwerkmonitoring ontwikkelt, gerund door staf en studenten, met de universiteit als klant. Daarnaast wordt de dienst voor het regionale MKB ingezet. De kostprijs is laag; de universiteit krijgt goede onderzoeksdata over cyberrisico's bij het MKB. Ook het CyberWeerbaarheidscentrum Brainport voor de HiTech industrie speelt hierbij een rol. Een win-win.

Kortom: via studenten en onderzoekers is het voor ervaren cybercriminelen vaak relatief eenvoudig in de systemen van onderwijs- en onderzoeksinstellingen te komen, zeker wanneer dit goed gefinancierde criminele organisaties betreft. Dat is niet alleen een risico voor ransomware-aanvallen, maar ook voor diefstal van intellectueel eigendom. Naar verwachting zullen onderwijsinstellingen in Zuid-Holland gemiddeld niet veel beter zijn voorbereid dan het merendeel van de onderwijsinstellingen.

Medewerker als menselijk schild voor het netwerk. Vrijwel elke medewerker in een organisatie werkt met digitale middelen, een desk- of laptopcomputer, een smartphone of andere apparatuur. De mens is voor een aanvaller een zwakke schakel waar men zich op richt, bijvoorbeeld via *phishing attacks*. We maken die allemaal wel eens mee. Vaak is het een bericht waarop je moet klikken om iets wat je dierbaar is of nodig hebt te verkrijgen. Via die link kan de aanvaller een account overnemen, je camera of microfoon aanzetten, of via je account binnendringen in een complex netwerk. Aanvallers gebruiken in sommige gevallen een aanpak om heel veel mensen tegelijk aan te vallen, waarop er dan altijd wel iemand reageert. Wanneer men als doel heeft een specifieke organisatie binnen te dringen of bepaalde kennis te verwerven, kunnen het heel gerichte en geavanceerde aanvallen zijn. Vaak wordt een slachtoffer eerst geprofileerd via *social media* om hem in de val te lokken. Het meest waardevol zijn accounts van IT-administrators, omdat die veel op de netwerken mogen doen. Ook accounts van leidinggevenden zijn populair, vanwege het feit dat die vaak meer toegang hebben tot bepaalde waardevolle bestanden. Zeker nu we vanwege COVID-19 veel van huis werken worden deze kwetsbaarheden groter; immers, de IT-afdeling heeft geen of maar een beperkte mogelijkheid de verbinding en thuiscomputer in de gaten te houden.

Verschillende organisaties werken aan het verbeteren van de basiskennis van de medewerkers. Dat kan bij introprogramma's voor nieuwe medewerkers, via een regelmatig terugkerende online-cursus of test. Bij meer volwassen organisaties worden ook *phishing test* gedaan, waarbij werknemers onverwacht een gesimuleerde *phishing*-aanval op hun scherm krijgen. Sommige cursussen analyseren ook anoniem de competentie van groepen werknemers en kunnen helpen vaststellen in welke delen van het bedrijf bepaalde digitale risico's hoger zijn.

Inmiddels worden er veel van deze *human factor* cyberoplossingen door gespecialiseerde bedrijven geleverd, soms zijn generieke cursussen gratis online beschikbaar.[xlviii] Wil een werkgever een cursus op maat, en ook feedback krijgen over cyberrisico's die afhankelijk zijn van kennis of gedrag van medewerkers moet die worden ingekocht. De gemeente Den Haag heeft een tender lopen om een uitgebreid pakket aan maatregelen te implementeren voor de eigen organisatie. Verschillende organisaties in Zuid-Holland werken ook met dergelijke programma's, inbegrepen de Provincie.

Conclusie competentie beroepsbevolking.
Het risico van onvoldoende competente cyberexperts staat al geruime tijd op de agenda. Met de *Human Capital Agenda* ICT, de *Human Capital Agenda Security* van HSD en het *Human Capital* Akkoord van de Provincie bestaat een goed plan wat zijn tijd nodig heeft om tot volledige uitwerking te komen. Dit plan wordt zowel nationaal als regionaal ondersteund. Toch is er nog een aantal kwetsbaarheden die aandacht behoeven:

- Weinig commissarissen en directeuren van bedrijven en organisaties managen cybersecurity en digitaal risico als een integraal onderdeel van de bedrijfsvoering. Het belang wordt wel begrepen, zeker bij toenemende digitalisatie, maar staat niet hoog op de agenda van risico's waarop een gestructureerde aanpak wordt toegepast. Bij gereguleerde ondernemingen is er natuurlijk aandacht voor *compliance* van cybermaatregelen die men moet nemen.

Risicomanagement op basis van het vertalen van technische risico naar bedrijfsrisico en *value at risk* is voor velen nieuw. Bij managementopleidingen en -trainingen is het managen van cyberrisico voor generalisten nog zelden integraal opgenomen in het curriculum. Er is een mooie aanzet van de *Cyber Security Academy* op de HSD: *Cyber Security for Executives: Taking the Lead*. Ook zijn er commerciële trainingen beschikbaar.

- De *Human Capital Agenda Security* van HSD stimuleert en programmeert activiteiten om de tekorten aan cyberspecialisten aan te pakken. Hierbij wordt zowel gewerkt aan scholing in secundair en tertiair onderwijs als omscholing. Digitale techniek en veiligheid is nog niet een onderwerp wat structureel vanaf jonge leeftijd (tenminste middelbare school) aandacht krijgt; eigenlijk zou ook elke beroepsopleiding en universitaire studie een module digitale technologie en veiligheid moeten bevatten om basiskennis en vaardigheden in deze digitale wereld te versterken.
- De Nationale Cyber Security Educatie Agenda zich richt op universitair en hoger onderwijs en beschrijft beschikbare '*core*' cybersecurity-opleidingen; er is echter onvoldoende beeld van inbedding van digitalisering en cybersecurity in het onderwijs als geheel. Elke student komt immers terecht in een beroep dat veel digitalisering kent.
- Security.nl geeft een goed overzicht van '*core*' cybersecurity-opleiding in het Middelbaar Beroeps Onderwijs. Een aantal MBO-opleidingen brengt cybersecurity breder in bij andere opleidingen maar dit is geen gemeengoed.
- Beroepsprofielen voor informatiebeveiligingsspecialisten zijn goed beschreven, maar commerciële cybersecurity, opleiding en -trainingen kennen geen nationale standaard, hetgeen het werven van competent personeel bemoeilijkt.
- Er zijn in samenwerking met MRDH goede initiatieven in ontwikkeling, zoals DCEC met name gericht op HBO en MBO, ook gericht op omscholing. De campus IT en Security in Den Haag biedt goede mogelijkheden voor verdere uitbouw van praktisch cybersecurity-onderwijs.
- Het bedrijfsleven is betrokken bij verschillende onderwijsactiviteiten. ICT-specialisten van bedrijven parttime inzetten als docent ICT, stageplaatsen beschikbaar stellen en onderwijsproeftuinen bij bedrijven zijn win-win's waaraan altijd meer behoefte is.
- Structurele aandacht voor de kennis en gedrag van de medewerker om digitaal veilig te werken kan bij veel organisaties, zowel overheid als bedrijven, meer aandacht krijgen. Cyber awareness training voor elke computergebruiker is een *quick-win* die risico beperkt. Zeker nu velen online vanuit huis werken neemt dit belang toe.
- De cyberveiligheid van de onderwijsinstellingen vergt aandacht. Zeker voor onderwijsinstellingen die ook onderzoek doen, geldt dat continue netwerkmonitoring en goed toegangsmanagement met *multifactor authentication* (MFA) aan te bevelen is. Veilig internet op campussen en studentenhuisvesting is geen norm en een punt van zorg.

Wat kunnen we er verder aan doen?

- De HCA-ICT en HCA Security zijn goede initiatieven voor het stimuleren van opleidingen en omscholing om voldoende en competente cyberspecialisten te verkrijgen. Dit heeft zijn tijd nodig. Een heldere definiëring van vraag en aanbod is in gang gezet, maar nog niet voltooid Dit is nodig om het programma bij te kunnen sturen. Meerjarige ondersteuning van HCA is gepland; voor cybersecurity is extra aandacht door publieke en private partijen is noodzakelijk:
    - Aan de vraagkant is er regionaal een actueel overzicht van de meerjarige behoefte aan bepaalde cybersecurity experts nodig. HSD is hiermee gestart.
    - Aan de aanbodkant is er behoefte aan een samenhangend meerjarenplan voor gecertificeerd cybersecurityonderwijs in de regio voor het middelbaar en hoger

onderwijs voor cybersecurityspecialisten. Dit plan moet ook aandacht hebben voor middelbaar beroepsonderwijs.
    - In navolging van de UK stimuleert de overheid dat er via het NCSC een landelijke certificering van m.n. commercieel cybersecurityonderwijs komt.
- Initiatieven voor online-onderwijs, simulaties en trainingen om grotere groepen te bereiken verdient verdere ondersteuning. Hier liggen kansen voor de regio; initiatieven die bijvoorbeeld *Cyber Central* [xlix] ontwikkelt, maar ook voor startups in het IT en veiligheidscluster kunnen bijdragen aan dergelijke programma's.
- Om de cyber awareness en kennis van digitaal risicomanagement bij bestuurders een toezichthouders te vergroten, kan de overheid samen met het bedrijfsleven onder de vlag van EBZ een programma opzetten om zoveel mogelijk directies en toezichthouders, vooral ook van MKB te bereiken. Dit programma bevat online componenten, zoals basis IT-kennis voor managers, korte workshops waarin bedrijven en organisaties in dezelfde (digitale) keten dit onderwerp en de afhankelijkheid van elkaar in de keten bespreken; lessons learned seminars waarin eerdere hacks worden doorgenomen en bestuurders en toezichthouders de governance van technologie bespreken en korte simulaties om het handelen bij cyber incidenten en crises bespreekbaar te maken. Seminars en simulaties moeten zo dicht mogelijk bij de doelgroep staan en de specifieke uitdagingen van die sector behandelen.
- Gestimuleerd door EBZ, kan LDE worden gevraagd om met Cyber Security Academy en economische/bedrijfskundige faculteiten kennisontwikkeling en onderwijs van digitaal risicomanagement voor zowel bedrijven als overheden verder te ontwikkelen, zowel voor bachelor/master studenten als voor executives. De Haagse Hogeschool werkt hier reeds aan voor kleiner MKB.
- De overheid (provincie/grote steden) kan stimuleren dat cybersecurityonderwijs in ieder geval vanaf de middelbare school, wellicht eerder, een vaste plek krijgt in het onderwijsprogramma. Daarbij hoort ook veilig gebruik van social media en privacyvraagstukken. Dit geldt ook voor beroeps- en academisch onderwijs; immers elk beroep, of het nou arts is of tuinbouwer wordt steeds digitaler.
- Het is aan te bevelen dat in het landelijk systeem van competentie ontwikkeling aandacht komt voor certificering van commerciële cybersecurity-opleidingen. Tenminste zou er een handleiding moeten komen om het inzicht in commerciële certificaten te verbeteren.
- De overheid en het bedrijfsleven stimuleren dat het onderwijs niet slechts gebruik maakt van traditionele leeromgevingen, maar ook van onlineonderwijs en simulaties. Kennisontwikkeling wordt gestimuleerd met competities en andere stimulerende vormen als hack-de-overheid, wargames, certificaten. Het richt zich niet alleen op techniek, maar ook op recht, management en andere relevante aspecten.
- De EBZ stimuleert bedrijven en organisaties om een programma op te zetten om de cybersecurity awareness van werknemers te verbeteren. Dit kan met generieke online-trainingen beginnen, maar het is aan te bevelen om cursussen aan te passen aan de specifieke omstandigheden in een sector of bedrijf. Dit moet starten bij de meest kwetsbare groepen.
- Het bestuur van onderwijsinstellingen doet er goed aan regelmatig de eigen cyberveiligheid van de instelling te bespreken, zeker wanneer ook waardevol wetenschappelijk onderzoek wordt uitgevoerd. Universiteiten zijn uiterst complexe omgevingen die aandacht vergen.
- Een paar suggesties: Wellicht kan TU Delft of HHS in navolging van TU Eindhoven en Brainport een SOC-functie opzetten voor eigen veiligheid maar ook laagdrempelig ten behoeve van MKB. Bredere ontplooiing van EDUROAM op campussen en bij studentenhuisvesting stimuleert de onderwijs- en onderzoek omgeving en beperkt het cyberrisico.

INVESTERINGEN IN RESEARCH & DEVELOPMENT (R&D) en INNOVATIE

Nationaal

Nederland ziet R&D, innovatie en samenwerking in de '*triple helix*' tussen het bedrijfsleven, kennisinstituten en overheid als essentieel voor economische groei en een verbeterde concurrentiepositie. [I] Het kabinet investeert 200 miljoen euro per jaar in fundamenteel onderzoek. Daarnaast komt er in deze regeerperiode 200 miljoen euro per jaar extra beschikbaar voor toegepast onderzoek. Onderdeel daarvan is een extra investering bij grote technologische instituten die aantoonbaar aan marktbehoeften tegemoetkomen en publiek-private samenwerking bij universiteiten en hogescholen met focus op bèta en techniek. Het topsectorenbeleid, gericht op samenwerking van bedrijfsleven, kennisinstellingen en overheid zal sterker worden gefocust op de economische kansen die de volgende drie grote maatschappelijke thema's bieden: energietransitie/duurzaamheid; landbouw/water/voedsel; en quantum/hightech/nano/fotonica. Hoewel IT en cybersecurity niet direct worden genoemd zouden ze integraal deel uit moeten maken van deze initiatieven. De Topsector ICT heeft als oogmerk deze samenhang te borgen. De overheid belooft als *launching customer* innovatie beter aan te jagen door meer gebruik te maken van de *Small Business Innovation Research* regeling (SBIR), bijvoorbeeld vanuit Defensie en Rijkswaterstaat. Het MKB verdient een krachtiger rol in het innovatiebeleid. De MKB Innovatiestimulering Regio en Topsectoren (MIT) en de innovatiekredieten voor het MKB worden uitgebreid. Om de internationale barrières voor digitaal ondernemerschap weg te nemen zal het kabinet zich in Europa inzetten om te komen tot een Europese digitale markt.

Het kabinet heeft inmiddels ter stimulering van haar beleid InvestNL opgericht en Mld.€ 2,5 als startkapitaal. InvestNL financiert goede plannen van ondernemers om Nederland duurzamer en innovatiever te maken. InvestNL kijkt naar maatschappelijke transities en langetermijnsucces, en helpt financieren wat niet financierbaar lijkt via traditionele investeringsmethoden. InvestNL focust op energietransitie en versnelt de groei van innovatieve scale-ups. Binnen de energietransitie denkt men dat onze toegevoegde waarde het grootst is op het gebied van *Elektrificatie en energie*, *Circulariteit*, *Agrifood* en de *Gebouwde omgeving*. Als het gaat om innovatieve scale-ups gaat het vooral om -naast bovenstaande gebieden- *Industriële technologieën.* Bij al deze initiatieven zal digitalisering een belangrijke rol spelen, en inherent weerbare en veilige oplossingen. Hier liggen dus kansen voor innovatieve cybersecurity scale-ups met name in de Operationele Technologie.

Groeifonds. Ook in de meest recente begroting van de regering is R&D en innovatie aanjagen een belangrijke doelstelling, ook als mogelijkheid om de door COVID-19 aangetaste economie weer te stimuleren. In de begroting 2020-2021 [Ii] kondigt de regering aan dat de Minister van Economische Zaken komend jaar met plannen zal komen om het 'duurzame verdienvermogen op de lange termijn te versterken'. Er komt een Nationaal Groeifonds van 20 miljard euro: komende 5 jaar elk 4 miljard euro, beheerd door het Ministerie van Financiën. Dit Groeifonds is niet gericht op alle noden en wensen op *dit* moment, maar op de Nederlandse welvaart in de toekomst. Sommige van die plannen kunnen uit het investeringsfonds worden betaald; andere wellicht door financiering uit het bedrijfsleven. Er zullen strenge voorwaarden gelden: de investeringen moeten ten goede komen aan de economische groei van Nederland over 20-30 jaar. Kennisontwikkeling, R&D, innovatie en infrastructuur lijken terreinen die het meest kunnen bijdragen aan productiviteitsgroei. Ook hier liggen mogelijk kansen voor cybersecurity en de versterking van een weerbare digitale economie van Zuid-Holland.

National Cyber Security Research Agenda (NCSRA) III. Als nadere invulling van het regeringsbeleid, is in 2018 door het cybersecurity platform voor hoger onderwijs en onderzoek (Dcypher) NCSRA III [Iii]

ontwikkeld ter ondersteuning van de Nationale Cyber Security Agenda. Dcypher [liii] is in 2016 opgericht door de Ministeries van Justitie & Veiligheid, Onderwijs, Cultuur & Wetenschap, Economische Zaken en Klimaat en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO). Later is ook het Ministerie van Defensie aangesloten. Dcypher zorgt voor agendering en coördinatie van wetenschappelijk en praktijkgericht cybersecurity-onderzoek en hoger onderwijs. Dat wil zeggen dat onderzoeks- en onderwijsagenda's tot stand komen na brede raadpleging van het veld (kennisinstellingen, ondernemingen, overheden). De NCSRA III beschrijft de onderzoekuitdagingen voor cybersecurity en privacy rondom vijf pijlers. De pijlers zijn: ontwerp; verdediging; aanvallen; governance en privacy. De NCSRA III fungeert als een referentieraamwerk voor thematische cybersecurity R&D-programma's. Dcypher is opgericht voor 4 jaar en haar mandaat houdt eind 2020 op. Momenteel wordt gewerkt aan een opvolging van Dcypher.

Kennis en Innovatieagenda (KIA) Veiligheid. De Nederlandse overheid heeft in het kader van het nieuwe missiegedreven topsectoren- en innovatiebeleid nadruk gelegd op vier maatschappelijke thema's: landbouw, water en voedsel; gezondheid en zorg; energietransitie en duurzaamheid; en veiligheid. Vijfentwintig missies zijn opgesteld door vakdepartementen in consultaties met vele partijen en topsectoren en vervolgens goedgekeurd in april 2019 door het kabinet. De topsectoren hebben deze missies verder uitgewerkt in vier thematische Kennis en Innovatie Agenda's (KIA's), uitmondend in Meerjarige Missiegedreven Innovatie Programma's (MMIP's). Uitvoering van de MMIP's in de vele vormen van publiek-private samenwerking draagt bij aan het bereiken van de gestelde missie-doelen, leidt tot het benutten van economische kansen voor grote en kleinere bedrijven, zowel in binnen- maar vooral ook in buitenland. De topsectoren High Tech Systemen en Materialen, Team Dutch Digital Delta, Topsector Creatieve Industrie Topsector Logistiek en Topsector Water & Maritiem hebben gezamenlijk de KIA Veiligheid [liv] ontwikkeld; ook Defensie is betrokken.

Het thema Veiligheid is afgebakend tot *security*. Ook binnen deze beperking heeft het thema een grote reikwijdte; uiteenlopend van het verdedigen tegen dreigingen van buiten, het voorkomen van georganiseerde criminaliteit, het beschermen van kritieke infrastructuren tot veiligheid op straat. Hiervoor is het nodig gebruik te maken van de nieuwste wetenschappelijke inzichten, (sleutel)technologieën en toepassingen met aandacht voor ethische en maatschappelijke aspecten. Daarbij zullen vaak combinaties nodig zijn van meerdere kennisgebieden, zowel technologisch, sociaal-maatschappelijk als organisatorisch.

De KAI beschrijft acht missies, waarvan cyberveiligheid er een is. De missie kent vijf deelprogramma's: bestrijden cybercrime; bevorderen ontwikkeling cybercompetenties; defensieve cybertechnologie; offensieve cybertechnologie (gerelateerd aan overheid); ketenweerbaarheid en governance. De deelprogramma's zijn uitgewerkt in focusgebieden. Deelprogramma defensieve cybertechnologie gaat vooral over het automatiseren van het veilig houden van systemen, zoals kwetsbaarheden simuleren, pentesten, *patchen* of automatiseren van operationele taken. Essentieel onderdeel binnen het deelprogramma cybersecurity is onderzoek naar de interactie tussen de mens en geautomatiseerde security tools, onder andere het kunnen blijven doorgronden van geautomatiseerde technieken en het optimaal in kunnen zetten van AI-technologie voor cyberveiligheid van organisaties. Inmiddels is in samenwerking met de provincie, de metropool regio Rotterdam-Den Haag, TNO, HSD en een aantal cybersecuritybedrijven een consortium opgestart om inhoud te geven aan dit thema.

Naast *artificial intelligence* zijn kennisvragen en innovatieve oplossingen voor *post-quantum computing* en cybersecurity van belang. Encryptie en *post-quantum* cryptografie zijn essentieel voor veilige

communicatie, en daarmee een fundament onder digitale weerbaarheid. Gesignaleerde kennisvragen en innovatieopgaven zijn de robuustheid van crypto-algoritmen in *post-quantum* tijdperk: *post-quantum* encryptie en *post-quantum* communicatiemethoden.

Versterken cybersecurity-innovatieketen en verbeteren valorisatie van onderzoek. De ambitie van Nederland om leidend te zijn bij cybersecurity vereist dat er een goede transfer ontstaat van cybersecurity kennis en onderzoek naar productontwikkeling en economische bedrijvigheid: valorisatie van cybersecuritytechnologie. Zuid-Holland en met name Den Haag heeft daar veel belang bij en heeft mede daarom ook geïnvesteerd in het IT en Security Cluster met als kern The Hague Security Delta.

Recent heeft de Minister van Economische Zaken en Klimaat de resultaten van een verkenning en vervolgaanpak cybersecurity kennisontwikkeling en innovatie met de Tweede Kamer gedeeld. [lv] De Minister herkent knelpunten in de R&D en innovatieketen, met name ook het gebrek aan succesvolle valorisatie van onderzoek in Nederlandse producten en kondigt een vervolgaanpak aan. De basis voor de gezamenlijke vervolgaanpak zal bestaan uit een nieuw **cybersecurity samenwerkingsplatform** dat de krachten op het terrein van onderzoek, innovatie en onderwijs moet bundelen. Binnen dit samenwerkingsplatform komen alle relevante partijen, expertise, instrumenten en middelen uit het cybersecuritydomein bij elkaar. Het platform zal zich richten op het bij elkaar brengen van kennisvragen en -aanbod. Ook zal het platform informatie over (financierings- en innovatie-) instrumenten beschikbaar stellen aan kennisinstellingen, het bedrijfsleven en medeoverheden. Hierbij valt te denken aan instrumenten zoals thematische calls uit de Nationale Wetenschapsagenda, toeslagen uit het missiegedreven topsectoren- en innovatiebeleid, *Small Business Innovation Research* (SBIR) en instrumenten uit Europese onderzoeksprogramma's als *Horizon Europe* en *Digital Europe*.

Een van de onderzoeken waarop het Ministerie zich baseert is een TNO-studie naar het versterken van de innovatieketen op het terrein van cybersecurity. [lvi] Het onderzoek stelt vast dat de belangrijkste *driver* voor innovatie de grote en toenemende vraag naar cybersecurityoplossingen is vanwege de steeds verder gaande digitalisering en cyberonveiligheid. Men onderkent echter een aantal barrières om de innovatie effectief te laten zijn. Zo is er een gebrek aan visie en sturing in de innovatieketen; publieke uitgaven aan cybersecurityonderzoek blijft achter bij andere Europese landen; complexiteit van instrumenten voor onderzoek en innovatie is een issue, vooral voor MKB-bedrijven en startups; er is een beperkt absorptievermogen bij bedrijven en overheden om nieuwe innovatieve producten te implementeren er is een gebrek aan goed opgeleide mensen. Het onderzoek beveelt aan om samenhang te creëren door thematisch aan de slag te gaan; om continuïteit in het instrumentarium te brengen (geen calls voor subsidies, maar een open loket); dat de overheid meer als *launching customer* moet optreden; en om MKB- en startups eerder en vaker bij innovatiestimulering te betrekken. Overigens pleit TNO er ook voor dat de overheid haar rol in het cyberveilig maken van de Nederlandse samenleving moet heroverwegen, in navolging van een advies van het *World Economic Forum*. De aanbeveling is om cybersecurity te beschouwen als een 'publiek goed'.

Cybersecurity samenwerkingsplatform. Hoewel de besluitvorming niet is afgerond, zijn de contouren van het nieuwe samenwerkingsplatform voor cybersecurity -opvolging van Dcypher- wel bekend. Het platform heeft het oogmerk om bij te dragen aan een veiliger, slimmer, digitaal autonoom en economische sterker Nederland. Het moet één loket worden voor vraag, aanbod en financiering voor cybersecurity-onderwijs, -onderzoek, -innovatie en toepassing. Nederland moet voldoende goed opgeleide cybersecurity mensen hebben, wil internationaal leidende expertise genereren en deze toepassen in Nederlandse producten. Daarbij kiest men in navolging van het TNO-onderzoek voor een

thematische aanpak waarbij per thema strategie wordt omgezet in praktische programma's en projecten die meerjarig worden gefinancierd. Het platform werkt met partners, publiek en privaat, die elk actief in programma's participeren en investeren. Het ligt voor de hand dat het Ministerie van EZK de kosten van het platform draagt. De kosten van programmering verlopen niet via het platform, maar het platform helpt met verschillende partijen, publiek en privaat financiering rondom thema en programma's rond te krijgen. Het platform zal een bureau krijgen en soepel de voortgang van Dcypher verzekeren, maar dan met een ander accent. Het is nog onduidelijk waar het bureau en het platform wordt ondergebracht en welke thema's gekozen zullen worden. De kans is groot dat het platformbureau in Den Haag wordt gehuisvest. Ook dit biedt weer kansen om actief te participeren in kennisopbouw, innovatie en bedrijvigheid in de regio rondom cybersecurity te vergroten.

Regionaal: Roadmap Next Economy
Al in 2016 heeft de Metropoolregio Rotterdam en Den Haag (MRDH), samen met de Ministers van Economische en Binnenlandse Zaken en de provincie Zuid-Holland een strategie ingezet om een voortrekker te worden in het bouwen van een slim, digitaal Europa. Daartoe heeft ze zich laten inspireren door een gerenommeerd Amerikaans adviesbureau, die de *Roadmap Next Economy* [lvii] heeft ontwikkeld. Het advies beveelt aan sterk in te zetten op het digitale *internet of things* (IoT) en een '*smart*' regio te worden. Het rapport geeft adviezen over een breed scala van digitale innovaties, zoals het ontwikkelen van een digitale toegangspoort tot Europa, de *smart energy* delta, circulaire economie, een regio met innoverend ondernemerschap alles gericht op een moderne innovatieve samenleving, die een economische *boost* aan de regio gaat geven.

De Economic Board Zuid-Holland (EBZ) stimuleert de implementatie van de *Roadmap Next Economy*. De Board bestaat uit ondernemers en bestuurders van bedrijven, kennisinstellingen en overheden in Zuid-Holland. De EBZ brengt partijen bij elkaar en maakt het verschil met netwerkkracht, denkkracht en lobbykracht. Ze organiseert task forces (TF) voor strategische thema's zoals *Human Capital* en transitiethema's uit de *Roadmap Next Economy*. De doelen van de roadmap zijn vertaald in de volgende transitiepaden: *Smart Digital Delta*; *Smart Energy Delta*; *Circular Economy* en *Next Education*. De *TF Digital Economy* is verantwoordelijk voor het transitiepad *Smart Digital Delta*.

De TF Digitale Economie. Digitalisering heeft verstrekkende gevolgen voor de regionale economie. De veranderingen in het digitale domein volgen elkaar snel op. Digitalisering tornt bovendien vaak aan het fundament van het verdienmodel en de bedrijfsvoering, levert natuurlijk kansen, maar ook bedreigingen op. De TF heeft de ambitie een adequaat antwoord hierop te hebben, zodat regionale clusters of sectoren van bedrijven een sterke competitieve positie vinden en behouden. Er moet een betrouwbaar digitaal vestigingsklimaat komen, dat naadloos is verbonden met een veilige *open-access* infrastructuur waar wordt samengewerkt aan innovatie van technologie en de toepassing daarvan. De valorisatie van innovatie moet zoveel mogelijk in de regio plaatsvinden. De TF werkt langs vier strategische sporen: connectiviteit, innovatie corridor, de mens centraal en cyberveiligheid. Uitgangspunt is dat er een sterke digitale infrastructuur komt, dat innovatie-initiatieven en proeftuinen in samenhang en gebruik makend van een sterk digitaal netwerk nieuwe oplossingen bedenken en implementeren voor de economische sectoren; dat deze *secure* en *resilient* zijn *by-design*; dat *privacy* wordt gewaarborgd en dat de mens waarop de economie draait centraal staat.

Digitaliseringsinnovaties. De regio kent talloze innovatie-initiatieven om Zuid-Hollands digitaliseringsstrategie om te zetten in praktische actie. Er zijn onderzoekslaboratoria, accelerators, field- en living labs om gezamenlijk innovatie-initiatieven met onderzoekers, MKB en startups,

onderwijs, gemeenten en burgers te ontwikkelen. In vrijwel alle gevallen wordt innovatie versterkt door toepassing van digitale technologie of van het benutten en toegankelijk maken van grote hoeveelheden gegevens.
Zonder compleet te willen zijn een overzicht van initiatieven (op alfabetische volgorde):

- **5G fieldlabs Zuid-Holland (Delft, Den Haag, Katwijk, Holland-Rijnland)** zijn een open platform gericht op het ontwikkelen en gebruiken van 5G en toepassingen. In Delft is het gecolloceerd met *The Green Village* op de TU Delft Campus. Het is een samenwerkingsverband met Living Lab Scheveningen, gemeente Katwijk, *Unmanned Valley* en de regio Holland-Rijnland. Ook is er een 5G Field Lab op het T-Mobile hoofdkantoor in Den Haag en bij The Hague Tech.
- **BioPartner Incubator @Leiden BioScience Park** is een programma in oprichting waarbij startups in life science en biotech worden geholpen bij de ontwikkeling van innovatieve oplossingen. Data science en Artificial Intelligence spelen daarbij een steeds grotere rol.
- **BlueCity (Rotterdam)** is een faciliteit die zich richt op experimenten voor een afval loze circulaire economie en samenleving: bouwen aan een wereld waarin er geen afval bestaat.
- **Defensie Cyber Innovation Hub (Den Haag)** is een accelerator in oprichting gericht op digitale transformaties in het hoog risico en hoog beveiligde domein. De accelerator zal initieel vooral voor defensie zelf werken maar kan uitgroeien tot een centrum voor cyberinnovaties voor overheden, vitale infrastructuur en diensten en bijdragen aan een kennistransfer naar andere economische sectoren. De nabijheid van NATO, Europol, TNO, veiligheidsdiensten en het defensie cybercommando helpt innovaties ook met startups te stimuleren.
- **Digital Factory for Composites (Den Haag)** is een faciliteit die cross-sectorale innovatie ondersteunt op het gebied van *digital manufacturing* and composietmaterialen.
- **Do IoT field lab – TU Delft** is een *one-stop-shop* waar bedrijven, gemeenten en andere publieke en private organisaties kunnen komen met vragen over onderzoek en innovatie voor mobiele communicatie en IoT. Het heeft een fysieke locatie waar experimenten kunnen worden uitgevoerd.
- **Dutch Optics Centre (DOC)(Delft)** is een initiatief van TNO en TU Delft om Nederlandse industrie te helpen groot te worden op het gebied van *optics* en *optomechatronics*. Zo helpt DOC met het valideren van concepten, maken van prototypes en kleinschalige productie op te schalen.
- **Duurzaamheidsfabriek (Dordrecht)** is een plek waar bedrijven, van klein tot groot, hun innovaties op het gebied van duurzame technologie, met als focus de maritieme maaksector en de energiesector.
- **Living Lab Scheveningen (Den Haag)** is een initiatief van de gemeente Den Haag om samen met bewoners, bezoekers en ondernemingen te experimenteren om nieuwe technologie en digitale uitvindingen uit te proberen in de stedelijke omgeving.
- **RoboHouse (Delft)** is een *smart industry field lab* waar innovatieve organisaties en mensen de mogelijkheden van cognitive robotics kunnen ontdekken, hun eigen applicaties kunnen ontwikkelen of ze kunnen testen in een industriële omgeving.
- **RAMLAB (Rotterdam)** missie is om te helpen met het adopteren van de *Additive Manufacturing* (een vorm van digitaal printen) om ervoor te zorgen dat industriële reserveonderdelen altijd en overal beschikbaar zijn.
- **RDM Campus (Rotterdam)** is een campus waar MBO en HBO-techniekonderwijs samenkomen om met bedrijven aan echte innovatieve projecten te werken.
- **Reyeroord (Rotterdam)** is een wijk waar de gemeente samen met de Veldacademie een living lab heeft opgezet om de wijk leefbaarder en duurzamer te maken. Het betreft fysieke (bijv. energietransitie) en sociale (bijv. armoede vermindering) aspecten.

- **SAM-XL (Delft).** *Smart Advanced Manufacturing* is een onderzoekscentrum op de Campus van TU Delft. Men ontwikkelt, demonstreert en beperkt risico's voor *smart manufacturing* oplossingen, met name gericht op de sector klein volume en grote variatie. De focus ligt op het geautomatiseerde productieproces van grote, lichtgewicht structuren, bijvoorbeeld voor luchtvaart, scheepvaart en windenergie.
- **SMITZH** helpt ondernemers bij het toepassen van smart manufacturing. Dit kan zijn slimme technologie implementeren of maaktechnologie ontwikkelen of testen. Maar ook bij netwerken of de juiste mensen vinden.
- **Station Delft Campus** wordt opgezet als living lab voor innovaties op gebied van mobiliteit en duurzaamheid; doel is te komen tot het stationsgebied voor de toekomst.
- **The Green Village (Delft)** verschaft een omgeving waarin universiteiten en bedrijven innovaties die bijdragen aan een sustainable toekomst kunnen ontwikkelen, testen en demonstreren.
- **The Hague Tech** is een innovatiegemeenschap die een veelheid van uiteenlopende tech startups huisvest, en vormt onderdeel van het Haagse IT en veiligheidscluster.
- **Unmanned Valley (Katwijk aan Zee)** is een field lab voor sensor gerelateerde technologieën en toepassingen. Men werkt met name aan innovaties op het gebied van onbemande technologie, autonome systemen en sensoren. Het voormalig vliegveld Valkenburg en een corridor naar zee maakt het mogelijk met drones en onbemande vliegtuigen te experimenteren.
- **World Horti Center (Naaldwijk)** is een kennis en innovatiecentrum voor de internationale glastuinbouwsector. Het onderzoekscentrum met 38 kasafdelingen werkt aan techniek, toelevering, sierteelt en voedingstuinbouw.
- **QuTech (Delft)** is een internationaal in hoog aanzien staand onderzoekscentrum voor Quantum Computing en Quantum Internet, in 2014 opgericht door TU Delft en TNO. Hier wordt gewerkt aan het internet van de toekomst, wanneer *quantum* technologie met extreem veel rekenkracht beschikbaar komt.
- **Yes! Delft (Delft) en Yes! Delft digital hub (Den Haag)** zijn accelerators die helpen goede ideeën en teams te vormen als startup en ze verder helpen te laten groeien tot succesvolle bedrijven. Yes! Delft koppelt startups aan potentiele klanten om samen door innovatie praktische problemen op te lossen. Yes! Delft *digital hub* richt zich met name op toepassingen in Artificial Intelligence en cybersecurity en is in het Haagse cybercluster gehuisvest. Yes! Delft Den Haag is in het proces om GovTECH op te zetten gericht op digitalisering van de overheid.

Secure-by-design, resilient-by-design & privacy-by-design. Aan innovatie-initiatieven geen gebrek. Hoe de initiatieven samenhangen en in welke mate ze daadwerkelijk succes gaan opleveren is onduidelijk. Door praktische digitale transformatie zal de Zuid-Hollandse economie en maatschappij wezenlijk veranderen en effectiever, efficiënter en wellicht leefbaarder maken. Er is echter ook een andere kant: een *quick scan* door de missies en opdrachten van deze initiatieven laat zien dat ze veiligheid, weerbaarheid en privacy van deze nieuwe innovaties niet of nauwelijks duiden. Veel van deze oplossingen zullen nieuwe risico's met zich meebrengen, nieuwe mogelijkheden om systemen lam te leggen, te spioneren of geld te stelen. Verschillende initiatiefnemers beamen de noodzaak veilig te zijn wel, maar vinden praktische uitvoering hiervan lastig. Dit is niet vreemd in de innovatieve tech wereld. Ontwikkelaars richten zich in eerste instantie op functionaliteit, niet op veiligheid of privacy. Vaak is er onvoldoende aandacht voor niet-functionele vereisten, zoals veiligheid. De discussie rondom de Corona-app is een voorbeeld. De initiële poging snel een app te bouwen ging mis omdat privacy en dataveiligheid niet geborgd kon worden. Daarna is de aanpak veranderd waarbij dit wel van begin af aan is meegenomen. *Secure-by-design, resilient-by-design* en borging van privacy zijn bij het merendeel van de bovengenoemde innovatie-initiatieven geen voorwaarde of opdracht, hopelijk een *after-thought*.

Maar dan is het vaak al te laat. Het zou goed zijn die initiatieven meer te verbinden met de kennis aanwezig in het cybercluster rondom HSD.

The Hague Security Delta (HSD). HSD [lviii] is een stichting die als doel heeft de samenwerking te bevorderen tussen bedrijven, overheden en kennisinstituten op het gebied van kennisontwikkeling en innovatie voor veiligheid, waarbij cybersecurity een hoofdrol speelt. HSD maakt deel uit van het internationale netwerk van cybersecurity clusters, *Global Epic*. Het kent zo'n 60 premium partners en ruim 140 netwerkpartners. HSD runt met de gemeente Den Haag de HSD Campus als ontmoetingsplaats voor entrepreneurs, studenten en professionals die werken in veiligheid. Het vormt de thuisbasis voor de Cyber Security Academy, een samenwerkingsverband tussen de universiteiten van Leiden, Delft en de Haagse Hogeschool. Ook is het de thuisbasis van HSD-office en zijn er verschillende cybersecuritybedrijven gehuisvest.

HSD Campus benoemt zich als het innovatiecentrum voor veiligheid en helpt haar partners met toegang tot kapitaal, talent, kennis, de markt en innovatie.

- Toegang tot kapitaal: HSD organiseert evenementen voor investeerders en innovators en verzorgt documentatie.
- Toegang tot talent: HSD heeft een *Human Capital Agenda*, helpt met het organiseren van de Internationale *Cybersecurity Summer School* en host een website voor talent in veiligheid.
- Toegang tot de markt: HSD organiseert (inter)nationale matchmaking evenementen; heeft een adviesteam voor MKB en helpt (met IQ) mee met soft landing voor buitenlandse ondernemingen en handelsmissies.
- Toegang tot innovatie: HSD heeft een model voor innovatie in veiligheid en helpt innovatieprogramma's en projecten op te zetten.

De huidige strategie is mede gebaseerd op een rapport van Policy Research Corporation (PRC) uit 2016 [lix] en een update van 2017 [lx]. De aanbevelingen van dat rapport zijn tot op heden deels uitgevoerd. Met name vraagarticulatie en *launching customer*schap blijft een uitdaging, met name voor de overheid (vaak als gevolg van aanbestedingspraktijken). Aanbevelingen PRC:

- Focus op vraagcreatie bij overheid en bedrijfsleven:
    - Formuleer waarde proposities vanuit het perspectief van de vraag; overweeg hierbij herindeling van de HSD-deelsectoren.
    - Organiseer '*launching customer*'-schap vanuit de overheid via een nieuwe, gedeelde innovatieagenda.
    - Wees als clusterorganisatie en gemeente de katalysator voor groei en plaats organisaties meer op de voorgrond: '*powered by HSD*'.
- HSD en de bedrijven in het cluster zijn een Nederlands exportproduct en het cluster is een aantrekkelijke vestigingsplaats voor buitenlandse organisaties:
    - Het vestigingsbeleid moet een 'open karakter' hebben; trek hierbij samen op met o.a. het Ministerie van EZ.
    - Richt acquisitieactiviteiten vooral op hoogwaardige werkgelegenheid (hoofdkantoren en R&D-activiteiten).
    - Blijf inzetten op '*enablers*' voor groei zoals een open onderwijs- en onderzoeksysteem en voldoende financiële ondersteuning (publieke R&D uitgaven).
- Excelleer in de regio en binnen het landelijk cluster:

- Benut de omvang en stootkracht van het veiligheidscluster in Den Haag ten gunste van de groei van het nationale cluster: regionale focus en beproeving gevolgd door opschaling op nationaal en internationaal niveau via Den Haag.
- Focus op sterkten van regionale innovatieregio's en werk samen op domeinen waar sprake is van overlap.
- Werk nationaal samen aan vraagarticulatie in het publieke domein.

HSD zal in 2020 een nieuwe meerjarenstrategie opstellen met als doel in te spelen op nieuwe ontwikkelingen en continuïteit te verzekeren. Het ligt in de verwachting dat de nieuwe strategie naast het vervolmaken van een aantal aspecten uit het Policy Report advies een aantal nieuwe aspecten zal bevatten:

- **Positionering** ten opzichte van het nieuwe **cybersecurity samenwerkingsplatform** voor onderwijs, onderzoek en toepassing.
- **Cross-sectorale aanpak voor de regio:** stimuleren van samenwerking binnen de sectoren Holland Instrumentation, Greenport Westland, maritiem/haven, biotech/medical en aerospace/space en vooral ook tussen die sectoren.
- **Bijdragen aan valorisatie**. Cybersecurity innovaties moeten dichter bij de economische sectoren en bedrijven komen te staan: dus cyber voor glastuinbouw; cyber voor biotech, etc. Innovaties worden gestimuleerd door living labs waarbij een paar grotere bedrijven in een sector helpen innovatie te trekken waardoor de massa aan MKB mee kan liften.
- **Cybertestbed, m.n. voor OT**. HSD wil meer aandacht geven aan cyberveilige Operationele Technologie. Om startups te helpen innoveren en een plek te bieden aan bedrijven die innovaties uit willen proberen, is een OT-testbed nodig waarbij HSD een rol wil spelen. Dit past in de gedachte dichterbij en voor sectoren te gaan innoveren. Er is al een begin van zo'n testbed: het simulatiemodel voor de botlektunnel, gebouwd door de Haagse Hogeschool voor Siemens.

Daarnaast ziet HSD sterke voordelen in colocatie van twee initiatieven ter versterking van het cluster:

- **CyberWeerbaarheidscentrum (Zuid-Holland)**; er is een globaal plan voor een CyberWeerbaarheidscentrum vergelijkbaar met Brainport. Onderzocht moet worden of financiering (publiek en/of privaat) van een cross-sectoraal regionaal centrum haalbaar is en of er behoefte is aan een dergelijk centrum. HSD geeft aan dat het een dergelijk centrum kan onderbrengen, maar de expertise ontbeert om dit te leiden of uit te voeren. Dat zou moeten liggen bij technische experts. Later in deze analyse komen we op dit onderwerp terug.
- **Cybersecurity samenwerkingsplatform**. Het ligt voor de hand dat de nieuwe organisatie van het Ministerie van Economische Zaken en Klimaat op of nabij de campus HSD wordt ondergebracht ter versterking van het ecosysteem; immers veel cybersecurity partijen zijn daar al aanwezig hetgeen coördinatie vergemakkelijkt. Waar dit platform wordt ondergebracht is tot op heden niet bekend.

InnovationQuarter (IQ). De kerntaak van IQ [lxi] is het duurzaam versterken van de economische structuur en het ontsluiten van het innovatieve vermogen van de regio Zuid-Holland. IQ houdt zich bezig met innoveren, investeren en internationaliseren in de regio Rotterdam – Den Haag, maar ook verder in de provincie. IQ is een onderneming met publieke aandeelhouders, gericht op het versterken van de economie en werkgelegenheid in Zuid-Holland. IQ is een neutrale speler in de regio en heeft geen winstoogmerk. IQ wordt ondersteund door de provincie, gemeenten Den Haag en Rotterdam en enige andere partijen.

IQ participeert in het cybersecurity cluster door partijen bij elkaar te brengen, samenwerking te promoten en kennis in te brengen. IQ constateert dat de markt voor cybersecurity voor Informatie Technologie vrijwel verzadigd is, ook omdat veel diensten worden uitbesteed naar de Cloud. Focus moet meer liggen op OT, *Industry 4.0* en *IoT*, maar ook verder op het gebruik van AI, *blockchain* of *quantum* technologie in cybersecurity. IQ richt zich op het verbeteren van cyberweerbaarheid van verschillende sectoren in de regio: maritiem/haven; life science/health; maakindustrie/aerospace (o.a. via Holland Instrumentation); glastuinbouw en energie. Kenmerkend is dat in veel van die sectoren maar beperkt cybersecuritykennis aanwezig is, terwijl er met waardevol IP gewerkt wordt en de bedrijfstakken digitaal kwetsbaar zijn.

Het ligt voor de hand cyberweerbaarheid en innovatie per sector als programma te promoten. Aangezien veel activiteit in handen is van het MKB, zouden enige grotere bedrijven dit initiatief moeten trekken met uitstraling op de keten. IQ is een samenwerkingsinitiatief begonnen met ondernemingen in de maakindustrie en Greenport. Het is lastig gebleken subsidie van DTC te krijgen; subsidie voor een CyberWeerbaarheidscentrum Glastuinbouw en Hightech maakindustrie is eerder afgewezen. DTC kan slechts subsidies voor een aantal projecten per jaar toekennen. Voor de maakindustrie is wel een basaal centrum met IQ opgericht dat door DTC wordt ondersteund, maar continuïteit is in gevaar.

Daarnaast **investeert** IQ actief in het (innoverende) bedrijfsleven met een **drietal fondsen**. *Uniiq*, samen met universiteiten, early stage proof of concept fonds; *Energiiq*, gericht op energiemarkt en *IQ-Capital*, fonds voor startups, scaleups en volwassen MKB in Zuid-Holland. Met name Uniiq (M€22) en IQ-Capital (M€80) zijn relevant voor cybersecurity. IQ-Capital betreft converteerbare leningen met minderheidsbelang van 50k€ tot 5M€. IQ is met HSD mede-initiatiefnemer van het Dutch Security TechFund van TIIN Capital. Cybersecurity is een groeimarkt waar de regio Zuid-Holland een sterke positie heeft, zowel nationaal als internationaal. Nederland is gebaat bij een sterk cybercluster en voldoende kapitaal is daarbij belangrijk. Met de investering in the Dutch Security TechFund wil IQ Nederland nog veiliger maken.[lxii]

IQ's rol bij **internationaliseren** wordt in het deel 'Diplomatie en handel' besproken.

IQ heeft een **sectorplan Cybersecurity** opgesteld, gericht op de komende jaren. Dit is nog geen geformaliseerd plan van aanpak. Het baseert zich op de SWOT-analyse Nederlandse cybersecuritysector van Verdonck, Klooster en Associates van 2016 en onderzoeken van o.a. Policy Research van 2017 over banengroei in het cybersecuritycluster. Het sectorplan benadrukt het complementaire karakter van HSD en IQ. Het beschrijft trends en marktkansen voor cybersecurity:

- Focus op ontwikkeling groeidomeinen zoals sleuteltechnologie blockchain, IA en quantum.
- Versterken cyberawareness en weerbaarheid in verschillende belangrijke sectoren zoals haven (FERM), Hightech/maak industrie of Greenport.
- Versterken internationale concurrentiekracht, o.a. door handelsbevordering.
- Vergroten beschikbaarheid (durf)kapitaal, ook via buitenlandse investeerders
- Verder vergroten beschikbaarheid van goed gekwalificeerde cyberspecialisten, o.a. door om- en bijscholing en het aantrekken van buitenlands talent.

Een sterk cybersecurity cluster als motor voor innovatie. De Gemeente Den Haag zet zich al geruime tijd in op de economische kansen die cybersecurity voor de regio biedt; de Provincie Zuid-Holland heeft

zich daarbij aangesloten. Dat was een van de redenen om HSD op te richten en ook IQ een rol te geven in het stimuleren van cyberbedrijvigheid. Het cybercluster is natuurlijk niet HSD alleen en de bedrijven die op HSD Campus gehuisvest zijn. HSD is wel een belangrijke motor van het cluster. Daarnaast dragen er veel organisaties bij aan cyberinnovaties in dit cluster, zoals Yes! Delft, The Hague Tech, binnenkort de Defensie *Cyber Innovation Hub* (in oprichting), naast natuurlijk alle publieke en private partijen zoals overheden en overheidsorganisaties, de universiteiten en hogescholen, onderzoeksinstellingen en een groot aantal bedrijven, zowel potentiële klanten voor cybersecurity als leveranciers.
Het cluster is internationaal bekend en effectief, maar natuurlijk bestaat de ambitie om verder te groeien.

De vraag is gerechtvaardigd wat de voorwaarden zijn voor groei en een goed en effectief cybercluster. Er is een aantal topclusters die wereldwijd in hoog aanzien staan. Bekende clusters zijn Be'er Sheva (CyberSpark) (Israël), Melbourne (Australia), Singapore, Tallinn (Estonia) en Maryland, USA (rondom NSA). Ook Engeland (rondom GCHQ/London), Duitsland (München/Berlijn) en Frankrijk (Bretagne) zijn effectief cyberinnovatie clusters aan het ontwikkelen. Een aantal zaken valt op:

- In vrijwel al deze gevallen bestaat er een **hechte samenwerking met defensie en de veiligheidsdiensten** als motor voor cybersecurity innovaties. Dit is logisch, omdat die organisaties sowieso meer aandacht besteden aan cybersecurity vanwege de hoge beveiligingsnormen van haar digitale systemen, maar vaak ook aan offensieve capaciteiten werken.
- Landen met een **hoge dreiging** zijn effectief en ontwikkelen snel. Israël en Estland voelen dagelijks de hete adem en dreiging in hun nek. Cyberveiligheid is een vanzelfsprekend nationaal belang; daarbij dempt de dagelijkse dreiging de neiging tot bureaucratiseren van overheidsprocessen.

Daarnaast is er een tiental succesfactoren voor de ontwikkeling van het cybercluster, die ook door HSD worden nagestreefd:

- **Beleid**: prioriteit geven aan een integrale benadering van veiligheid.
- **Internationaliseren**: altijd over de grenzen heen werken vanuit kennisontwikkeling en marktperspectief.
- **Samenwerking**: organiseren van een stabiele basis om (cyber)security te stimuleren.
- **Kennisinstituten**: samenbrengen als motor van opleiding en onderzoek.
- **Innovatie en R&D**: zorg voor projecten met een hoog profiel.
- **Entrepreneurs**: trek leidende bedrijven aan en help deze te ontwikkelen.
- **Kapitaal en investeringen**: draag zorg voor een ontwikkelfonds en trek *Venture Capital* aan.
- **Kwalitatieve leefomgeving**: help om aantrekkelijk wonen en ondernemen mogelijk te maken.
- **Human Capital**: trek goede mensen aan en leid deze op.
- **Infrastructuur**: zorg voor een goede infrastructurele omgeving als factor voor succes

Het cybercluster rondom HSD heeft op al deze vlakken successen behaald, maar harde cijfers ontbreken. Wellicht blijft het aantrekken van voldoende kapitaal en investeringen achter blijft. Dit heeft waarschijnlijk te maken met de valorisatieproblematiek. *Venture Capital* investeerders zijn pas werkelijk geïnteresseerd als er daadwerkelijk marktperspectief is, ook internationaal, voor een cybersecurityproduct. Voorts lukt het nog niet goed om grote internationale IT-integratie bedrijven zich in de regio te laten vestigen en mee te laten investeren; kennelijk kan je bij dit cluster nog onvoldoende kennis en innovaties ophalen. *Human capital* blijft een issue vanwege de grote vraag aan cybersecurityspecialisten, met name technisch personeel.

HSD en IQ spelen als motor een belangrijke rol om alle partijen in het cybercluster samen te laten werken. Het is niet altijd helder wie daarbij welke taken vervult. De nabijheid van Defensie, Europol, NATO en andere internationale organisaties kan beter worden uitgebuit, zeker als dat naar buitenlands voorbeeld een belangrijke *driver* is voor succes.

Wat betekent dit voor de regio?
R&D en innovatie vormen een kernpunt van het regeringsbeleid om op langere termijn de groei in Nederland aan te jagen. Ook wordt er nationaal geïnvesteerd in cybersecurity R&D en innovatie, onder meer om minder afhankelijk te zijn van buitenlandse oplossingen. Er zal meer thematisch gewerkt worden om focus aan te brengen op onderzoek en innovaties. Er is daarbij meer aandacht voor valorisatie en het ontwikkelen van bedrijvigheid. Naar alle waarschijnlijkheid zal het nieuwe cybersecurity samenwerkingsplatform in de regio worden gevestigd. Dit zijn kansen voor de regio, zowel voor opleidings- en onderzoekscentra als voor cybersecuritybedrijven. Maar ook voor de Zuid-Hollandse economie die digitaal weerbaarder moet worden.

Zuid-Holland en de metropool Rotterdam-Den Haag hebben voluit ingezet op digitalisering. Er zijn in de regio talloze digitaliseringinitiatieven gaande: living labs, proeftuinen om zo goed mogelijk gebruik te kunnen maken van digitalisering, *IA, robotics, 5G, IoT, quantum* en meer. Er is te weinig aandacht om deze initiatieven vanaf het ontwerp veilig en weerbaar te maken waarbij borging van privacy een voorwaarde is.

De regio heeft al een levendig cybersecurity cluster en veel randvoorwaarden voor succesvol innoveren zijn reeds ingevuld. Er is financiële stimulering van innovaties, hoewel het voor startups lastig is om de juiste ingang tot fondsen te vinden; IQ helpt cybersecurity bedrijven en startups ook financieel; IQ heeft een sterk netwerk met de bedrijven in de regio en kan duiden waar cyberweerbaarheid een uitdaging is. HSD heeft een uitstekend nationaal netwerk en staat internationaal op de kaart, er zijn tal van andere initiatieven om cybersecuritybedrijvigheid te stimuleren. Toch is er nog wel wat te verbeteren.

Cybersecurity innovaties die ontwikkeld zijn in de regio bereiken maar mondjesmaat regionale overheden en bedrijven. Er is meer focus nodig vanuit het cybercluster rondom HSD om de veiligheid en weerbaarheid van de economische sectoren te helpen verbeteren. Cyberveiligheid moet niet moeilijk zijn, maar gewoon en automatisch. Een tuinbouwer moet zich kunnen focussen op tomaten, niet op security-updates. Dichterbij sectoren als de haven, maritiem, energie, glastuinbouw, hightech maakindustrie en *air&space* betekent ook dat meer aandacht nodig is voor innovaties voor veilige en weerbare operationele technologie. Overigens kunnen de sectoren zichzelf ook beter organiseren als behoeftesteller van innovaties zodat focus aangebracht kan worden op knelpunten en rondom die behoeftes coalities kunnen worden gebouwd om te experimenteren met veilige en weerbare oplossingen.

Overheden zouden meer hun rol als *launching customer* moeten nemen. Inkoopprocessen en te gedetailleerde beschrijving van behoeften zitten dat vaak in de weg. Startups hebben niet de middelen en energie om veel te investeren in aanbestedingen en de trage procedures van de overheid. Inkoopprocessen moeten moderniseren om innovatief werken beter mogelijk te maken zodat de regionale overheid slimme lokale producten kan verwerven.

Het cybersecuritycluster moet zich organiseren om met één mond te gaan spreken richting het nieuwe nationale cybersecurity samenwerkingsplatform om de belangen van de provincie te borgen. Verder kan het cluster zich verder optimaliseren door de relatie met defensie, NATO en de veiligheidsdiensten te versterken. Overigens moeten die organisaties ook meer gebruik gaan maken van de energie en kennis van jonge onderzoekers en startups; voor hen geldt ook dat inkoopprocessen moeten moderniseren. Er zijn in het buitenland voorbeelden hoe dit kan. [lxiii] De kennistransfer van de cybersecurity voor hoog beveiligde systemen naar andere economische sectoren biedt kansen.

Het cybercluster heeft een sterke hand nodig om partijen bijeen te brengen om economische kansen te verzilveren. HSD en IQ vervullen beide een deel van deze rol, maar er is overlap en onduidelijkheid met name over de rol in innovatie, niet over investeren en internationaliseren. Samenhang en focus is in alle initiatieven crux om beter bij te dragen aan veilige en weerbare regionale economie.

Kansen voor de regio

Cybersecurity R&D en innovatie biedt veel kansen voor de regio en gaat hand in hand met de ambitie van de *Roadmap Next Economy*. De nieuwe focus en investeringen vanuit het Rijk kunnen een nieuwe impuls geven aan het IT en veiligheidscluster in de regio, maar ook de Zuid-Hollandse economie helpen weerbaarder te maken. Een aantal actielijnen kan worden ingezet:

- Er is een commitment van de rijksoverheid om meer en gefocust te investeren in cybersecurity R&D en innovaties via een thematische aanpak. De regio moet analyseren welke thema's voor de economie het belangrijkst zijn en actief lobbyen om deze als thema voor de nationale aanpak te kiezen. De thema's moeten de belangrijke sectoren in de regio helpen. Naast automatiseren van IT-security/SOC, is ook cyberveiligheid van OT, (*post-quantum*) cryptologie en veilig IoT relevant voor de regionale industrie, tuinbouw en overheid.
- HSD en IQ zijn een goede motor voor de regionale cyberinnovaties en bedrijvigheid. Het is gewenst dat slechts één organisatie verantwoordelijk is voor het toezichthouden op regionale cybersecurity R&D- en innovatie-initiatieven en tevens dient als een contact voor regionale nationale en internationale samenwerking. Beide organisaties en hun boards moeten de governance van het cluster helderder maken; beide organisaties zijn voorwaardenscheppend en moeten andere organisaties en initiatieven helpen meetbaar effect te realiseren.
- Er moet ook één organisatie in de regio zijn die zich richt op het meten van en rapporteren over de mate van succes van valorisatie van technologie innovatie (dus van research naar product of dienstverlening) met de focus op oplossingen die veiligheid en weerbaarheid van de digitale omgeving verbeteren. Meetbaar effect is kijken naar nieuw ontwikkelde cyberproducten die door bedrijven of de overheid gekocht worden; niet hoeveel startups we helpen. Immers, de meest innovaties (en startups) sneuvelen voor die eindstreep.
- HSD is goed gepositioneerd om een centrale hub te worden voor cybersecurityinnovatie, maar moet dan ook dichter bij de economische sectoren gaan staan en tevens beter gebruik maken van het bedrijfsnetwerk van IQ.
- De collaboratie met nieuwe cybersecurity samenwerkingsplatform is vitaal. HSD kan de *primus inter pares* zijn voor de regio.
- Een organisatie moet de *lead* moeten krijgen om de in de provincie/regio aanwezige cyber innovation hubs en start-/scale-ups te ondersteunen bij het vinden van financiële middelen (*grants*, subsidies, investeringsgeld) voor de innovatie in Europa, in Nederland en bij het bedrijfsleven, in samenwerking met het nieuwe cybersecurity samenwerkingsplatform. Het succes moet meetbaar en transparant zijn. IQ financiert zelf innovatieve bedrijven en heeft een goed netwerk; vraag is of er dan sprake zou zijn van belangenverstrengeling.

- Hechtere samenwerking met defensie/veiligheidsdiensten en deze samenwerking beter integreren in het cybercluster in de regio gaat beide partijen helpen; kennistransfer van de hoog beveiligde digitale systemen naar de economie versterkt de effectiviteit van het cluster.
- Ook de economisch sectoren zouden kunnen helpen door één aanspreekpunt voor innovatie te organiseren: een *linking pin* naar de cybersecurity accelerators en startups zodat die de cyberuitdagingen van de sector beter te begrijpen. Deze innovatiemanagers helpen met het delen van kennis over de sector en helpen bij het opzetten van *Proofs of Concept*, in een field lab of een living lab bij een bedrijf of een keten van bedrijven. Voor startups die tegen een markt gereed product aanzitten, is dit een van de moeilijkste fasen om tot de markt door te dringen. De vraag is of deze *linking pin* in de sector zelf moet zitten of in de *business development teams* van IQ.
- Digitaliseringsinitiatieven moeten worden gestimuleerd om *secure-by-design, resilient-by-design* oplossingen te ontwikkelen en *privacy-by-design* te borgen. Dit zou een voorwaarde moeten zijn bij overheidssubsidies.
- De regionale overheid moet haar inkoopprocessen vereenvoudigen, zodat startups makkelijker kunnen deelnemen; de inkoopprocessen vragen minder om een specifieke in detail beschreven oplossing, maar eerder om een probleem of kwetsbaarheid weg te nemen. Inkoop-innovatie moet ook aandacht krijgen van de rijksoverheid als belangrijke partij bij het verwerven van cybersecurity-oplossingen. Alleen dan kan de overheid haar taak als *launching customer* naar behoren uitvoeren.
- Om te kunnen sturen moet innovatiesucces meetbaar worden gemaakt. Een organisatie zou dat namens de regio moeten volgen en aan de EBZ/TF Digital Economy rapporteren; Als HSD de primus inter pares is, dan zozu het voor de hand liggen (*checks and balances*) dat IQ die rol op zich neemt:
    - Bewijs van de inspanning van (regionale) overheden om cyber security R&D te ondersteunen, te stimuleren, en te onderhouden. Daarbij is vooral van belang dat overheden zelf in belangrijke mate de ontwikkelde oplossingen implementeren in hun operationele omgevingen (*launching customer*).
    - Bewijs van commerciële inspanning (bijv. cyber innovation hubs; living labs) om R&D te ondersteunen, te stimuleren, en te onderhouden. Daarbij is vooral van belang dat bedrijven zelf in belangrijke mate de ontwikkelde oplossingen implementeren in hun operationele omgevingen (*launching customer*).
    - Bewijs van succesvolle valorisatie van R&D en toepassing in de regio.
    - Bewijs dat daadwerkelijk de cyberbedrijvigheid in de regio is gegroeid; dit volgen als onderdeel van het Bruto Regionaal Product.
- Tot slot: het kabinet zoekt naar innovatieve initiatieven voor het groeifonds, initiatieven die een lange termijn en duurzaam effect hebben op de economie. Onder leiding van de EBZ zou een *brainstorm* kunnen plaatsvinden om voor de regio kansrijke initiatieven te bedenken die digitalisering in de regio veilig en weerbaar maken en houden, zodat daardoor de economie duurzaam kan groeien. De gewetensvraag daarbij is of de noodzakelijke innovatie en weerbaarheid er met alleen marktwerking gaat komen. Of moet de overheid een forse impuls geven om de markt te verleiden samen een oplossing te vinden voor een duurzame toekomst?

DIPLOMATIE EN HANDEL

Diplomatie

De regering ziet cybersecurity als een belangrijk onderdeel van buitenlandse politiek; ze is een actief deelnemer aan diplomatieke onderhandelingen om de waarden en normen van het gebruik van het internet te beïnvloeden. Het Ministerie van Buitenlandse Zaken heeft een goede cyberexpertise opgebouwd en is betrokken bij tal van internationale discussies over cybersecurity, cybercrime detectie en veroordeling, samenwerking tussen CSIRTs en bescherming van kritieke informatie infrastructuren, *confidence building measures*, *cyber capacity building*, *internet governance*, digitaal recht en internationale normen voor verantwoordelijk gedrag van staten in het cyber domein. Nederland is vanaf haar eerste strategie heel actief op het internationale toneel, inbegrepen samenwerking met de Verenigde Naties, Raad van Europa, NATO, de Europese Unie, de Organisatie voor Economische Samenwerking en Ontwikkeling en vele anderen. Daarnaast wordt cyber besproken met de *International Telecommunication Union* (ITU), het *Internet Governance Forum* (IGF) en het World Economic Forum. In 2015 werd in Den Haag de 4de *Global Conference on Cyberspace* (GCCS) gehouden, een platform voor regeringen, intergouvernementele organisaties, academia en de *tech community* om *best practices* en kennis voor cyber capacity building uit te wisselen. De GCCS conferentie leidde tot de oprichting van het *Global Forum on Cyber Expertise* (GFCE), waarvan inmiddels meer dan 115 leden en partners vanuit de hele wereld bij zijn aangesloten. Het GFCE, waarvan het uitvoeringsbureau in Den Haag is gevestigd, richt zich op wereldwijde *cyber capacity building*. Ook leidde de GCCS tot de oprichting van de *Global Commission on Stability of Cyberspace* (GCSC) met als doel om een continue internationale dialoog over beleid en normen in het digitale domein te organiseren.

Nederland is ook het *The Hague Process* gestart, een serie van bijeenkomsten tussen meer dan 50 landen en de ontwikkelaars van het Tallinn Manual 2.0 over de toepassing van internationaal recht in het cyber domein. Daarnaast is Nederland samen met Estland het *Cyber Norms Platform* gestart om tot gezamenlijke inbreng te komen voor de UN-groep van overheidsexperts over de toepassing van internationaal recht in het cyber domein.

Gemeente Den Haag streeft ernaar, samen met de regering, niet alleen de stad voor internationaal recht en veiligheid te zijn, maar zich ook te ontwikkelen als een internationaal centrum voor cyberdiplomatie, teneinde samen met internationale experts, beleidsmakers, diplomaten, militair personeel en NGO's het vreedzaam gebruik van het cyberdomein te bevorderen. Dit initiatief heeft ook positieve uitwerking op de lokale economie, omdat meer organisaties zich om deze reden in Den Haag vestigen, of hun organisatie hier versterken.

Nederland investeert structureel M€ 5 in cyberdiplomatie en heeft op de belangrijkste ambassades cyberdiplomaten gepositioneerd. Daarnaast is er een team van specialisten om de 140 diplomatieke posten bij te staan met cyberkwesties. [lxiv]

Handelsbevordering

Het Min BuZa heeft recent een digitale agenda voor buitenlandse handel en ontwikkelingssamenwerking opgesteld. [lxv] Het beleid zet zich in voor digitalisering voor ontwikkeling van achtergebleven landen; noodzakelijke aanpassingen in het handelssysteem, Nederland positioneren als digitale koploper en het stimuleren van veiligheid en vrijheid op het internet. Het oogmerk is om conflicten en instabiliteit te voorkomen, armoede en maatschappelijke ongelijkheid te verminderen, duurzame inclusieve groei en

klimaatactie wereldwijd te bevorderen en het internationaal verdienvermogen van Nederland te versterken.

In het kader het bevorderen van deze agenda, en met name internationale handel prioriteert Nederland samenwerking met een aantal partnerlanden.

- **Duitsland**: samenwerking in hoogtechnologische markten aan energietransitie, elektromobiliteit, cybersecurity en sleutel technologieën.
- **Verenigde Staten**: Silicon Valley is een belangrijke bestemming voor Nederlandse startups en scale-ups, als partner voor innovatie. Samenwerking is verder gericht op *smart&green mobility* en innovatie in de zorg; en Nederland werkt op diverse terreinen samen met de VS als cybersecuritypartner.
- **India**: Hier ligt de focus op digitalisering van de gezondheidszorg, *affordable medical devices* en *digital health& diagnostics* en *eHealth*. *Secure-by-design* digitale gezondheidszorg is zeker voor India zeer relevant. Samenwerking van het cybercluster met de biotech- en life-science sector ligt voor de hand.
- **Japan**: er is een samenwerking op het gebied van cybersecurity, onder meer ter ondersteuning van kritieke infrastructuur ten behoeve van de Olympische Spelen.
- **Singapore**: recent is een *government-to-government* werkgroep opgestart voor samenwerking over kennisintensieve producten en diensten onder meer op het terrein van digitalisering.

Het kabinet werkt samen met TechLeap, voorheen Startup Delta [lxvi] aan een sterkere positionering van Nederlandse startups en scaleups in het buitenland, met de nadruk op tech-ondernemers. Via de zes prioritaire start-up hubs (priohubs) Berlijn, Parijs, Londen, Singapore, Boston/New York City en San Francisco/Los Angeles worden startende bedrijven uit de topsectoren HTSM en ICT geholpen zich beter te positioneren. Deelgebieden zijn kunstmatige intelligentie, *blockchain*, robotica, fintech en *cybersecurity*.

InnovationQuarter heeft een belangrijke rol bij internationalisering van bedrijvigheid rondom cybersecurity. IQ helpt bij handelsbevordering van Nederlandse bedrijven in het buitenland, met nadruk op Noord-Amerika, Duitsland, Scandinavië, India, Japan en Taiwan. Dit is van belang omdat de cybermarkt voor bedrijven in Nederland te klein is voor serieuze groei. Er is een globaliseringsprogramma (Globaliser) met ongeveer acht actieve bedrijven; er wordt gewerkt aan het door RVO gesubsidieerde programma Partners for International Business (PIB) en het netwerk Trade & Innovate. IQ heeft twee Partners for International Business (PIB) consortia mee opgezet, voor Duitsland en voor de VS. Afstemming vindt plaats met HSD, Rijksdienst voor Ondernemend Nederland (RVO) en het postennetwerk van Buitenlandse Zaken. Met HSD is een meerjarenroute uitgestippeld om draagvlak bij de Rijksoverheid te creëren en het thema cyber te agenderen.

IQ brengt tevens de internationalisering van het MKB in kaart. Ook worden handelsmissies georganiseerd, o.a. Naar USA (RSA-San Francisco en Maryland) en Duitsland. Ook is er een digitaal matchmaking evenement met Canada georganiseerd. Het programma voor Duitsland is vanwege COVID-19 vertraagd in uitvoering, maar is ambitieus en zal deels digitaal doorgang vinden. Ook zijn er activiteiten met Scandinavië, India, Japan en Taiwan.

Nederland is ook actief betrokken om bedrijven binnen haar grenzen te halen, samen te werken met buitenlandse ondernemingen of diensten uit te besteden om zo economische toegevoegde waarde te genereren. Voor Den Haag is de economische ontwikkeling op het gebied van veiligheid en cybersecurity

een topprioriteit waarbij innovatie in een open setting als belangrijk wordt gezien. Het is helder dat daardoor niet elk bedrijf naar het IT en veiligheidscluster gehaald kan worden. Er wordt gewerkt aan strategisch vestigingsbeleid waarbij een afweging gemaakt wordt tussen (nationale) veiligheidsbelangen en economische belangen.

Voor bedrijven die zich in Nederland willen vestigen zijn het *Netherlands Foreign Investment Agency* (NFIA) en de Rijksdienst voor Ondernemend Nederland de eerstaangewezen partijen. IQ speelt voor de een belangrijke rol voor cybersecurity. Bij twijfel kan NFIA verder achtergrondonderzoek laten doen. Bij bedrijven in de vitale sectoren zijn afhankelijk van de sectorspecifieke regels van toepassing waar een bedrijf aan moet voldoen. Voor cybersecurity-ondernemingen is niet altijd goed vast te stellen welke criteria moeten worden gehanteerd; dat vergt overleg tussen verschillende partijen. Zo kan een bedrijf dat werkzaam is in oplossingen voor een hoger beveiligingsniveau, impact hebben op andere bedrijven die in hetzelfde gebouw zijn gevestigd. Dat kan leiden tot hogere beveiligingskosten voor iedereen en vergt overleg.

Als het gaat om vestiging van buitenlandse cybersecurity-ondernemingen in het Haagse IT en Veiligheidscluster, zijn IQ, gemeente Den Haag en HSD vrijwel altijd actief betrokken. Er is goed operationeel overleg tussen deze partijen, NFIA, RVO, het Ministerie van Economische Zaken en Klimaat en andere betrokken ministeries om vestigingsafspraken met die partijen te maken.

Wat betekent dit voor de regio?
Cyber diplomatie is een nationale verantwoordelijkheid. De stad Den Haag heeft slim ingespeeld op de actualiteit van cyberdiplomatie door Den Haag naast staf van internationaal recht en veiligheid ook te positioneren als internationaal centrum voor cyberdiplomatie. Dit is een gezamenlijke inzet van het Rijk en de gemeente en legt geen windeieren. Er is groei van internationale organisaties in Den Haag, ook op dit onderwerp. Ook de faculteit Cyber Governance van de Universiteit Leiden in Den Haag draagt effectief bij aan het internationale debat. Dit trekt weer internationale studenten en faculteitsstaf aan.

Internationale handelsbevordering is een nationale verantwoordelijkheid, maar steeds meer spelen de regio's een belangrijke rol. Nationaal zijn zowel het Ministerie van Buitenlandse Zaken als het Ministerie van Economische Zaken en Klimaat betrokken. IQ en HSD, daarvoor medegefinancierd door de provincie en de gemeente Den Haag, stimuleren cyberbedrijvigheid in de regio internationaal via een goede samenwerking met het diplomatiek netwerk van het Ministerie van Buitenlandse zaken, met internationale netwerken van maatschappelijke organisaties, publiek en privaat, universiteiten, onderzoeksinstellingen en andere overheden. Zowel HSD als IQ participeren in nationale beleidsontwikkeling en uitvoering, onder meer door deelname aan internationale handelsmissies en startups en scale-ups te stimuleren hun producten in nieuwe markten te positioneren.

Daarnaast gebruikt de provincie/regio het internationale netwerk om zich te promoten als voorbeeld voor regionale digitale transformatie en tegelijkertijd als een digitaal weerbare regio, met als doel buitenlandse bedrijven en personeel met hoogwaardige technische kennis aan te trekken.
IQ heeft al verschillende buitenlandse bedrijven een goede landingsplaats in het cybercluster bezorgd. De Provincie en de grote steden zijn actief om de aantrekkelijkheid van de provincie/regio als vestigingsplaats te promoten voor bedrijven die de economie en werkgelegenheid kunnen versterken binnen de randvoorwaarden van het economisch beleid (o.a. duurzaamheid) en (nationale) veiligheid. Hierbij benadrukt ze de sterke digitale infrastructuur en cyberweerbaarheid van de provincie/regio.

Is verbetering mogelijk?
Er gebeurt al veel voor cyberdiplomatie, handelsbevordering van cybersecurity technologie en vestiging van internationale cyberbedrijven. Wellicht kunnen HSD en IQ afstemmen om het volgende te organiseren:

- De nationale diplomatie verder verstrengelen met handelsbevordering, door bijvoorbeeld de cyber-ambassadeur vaker met ondernemers op pad te laten gaan naar het buitenland.
- Versterken van een one-stop-shop voor de promotie export van cybersecurity technologie, vraagbaak voor MKB-bedrijven, met eenvoudige toegang vanuit de regio. IQ heeft deze rol op zich genomen als onderdeel van *Trade & Invest NL*, gesteund door HSD als kennispartner.
- Een overzicht maken en actueel houden van alle relevante beschikbare nationale en internationale relevante contacten en wie verantwoordelijk is voor de relatie.
- Het articuleren van wat de doelstelling is voor de samenwerking met deze relaties en sturing geven aan het bereiken van die doelstellingen.

CRISIS BEHEERSING

Nederland en zeker ook de provincie Zuid-Holland drijft op digitale systemen. Die digitalisering brengt ons veel economisch voordeel, maar het maakt onze fysieke wereld ook kwetsbaar: een klein incident kan al grote gevolgen hebben op het maatschappelijk leven. Denk aan een KPN-storing met impact op 112, de ransomware aanval op de Universiteit Maastricht, of de Citrix-problematiek, die niet alleen het Medisch Centrum Leeuwarden hermetisch afsloot, maar ook de Rijksoverheid tot verregaande maatregelen dwong. In deze regio herinneren we ons zeker de NotPetya aanval op de APM-terminals in de haven van Rotterdam in 2017, die zowel binnen het bedrijf, maar ook daarbuiten verregaande gevolgen had.

De Wetenschappelijke Raad voor het Regeringsbeleid is kritisch over de voorbereiding op digitale ontwrichting.[lxvii] Ze stelt vast dat digitale incidenten vaak het hart van de samenleving raken en dat Nederland onvoldoende is voorbereid. Digitale ontwrichting ontstaat door de verwevenheid van de digitale wereld met de fysieke en sociale wereld. Digitale incidenten tasten zichtbaar de belangrijkste maatschappelijke processen aan. Dergelijke verstoringen leiden vaak tot grote maatschappelijke schade. WRR geeft adviezen om kwetsbaarheden aan te pakken als het gaat om paraatheid, terugvalopties, meer crisisoefeningen om processen en procedures te testen, versterken en verdichten netwerk voor signalering, verkleinen afhankelijkheden met buitenlandse dienstverleners en goede belegging van verantwoordelijkheden, zowel publiek als privaat.

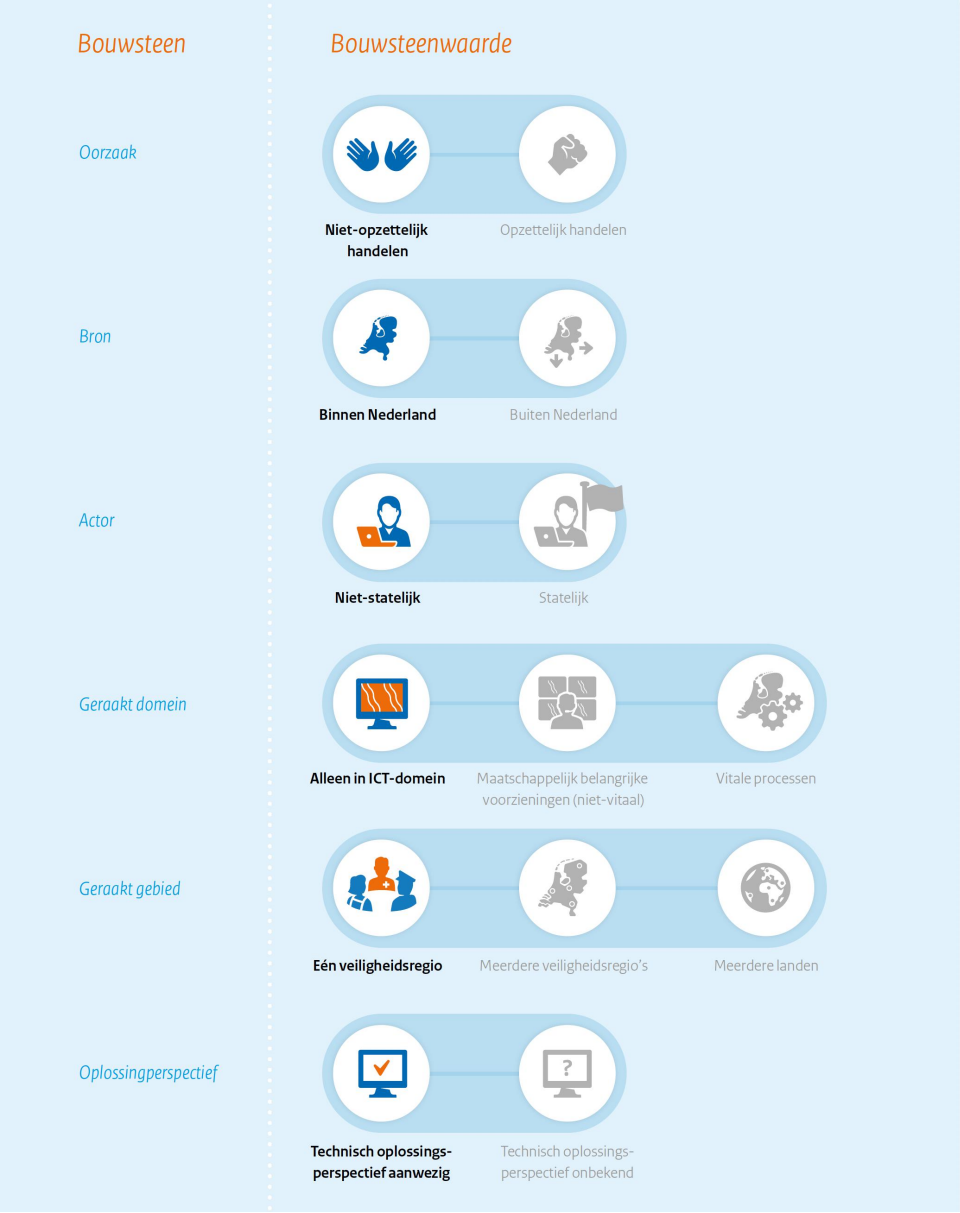
Nationaal Crisisplan Digitaal. Recent is het 'nationaal crisisplan digitaal' [lxviii] van de Nationaal Coördinator Terrorismebestrijding en Veiligheid uitgekomen. Dit crisisplan is van toepassing op de digitale ruimte: "Het conglomeraat van ICT-middelen en -diensten dat alle entiteiten die digitaal verbonden kunnen zijn bevat permanente, tijdelijke en plaatselijke verbindingen en gegevens die zich in dit domein bevinden (o.a. data, programmacode, informatie), waarbij geen geografische beperkingen zijn gesteld".

Conform de Wet beveiliging netwerken en informatiesystemen (Wbni) is een incident "elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen". Daarbij gaat het om beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van netwerk- en informatiesystemen. Het crisisplan digitaal richt zich op de beheersing van incidenten met aanzienlijke maatschappelijke gevolgen. Hieraan kunnen de volgende typen incidenten/dreigingen ten grondslag liggen:

- **Verstoring/sabotage**: het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of –diensten.
- I**nformatiemanipulatie**: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
- **Informatiediefstal**: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- **Spionage**: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
- **Systeemmanipulatie**: aantasting van informatiesystemen of –diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of –diensten. Deze worden daarna ingezet om andere aanvallen uit te voeren.
- **Storing/uitval**: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.

- **Datalek**: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

Het plan beschrijft soorten incidenten en crises die ook allemaal in de Provincie Zuid-Holland kunnen voorkomen**:**



En de processtappen en actoren in de digitale en generieke crisisstructuur.

Belangrijkste actoren per processtap

Processtap	Betrokken actor
Incidentanalyse (oordeelsvorming, duiding)	Digitale dienstverleners getroffen partijen
	NCSC
	CSIRT DSP
	AIVD
	MIVD
	ICT Response Board
	ISAC's
	Ministerie van Buitenlande Zaken
	NCTV
	Internationale netwerken
Attributie en opsporing	Digitale dienstverleners getroffen partijen
	Politie
	KMAR
	AIVD
	MIVD
	Openbaar Ministerie
	Ministerie van Buitenlandse Zaken
	Internationale netwerken
Bestrijding oorzaak	Digitale dienstverleners getroffen partijen
	Politie
	Sectorale CERT's
	NCSC
	Internationale netwerken
Gevolgbestrijding	Digitale dienstverleners getroffen partijen
	Getroffen partijen
	Veiligheidsregio's
Besluitvorming	Aanbieders vitale processen
	Aanbieders getroffen voorzieningen
	Burgemeester
	Voorzitter veiligheidsregio
	Vakminister
	Ministeriële Commissie Crisisbeheersing

Processtap	Betrokken actor
Informatie-voorziening	Digitale dienstverleners getroffen partijen
	NCSC
	NCC, LOCC
	Internationale netwerken
	Sectorale CERT's
	OKTT's
Notificatie slachtoffers	Digitale dienstverleners getroffen partijen
	Politie
	NCSC
	Sectorale CERT's
	OKTT's
Cyberdiplomatie	Ministerie van Buitenlandse Zaken
Evt. offensieve reactie	Ministerie van Algemene Zaken
	Ministerie van Buitenlandse Zaken
	Ministerie van Defensie
	Ministerie van Justitie en Veiligheid
	AIVD
	MIVD
Communicatie	Digitale dienstverleners
	Getroffen partijen
	CSIRT DSP
	NCSC
	Hulpverleningsdiensten
	Burgemeester
	Voorzitter veiligheidsregio
	Vakminister
	Openbaar Ministerie
	NCTV/Nationaal Kernteam Crisiscommunicatie
Toezicht en handhaving	Sectorale toezichthouders
Vervolging	Openbaar Ministerie
	Europol
	Eurojust

Binnen de provincie Zuid-Holland is er vooral een rol weggelegd voor de veiligheidsregio's, lokaal gezag, de politie en sectorale CERTs. Met de nationaal essentiële dienstverleners wordt samengewerkt via de ISACS om informatie uit te wisselen. Het plan leunt regionaal sterk op de bijdrage van het Landelijk Dekkend Netwerk van Cybersecurity samenwerkingsverbanden, terwijl momenteel nog maar vier sectorale CERTs zijn aangewezen om informatie mee te delen:

- Z-CERT voor de zorg
- IBD voor de gemeenten
- SURFnet voor de universiteiten en hogescholen
- CERT Waterschapsmanagement

Daarnaast werkt het NCSC nauw samen met het DTC en CSIRT-DSP [lxix] voor digitale dienstverleners. In de provincie is het landelijk dekkend netwerk maar beperkt uitgerold, hetgeen betekent dat weliswaar naast de nationale AED's, ziekenhuizen, waterschappen, scholen en universiteiten zijn ingebed in de nationale structuren, maar het gros van de bedrijven in de regio die niet-essentiële diensten leveren dus niet.

G4 Gemeenten (in Zuid-Holland Rotterdam en Den Haag). De vier grote Nederlandse gemeenten hebben zich het advies van de WRR aangetrokken en hebben gezamenlijk advies gevraagd hoe het handelingsperspectief bij digitale crises kan worden verbeterd. Bureau Berenschot heeft een Handreiking Cybergevolgbestrijding G4-gemeenten [lxx] ontwikkeld in twee delen: deel 1: 'Warme fase – Praktische handvatten tijdens een cybercrisis' en deel 2: 'Koude fase- cybergevolgbestrijding'. De crisisplannen van de grote steden zijn nog erg gericht op de fysieke crisis, en niet op digitale ontwrichting. [lxxi] Het ligt in de bedoeling dat in het najaar 2020 de G4 gemeenten een oefening organiseren waarbij de handreiking ook aan de praktijk wordt getoetst. De handreiking is tot stand gekomen in samenwerking met de Nationale Politie, het Openbaar Ministerie, Nationaal Crisiscentrum, NCSC, veiligheidsregio's, de G4 gemeenten en verschillende CISO's van bedrijven en de vier gemeenten.

Veiligheidsregio's. De taken en organisatie van een veiligheidsregio staan beschreven in de Wet veiligheidsregio's. De belangrijkste taken van een veiligheidsregio zijn:

- Branden voorkomen en bestrijden
- Voorbereiden op risico's, rampen en crises
- Coördinatie, beheersing en bestrijding van rampen en crises

De crisisplannen van de grote steden zijn nog erg gericht op de fysieke crisis, en niet op digitale ontwrichting. [lxxii] Het ligt in de verwachting dat na de G4-oefening waar de Handreiking Cybergevolgbestrijding G4-gemeenten wordt getoetst input zal zijn voor de aanpassing van de crisisplannen van veiligheidsregio's.
Juist Veiligheidsregio's moeten hun digitale interne organisatie op orde hebben; we zijn er bij rampen en crisis immers van afhankelijk. Op 14 september j.l. bleek dat de Veiligheidsregio Noord en Oost Gelderland is aangevallen door een ransomware aanval. [lxxiii] De vraag is gerechtvaardigd of dit bij Veiligheidsregio's in Zuid-Holland ook kan gebeuren.

Cybercrisis oefeningen. Om voor een crisis klaar te zijn moet je oefenen. Crisisbeheersing is complex, betekent samenwerking met veel stakeholders en is ook geen alledaagse activiteit. Daarom moeten processen en procedures door te oefenen en simuleren worden getoetst en actueel gehouden. Regelmatig oefenen in verschillende verbanden (binnen bedrijf en organisatie; in samenwerking met gemeenten en stakeholders; binnen de veiligheidsregio, nationaal en internationaal) is van groot belang. In veel documenten wordt de ambitie om regelmatig digitaal crisismanagement te beoefenen onderstreept. Helaas is de praktijk weerbarstiger.

De **nationale cyberoefening** ISIDOOR wordt elke twee jaar gepland. ISIDOOR I was in 2015; ISIDOOR II in 2017. ISIDOOR III is uitgesteld tot 2021. Bij ISIDOOR II deden zo'n 60 publieke en private partners mee aan de vierdaagse nationale cyberoefening die de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) organiseerde. Spelers kwamen uit verschillende sectoren zoals energiedistributie, drinkwater, nucleair, keren en beheren van oppervlaktewater, chemie, telecom en de haven. Daarnaast hebben diverse ministeries mee geoefend. Doel van de oefening was de gezamenlijke aanpak, samenwerking en coördinatie bij een cybercrisis testen. Tijdens de oefening werden verschillende

cyberincidenten gesimuleerd in een zogenaamde ICS/SCADA-omgeving. ICS/SCADA zijn meet- en regelsystemen die industriële processen aansturen zoals bij waterzuiverings- of energiebedrijven.

Ook worden geregeld **internationale cyber oefeningen** gehouden, door de NAVO of door de EU. Bij de jaarlijkse oefening *Cyber Coalition* van NAVO zijn nationale delegaties uitgenodigd, waarbij soms ook het bedrijfsleven participeert. EU (ENISA) organiseert om het jaar de oefening *Cyber Europe*. Het plan voor 2020 was een scenario rondom gezondheidszorg, met als deelnemers nationale CSIRTs, cybersecurity autoriteiten, ministeries van gezondheidszorg, zorgverleners, eHealth dienstverleners en verzekeraars. Vanwege Corona is de oefening helaas uitgesteld.

Regionale cyberoefeningen. Veiligheidsregio's beoordelen hun eigen voorbereiding op cyberwaakzaamheid en cybergevolgbestrijding met respectievelijk een 5 en 6 (*out-of-ten*).[lxxiv] Door de veiligheidsregio's worden diverse activiteiten ondernomen om zich beter voor te bereiden. Als belangrijkste activiteiten worden genoemd: het opbouwen en onderhouden van regionale/landelijke netwerken, het opbouwen van cyberkennis en -expertise en het oefenen met cyberscenario's. Voor veel veiligheidsregio's is het nog zoeken hoe zich adequaat te prepareren op digitale verstoringen.
Om goed te kunnen anticiperen op cyberrisico's willen veiligheidsregio's:

- Cyberrisico's in de omgeving in beeld brengen samen met partners;
- Ontwikkelingen van het Cybersecuritybeeld Nederland vertalen naar de eigen regio;
- Duidelijkheid krijgen over de rollen, taken en bevoegdheden van alle betrokken actoren (landelijk, regionaal, lokaal), inclusief hun eigen rol en de benodigde expertise;
- Procedures rond alarmering, opschaling en besluitvorming verhelderen (bijvoorbeeld door middel van een specifieke cybercrisisfunctionaris);
- De eigen expertise van cyberbronbestrijding en cybergevolgbestrijding vergroten;
- Cyberscenario's uitwerken en (samen met partners) oefenen;
- Een landelijk aanspreekpunt inrichten voor cyberrisico's (koud) en bij cyberincidenten (warm).

Kortom: ook voor de veiligheidsregio's is er nog een weg te gaan en de vraag is gerechtvaardigd welke middelen daarvoor zijn gereserveerd.

G4 oefening. Naar aanleiding van het advies van Bureau Berenschot (handreiking cybergevolgbestrijding) hebben de 4 grote steden besloten dit najaar een gezamenlijke oefening te houden om de nieuwe aanpak te beproeven. De lessen zullen worden dan worden vertaald naar een nieuw crisisplan digitaal voor de betrokken veiligheidsregio's.

Overheid en gemeenten. Ook de overheid heeft ook een oefenambitie. Dit najaar worden een online overheid brede cyberoefening en webinars uitgevoerd voor *professionals*, managers en bestuurders van alle overheden. Dit zijn werknemers bij het Rijk, zelfstandige bestuursorganen, provincies, gemeenten, waterschappen en agentschappen. De serie activiteiten vinden plaats gedurende de maand oktober en worden georganiseerd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Vereniging Nederlandse Gemeenten, ICTU en NL DIGIbeter.

Sectorale cyberoefening. SURFnet is een organisatie die de sector universiteiten en hogescholen helpt met digitale weerbaarheid. Zij organiseert elke twee jaar een grootschalige, landelijke cybercrisisoefening. OZON beoefent crisismanagement tijdens een cybercrisis, maar toets ook hoe goed een instelling is voorbereid. Deelname door instellingen is facultatief. OZON 2016 en 2018 hebben interessante lessen opgeleverd. In 2016 constateert men dat het bewustzijn bij deelnemers aan de oefening is toegenomen, maar bij veel andere partijen die niet deelnamen achterblijft. Men concludeert

dat cybersecurity een integraal onderdeel moet zijn van crisismanagement en dat er heldere afspraken nodig zijn over proces, rollen en taken en het delen van informatie tussen instellingen. Ook onderkende men onduidelijkheid over landelijke coördinatie en pleit men voor vaker oefenen.[lxxv] In 2018 deden 50 organisaties en zo'n 2000 medewerkers mee. Men constateerde moeizame communicatie tussen de IT-ers en management en bestuurders, door het gebrek aan basis technische kennis van die laatste groepen. Ook vraagt men aandacht voor verbeterde afspraken over rollen en kennisdeling binnen de educatiesector tijdens een crisis.

Sinds 2017 beoefent de haven van Rotterdam cybercrisismanagement jaarlijks in de oefening CyberNautics. [lxxvi] Op 1 november 2019 oefenden de nautische ketenpartners in de Rotterdamse haven. Daarbij was het doel dat alle nautische partners die mogelijk betrokken raken bij een cyberincident, de crisiswerkwijze met elkaar trainen. Dit jaar werd het strategisch-bestuurlijk niveau geoefend door bestuurders verschillende dilemma's voor te leggen. In deze gezamenlijke oefening waren in 2019 de Veiligheidsregio Rotterdam-Rijnmond, Divisie Havenmeester van het Havenbedrijf Rotterdam, Loodswezen, Kustwacht, Portbase, Rijkswaterstaat, Douane, Nationaal Cyber Security Centrum en Deltalinqs betrokken.

Bedrijven en organisaties. Zeker bedrijven waarbij het uit de hand lopen van incidenten grote maatschappelijke invloed heeft (bijvoorbeeld een milieugevolg), doen geregeld crisis- of rampenoefeningen. Voor dergelijke bedrijven gelden regels, die ook worden ge-audit. Er is geen data beschikbaar in welke mate andere bedrijven in de Zuid-Hollandse economie dergelijke oefeningen organiseren om beter voorbereid te zijn op cyberincidenten en -crises. Net als bij de overheid staat het beoefenen van crises veroorzaakt door digitale ontwrichting nog in de kinderschoenen.

Wat betekent dit voor de regio?
De conclusie van de WRR dat Nederland onvoldoende is voorbereid op digitale ontwrichting geldt helaas ook voor de provincie Zuid-Holland. Procedures zijn vooral toegespitst op fysieke crises en houden onvoldoende rekening met digitale ontwrichting: er wordt weinig of niet geoefend. Zeker delen van de economie die geen AED zijn, moeten alles zelf regelen. De Rotterdamse haven vormt een positieve uitzondering. Er wordt elders weinig samengewerkt binnen economische sectoren, laat staan cross-sectoraal. Hoewel het beleid van de overheid sterk afhankelijk is van een Landelijk Dekkend Netwerk van Sectorale CERTs, zijn er nauwelijks van dergelijke CERTs in de provincie opgericht. De Rijksoverheid en de G4 gemeenten hebben de bal van WRR wel opgepakt en zijn bezig met aangepaste processen en procedures, maar die moeten nog geïmplementeerd en beoefend worden. Veiligheidsregio's wachten op de uitkomst van de G4 oefening en binnen economische sectoren is het stil. Alleen universiteiten en hogescholen kunnen gebruik maken van de diensten van SURFnet en om het jaar cybercrises beoefenen.

Wat kunnen we eraan doen?

- De provincie en de grote gemeenten moet in haar cyberbeleid expliciet haar ambitie aangeven om crisisbeheersing als gevolg van digitale ontwrichting op peil te krijgen en daarvoor middelen reserveren. De overheid moet beter voorbereid zijn om de impact van digitale ontwrichting op de maatschappij en de economie te beperken en snel terug te veren. Helder is dat in het huidige crisismanagement concept van Nederland de provincie een indirecte rol heeft, en de bal ligt vooral bij de vier veiligheidsregio's in de provincie. Twee daarvan hebben die bal al opgepakt samen met de G4 gemeenten. Ook het bedrijfsleven moet bijdragen aan deze ambitie. De economie van de provincie is kwetsbaar als digitale incidenten uit de hand lopen.

- Veiligheidsregio's moeten in regionale crisis- en rampenplannen digitaal risico beter inbedden, daarbij het voorbeeld van Rotterdam Rijnmond en Den Haag/Haaglanden volgend (handreiking Bureau Berenschot) en deze beoefenen om ze up-to-date te houden. In die plannen is helder vast gelegd wie welke verantwoordelijkheid heeft en hoe informatie wordt gedeeld. In die plannen wordt niet alleen beschreven hoe de crisis wordt beheerst, maar ook hoe met zo min mogelijk maatschappelijke en economische impact wordt teruggeveerd naar de normale situatie.
- Veiligheidsregio's moeten een risico-assessment van hun digitale administratieve organisatie en deze op orde brengen, mocht daar aanleiding toe zijn. Als gevolg van het incident bij de veiligheidsregio Oost-Gelderland is deze actie opgestart.
- Om het Landelijk Dekkend Netwerk van Sectorale CERTs in de provincie te verdichten is het gewenst dat elke economische sector in de regio, wellicht met steun van de overheid, van een sectoraal CERT gebruik kan maken om de bedrijven te helpen bij incidenten en crisis. Regionale economische sectoren kunnen zich op deze wijze, net als in de Rotterdamse haven, verenigen om de sector te versterken tegen digitale ontwrichting. Dit start met het ondersteunen van bedrijven bij het voorkomen en beheersen van cyberincidenten, het ontwikkelen van crisisplannen tot het testen van die plannen door simulaties en oefeningen voor cyber crisisbeheersing binnen de sector te organiseren, waarbij lokale of regionale overheden en de bedrijven deelnemen. FERM en SURFnet zijn goede voorbeelden.
- Cyber oefenkalender. Een entiteit op provinciaal niveau moet een simulatie- en oefenprogramma voor digitale crises opzetten en afstemmen tussen Rijk, Veiligheidsregio's, economische sectoren en grotere bedrijven in de regio. Voorkomen moet worden dat voor elke oefening het wiel opnieuw wordt uitgevonden. Wellicht kan een consortium meerjarig dit oefenprogramma verzorgen, inbegrepen het maken van evaluaties. Er moet aandacht zijn voor sectorale, cross-sectorale samenwerking bij crises en inbedding in de crisisstructuren van de overheid, rekening houdend met prioriteitstelling: grootste economische en maatschappelijke impact eerst en vaker.
- Crisisbeheersing is een publieke en private verantwoordelijkheid. De provincie en gemeenten moeten voldoende middelen in de begrotingen alloceren voor uitvoering van de cyberoefenkalender, waarbij de bedrijven daarnaast eigen middelen vastleggen voor deelname.
- Naast de oefenkalender worden regelmatig series van seminars voor stakeholders, publiek en privaat, in alle relevante sectoren over voorkomen van digitale crisis en over hoe tijdens een crisis te handelen. Deze seminars zijn ter voorbereiding van de oefeningen. Ook voor deze seminars worden middelen (tijd en geld) gereserveerd door overheid en bedrijfsleven.

SYNTHESE: *"HOUSTON – WE HAVE A PROBLEM….. AND AN OPPORTUNITY!"*

Op basis van de CRI2.0 methode hebben we acht aspecten van cyber gereedheid van de provinciale economie geëvalueerd. Dit memorandum is een synthese van die analyse. We kunnen niet anders vaststellen dat een belangrijk deel van de economie, met name het MKB 'niet cybergereed' is. Er is een groep koplopers, waaronder gereguleerde bedrijven en bedrijven en organisaties die zijn geïdentificeerd als nationale vitale dienstverleners (AED) en digitale dienstverleners, die het onderwerp serieus neemt en de risico's actief indamt. Tegelijkertijd is de bereidheid om de koe bij de horens te vatten in het merendeel van de economie niet groot. Het cyberrisico krijgt weinig aandacht.

Van de economische sectoren steekt de Rotterdamse haven er positief uit, overigens nadat ze in 2017 een forse *wake-up call* heeft gehad met de NotPetya-aanval waar onder andere APM-terminals schade door heeft geleden. We willen voorkomen dat ook in andere sectoren eerst een *wake-up call* nodig is om voldoende aandacht te krijgen voor dit onderwerp. Bedrijven die defensie en veiligheid ondersteunen, hebben de zaken ook op orde, daartoe wettelijk gestimuleerd door onder meer de regeling Algemene Beveiligingseisen Defensieopdrachten (ABDO).

Overigens zijn er meer lichtpunten. Er is, geleid door de Economic Board Zuid-Holland (EBZ), veel aandacht voor *Human Capital* in de IT en cybersecurity. Ook waar het gaat om innovatie zijn er plannen om de valorisatie van onderzoek in Zuid-Hollandse cyberproducten te verbeteren, zodat de economie beter kan profiteren van de investeringen in R&D.

Kosten van cyber onveiligheid zijn niet helder. Er is geen ondubbelzinnige analyse van de kosten van cybercrime voor de economie. Een globale indicatie is dat de economie van Zuid-Holland jaarlijks tussen de 2 en 4 Mld. euro verliest aan cybercrime. In 2016 heeft Deloitte vastgesteld dat cybercriminaliteit Nederlandse organisaties rond de tien miljard euro per jaar kost [lxxvii]. De omvang van de Zuid-Hollandse economie is ongeveer 25% van de nationale, dus indicatief was de *value at risk* in 2016 ongeveer 2,5 Mld. euro. Het *Ponemon Institute* en *Accenture* doen jaarlijks een onderzoek naar de kosten van cybercrime om de economische kosten van cyber criminaliteit te kwantificeren [lxxviii]. Dit onderzoek gaat over de gedigitaliseerde westerse wereld, niet per se Nederland, maar indiceert dat de kosten het laatste jaar 12% zijn gestegen en 72% in de laatste vijf jaar. *Lifescience* kent een kostenstijging in het laatste jaar van zelfs 74%. Het Centraal Bureau voor de Statistiek geeft in zijn Cybersecuritymonitor [lxxix] aan dat rond 15% van de bedrijven in de bedrijfstakken raffinaderijen en chemie, de voeding- en genotsmiddelenindustrie, de elektrische en elektronische industrie, de ICT-sector, vervoer en opslag, banken en verzekeraars en R&D uitval en kosten hebben van ICT-diensten door aanval van buitenaf. De grootste uitval en kosten zien we bij de telecomindustrie, rond 30% van de bedrijven. Dit is allemaal indicatief; geen cijfers gebaseerd op onderzoek in de regio. We hebben ook geen goed inzicht in de kosten, maar ook niet waar de risico's het grootst zijn, omdat nauwelijks wordt gemeld of aangifte wordt gedaan, met name door het MKB.

Als de waarde van het risico dat de economie loopt onbekend blijft, is het lastig vast te stellen welke inspanningen nodig zijn om te voorkomen dat de economie schade leidt en voorts welke prioriteit het onderwerp cybersecurity op de agenda van overheid en bedrijven zou moeten krijgen.

En de opbrengsten zijn ook niet klip en klaar! Cybersecurity is niet alleen een kostenpost. Een veilige en weerbare economie die beter bestand is tegen cyberaanvallen zal meer opbrengen dan een minder weerbare. Criminele organisaties gaan voor makkelijk geld met weinig pakkans; de zwakste schakel wordt het aanvalsdoel. Een goed beschermde economie heeft er dus minder last van cybercrime. Dat geldt overigens niet voor *state-sponsored* cybercriminelen. Die zijn vooral gericht op specifieke doelwitten, of het nu ontwrichting van de maatschappij is of spionage om de eigen economie of buitenlandse politiek te bevoordelen. Deze aanvallen komen de laatste jaren meer voor, maar zijn vaak gericht op specifieke doelen, die vaak tot de AED-organisaties behoren.

De opbrengsten van IT en cybersecurity-ondernemingen zijn significant. Cybersecurity biedt een kans als groeisector. Tegelijkertijd kan een regionale cyberindustrie de bedrijfscontinuïteit van de regionale economie helpen borgen terwijl we groeiende afhankelijkheid van digitale systemen en toenemende dreiging van cybercrime zien. De cijfers voor Nederland laten inderdaad een groei zien. SEO Economisch Onderzoek schatte de toegevoegde waarde van de cybersecuritysector voor Nederland in 2014 rond de 4 Mld. euro (ongeveer 10% van de omzet van de ICT-sector als geheel) met een jaarlijkse groei van rond de 7%. Cybersecurity groeide jaarlijks 14,5 % sneller dan de ICT sector zelf. [lxxx] Overigens geldt ook hier dat er geen goed inzicht is in actuele cijfers voor de regio, maar de regio heeft een actief cybercluster rondom The Hague Security Delta (HSD) ontwikkeld; dit betekent dat naar alle waarschijnlijkheid een belangrijk deel van die omzet in de regio neerdaalt.

De regio moet kosten en opbrengsten in kaart brengen. Het is gewenst dat de kosten (*value-at-risk*) en opbrengsten van cybersecurity voor de regio, ook per sector helderder worden. Alleen dan kunnen er goede beleidskeuzes worden gemaakt, door zowel overheid als het bedrijfsleven. Overigens geldt hetzelfde voor individuele bedrijven en organisaties: kwantificeerbaar maken van risico's als gevolg van digitale uitval, inbegrepen cybercrime helpt het onderwerp een integraal onderdeel te maken van de besluitvorming over de bedrijfsvoering.

Het onderwerp is lastig voor bestuurders en bedrijfsleiding. Veel van de geïnterviewde personen gaven aan het belang van cybersecurity te zien, maar er niet actief mee bezig te zijn als onderdeel van de bedrijfsvoering. Voor het merendeel van het MKB is het een onderwerp net als veel andere en niet hoog op de prioriteitenlijst. Dit ligt onder meer aan gebrek aan kennis van de risico's en de mogelijke schade als gevolg van IT-uitval en cybercrime; het ontbreken van een goede methodiek om dit digitaal risico te managen; onwetendheid van de regulering rondom cybersecurity; het een zaak van de IT-afdeling of de ICT-dienstverlener te vinden; ICT te ingewikkeld te vinden, vooral als er geen IT afdeling is; en onwetendheid over processen rondom incidentmanagement die het gevolg zijn van cybercrime. Dit laatste heeft ook impact op het doen van aangifte. Verscheidene geïnterviewden zeggen kennis te hebben van succesvolle *ransomware*-aanvallen in hun omgeving, maar geven aan dat waarschijnlijk *ransom* wordt betaald om de bedrijfsvoering voortgang te laten vinden. Transparantie ontbreekt.

Gebrek aan aandacht van bestuurders en bedrijfsleiding is een punt van zorg, zeker vanuit het perspectief dat we steeds verder gaan met digitaliseren van de bedrijfsvoering om economisch voordeel te realiseren. We kunnen ons weinig processen voorstellen die niet afhankelijk zijn van automatisering. Daarbij hoort tegelijk aandacht voor toenemende risico's als gevolg daarvan.

We zijn weinig expliciet over het belang van cyberveiligheid en -weerbaarheid voor de economie. Waar bestuurders in de regio aangeven het onderwerp belangrijk te vinden, zien we dit niet vaak terug

in formeel beleid. Het onderwerp cybersecurity wordt niet expliciet benoemd, staat vaak niet expliciet benoemd in begrotingen en ook is het onderwerp niet bij één persoon belegd. Positieve voorbeelden zijn de gemeente Den Haag (*Resilience Officer*) en het havenbedrijf Rotterdam (*Port Cyber Resilience Officer*). Waar het onderwerp eenhoofdig is belegd, zien we stappen naar betere weerbaarheid genomen worden. Ook de economische sectoren (behoudens de Rotterdamse haven) dragen het onderwerp weinig expliciet uit. Of het nu de glastuinbouw is, of de *life science*/biotech sector of de hightech maakbedrijven: de industrieën zijn ketens van klanten, producenten, logistiek en toeleveranciers die digitaal verbonden zijn en daarmee kwetsbaar.

De risicomanagementcultuur kan beter als het gaat om digitaal risico. Risicomanagement is inherent verbonden met ondernemen. Ook de overheid versterkt haar processen voor risicomanagement. Behoudens een kleine kopgroep staat het managen van digitaal risico: risico als gevolg van uitval van ICT, dataverlies waaronder persoonsgegevens en intellectueel eigendom, en cybercrime niet hoog op de lijst van belangrijke '*risk*' onderwerpen. Voor gereguleerde onderneming (zoals nationaal aangewezen essentiële dienstverleners) is dit anders; zij moeten immers *compliant* zijn met die wetten of regels. Via audits wordt vastgesteld of er aan de regels wordt voldaan. Hoewel *compliant* zijn een goede eerste stap is, borgt het de minimum standaard van cyberrisicomanagement. Een goede vertaling van de digitale risico's naar bedrijfsvoeringsrisico 's (welke kwetsbare systemen ondersteunen welke bedrijfsprocessen) en *value-at-risk* (wat is de waarde van het risico dat door cyberaanval door het bedrijf wordt gelopen) is noodzakelijk voor besluiten over bedrijfsvoering en borgen van aandeelhoudersbelangen. Bedrijfsvoeringsopleidingen en *executive* trainingen kunnen meer aandacht aan dit onderwerp besteden.

Het MKB heeft hulp nodig. Waar de rijksoverheid de cyberveiligheid en -weerbaarheid van ruim 100 aangewezen essentiële dienstverleners (van belang voor nationale veiligheid) in Nederland ondersteunt, staat het gros van het MKB er alleen voor. De initiatieven van het Digital Trust Center gericht op het MKB zijn vooralsnog een druppel op de gloeiende plaat. Het tempo van implementatie is te laag. Het stimuleren van een landelijk dekkend netwerk van cybercentra is een goed initiatief, maar heeft in Zuid-Holland nog niet veel bedrijven bereikt. Ook het Centraal Plan Bureau is kritisch over de aanpak en ziet risico's in een decentrale aanpak. De veelheid van initiatieven op het gebied van samenwerking en voorlichting kan tot inefficiëntie of inconsistentie leiden. [lxxxi] Het MKB pakt cybersecurity niet vanzelf op en heeft hulp nodig op verschillende vlakken:

- **Begrip van cyberrisico**: wat is mijn risico en wat kan ik eraan doen; welke verplichtingen heb ik (zoals voor AVG); hoeveel cybersecurity investeringen zijn genoeg, wanneer is het een overkill; wat zijn betrouwbare oplossingen en cyberdienstverleners; moet ik me verzekeren? Zeker voor het MKB is dit een forse uitdaging, waarnaar de Haagse Hogeschool interessant onderzoek heeft gedaan [lxxxii].
- **Incident response**: wat moet ik doen als er een aanval is op mijn bedrijf; wie kan ik bellen voor eerste hulp; welke instanties moet ik informeren; wel of geen *ransom* betalen aan cybercriminelen; moet ik aangifte doen?
- **Information sharing**: hoe kom ik aan actuele informatie over cyber dreiging en kwetsbaarheden voor mijn organisatie; hoeveel tijd en geld moet ik daarin investeren? En wie informeer ik als mijn bedrijf zelf is aangevallen; met wie deel ik die kennis en lessen zodat de impact in de sector beperkt kan blijven; deel ik dat ook met de concurrentie, gaat cyberveiligheid boven competitiebelangen?

- **Awareness training**: moet ik tijd en geld besteden aan het trainen van mijn personeel; ben ikzelf voldoende geschoold; moeten we incident response plannen beoefenen? Wie koopt die training of oefening dan in? Hebben we daar voldoende kennis voor?
- **Innovatie**: wanneer ga ik ICT-systemen vernieuwen of hun veiligheid verbeteren; voor welke oplossingen kies ik dan; ga ik in zee met de grote multinationale providers ($$$) of juist met innovatieve bedrijven in de buurt; hoe test en valideer ik hun oplossingen?
- **Crisismanagement**: wat gaan we doen als het echt uit de hand loopt na een cyberaanval, bijvoorbeeld wanneer zo'n aanval meerdere bedrijven geraakt heeft en er ook fysieke schade aan de omgeving ontstaat; met wie werken we dan samen; hoe managen we de crisis in de organisatie; hoe gaan we om met de media; hoeveel tijd moeten we inruimen om dit te beoefenen en welke scenario's dan?

Het is rijksbeleid om het MKB via een **landelijk dekkend netwerk van cybercentra** te helpen, bij voorkeur per economische sector. Het Digital Trust Center speelt daarbij een belangrijke rol als *linking pin* naar het Nationale Cyber Security Center. Zo zijn er verschillende sectorale centra – vaak stichtingen of *not-for-profits* - opgericht voor de zorg (Z-CERT), voor onderwijsinstellingen (SURFnet), voor watermanagement (CERT-WM) voor de gemeenten (IBD-CERT). Een aantal andere zijn in het proces om ook door het rijk te worden geaccrediteerd voor het verkrijgen van hoogwaardige informatie, zoals Cyber Weerbaarheidscentrum Brainport Eindhoven [lxxxiii], FERM Haven Rotterdam [lxxxiv], Cybersecurity Centrum Maakindustrie in oost Nederland [lxxxv], of Connect2Trust [lxxxvi] Holland Instrumentation heeft een beginnende dienstverlening opgezet.

Verdicht het netwerk regionaal. Het netwerk is echter bij verre van landelijk dekkend; in de regio wordt maar een klein deel van het MKB bereikt. [lxxxvii] Het is moeilijk gebleken centra op te richten met een businessmodel dat ook zonder subsidies houdbaar is. Het is overigens wel de weg te gaan om – onder voorwaarden - **nieuwe Cybersecurity Centra** op te richten, of aan te sluiten bij bestaande centra. Een van die voorwaarden is dat in de regio één concept van Cybersecurity Centra moet worden opgezet, met gelijksoortige procedures en processen, zodat ze goed als een netwerk kunnen samenwerken. De centra moeten wel gericht zijn op de specifieke issues van de sector. Cybersecurity Centra kunnen met name het MKB ontzorgen op een economisch verantwoorde manier. Samendoen is immers altijd beter en goedkoper dan apart. Voor bedrijven die in ketens werken is die samenwerking nog belangrijker. Om verschillende reden heeft samenwerking in economische sectoren de voorkeur: een economische sector heeft ondernemersorganisaties en kent elkaar; dit is nodig voor het onderlinge vertrouwen om gezamenlijk een uitdaging op te pakken; heeft specifieke digitale oplossingen en kwetsbaarheden, en is vaak genetwerkt, leveranciers en toeleveranciers zijn digitaal verbonden. Overigens is een regionaal dekkende samenwerkingsvorm voor bepaalde functies die niet sectoraal op te pakken zijn, of heel kostbaar zijn, ook goed mogelijk.

Begin een cybercentrum alleen als er voldoende draagvlak is. De ambitie van die centra moet wel zijn afgestemd op de bereidheid van de deelnemers om financieel bij te dragen: oftewel, begin alleen als de sector dat wenst en begin niet met een te grote broek aan, maar met bijvoorbeeld minder kostbare taken als het verhogen van awareness en risicobegrip bij bestuur en bedrijfsleiding. Als beide zich beter ontwikkelen, zal er ook de bereidheid toenemen om meer middelen te besteden en aanvullende diensten af te nemen. Bijlage D beschrijft een aantal *best-practices* voor het opzetten van een cybersecuritycentrum.

Voorlopers in de regio. In navolging van FERM, het cybersecurity centrum voor de Rotterdamse haven, ligt het voor de hand cybersecuritycentra te starten voor Greenport en voor Biotech, maar draagvlak moet verder worden opgebouwd. Samenwerking met onderwijs in informatietechnologie kan helpen een win-win te realiseren: praktijkervaring voor studenten, betaalbare oplossingen voor het MKB. Het Greenport Cybersecurity Centrum kan het startpunt zijn van een centrum voor de landelijke glastuinbouw. Biotech kan zich later richten tot de hele biotech/pharma sector in Nederland. Ook Holland Instrumentation kan de bij IQ gestarte functie (HI Cybersecurity Network) omzetten tot een feitelijk cybersecuritycentrum voor de sector, of aanhaken bij het Cybersecurity Centrum Maakindustrie, dan wel het Cyber Weerbaarheidscentrum Brainport. Overigens is helder dat '*it takes two to tango*'. En …groter is niet per definitie beter!

Overweeg een regionale cyberbrandweer. AED-bedrijven en organisaties kunnen bij een cyberincident eerste hulp krijgen van het nationale *Cyber Security Incident Response Team*. Voor niet- AED-bedrijven heeft het nationale CSIRT geen leverplicht. Toch is het van belang dat niet-AED bedrijven bij een cyberincident acuut help kunnen krijgen om de impact van het incident te beperken en snel terug te kunnen veren naar de normale bedrijfsvoering. De cyberbrandweer doet eerste hulp; en verwijst naar expertbedrijven die het forensisch onderzoek kunnen doen en kunnen helpen bij herstel van de OT en OT ondersteuning van het bedrijf. Een CSIRT of CERT-functie vergt hoogwaardige expertise en ervaring, en is waarschijnlijk te kostbaar om per sector in te richten. Hier is wellicht een regionale oplossing het beste. Dit CSIRT-ZH kan de spin in het web zijn van sectorale cybersecurity centra.

De overheid en het bedrijfsleven kunnen het MKB helpen. Organisaties werken in ketens en zijn in grote mate afhankelijk van toeleveranciers. Die ketenprocessen worden steeds digitaler. Het is niet meer genoeg om alleen de eigen organisatie veilig en op orde te hebben; als de *supply chain* de zwakste schakel is, wordt dat de aanvalsvector. Overheid en grotere bedrijven hebben er dus belang bij om te zorgen dat de toeleveranciers digitale veilige organisaties zijn. Maar in hoeveel contracten worden er eisen gesteld aan de mate van digitale veiligheid van de toeleverende onderneming? Of dat men verzekerd is voor cyberrisico? Wordt er gemonitord en ge-audit in de keten? Hoe vaak stellen banken eisen aan cybersecurity bij investeringen? En welke hulp bieden die organisaties aan de keten om het risico te verminderen? Het valt te overwegen net als Defensie (ABDO) heldere eisen te stellen bij aanbestedingen of contractvorming voor toeleveranciers en dienstverleners. En zouden de grotere bedrijven, hoger gepositioneerd in de ketens de Cybersecurity Centra niet kunnen meefinancieren? Daar ligt immers direct belang.

We maken goede stappen met de Human Capital Agenda. Onder regie van de EBZ is de taskforce human capital opgericht die al een aantal jaren werkt aan het realiseren van het Human Capital Akkoord en een actieve Human Capital Agenda. Voor 'veiligheid', en ook cybersecurity als onderdeel daarvan is er een apart initiatief dat wordt uitgevoerd door The Hague Security Delta met als doel vraag en aanbod in kaart te brengen, af te stemmen en te stimuleren. Onderwijsinstellingen maar ook het bedrijfsleven zijn actief betrokken. Dit publiek-private initiatief levert zichtbaar resultaat op, maar is tegelijkertijd een actie die lange adem vereist. Is het akkoord en de agenda een model dat ook voor het stimuleren van cyberveiligheid en -weerbaarheid binnen het digitale domein kan werken?

Digitaliseringsinitiatieven mogen de economie niet kwetsbaarder maken. Het is fantastisch om te zien hoeveel digitaliseringsinitiatieven, proeftuinen, living labs er wel niet zijn in de regio om de voordelen van 5G, IoT en andere innovaties te benutten. Bij deze initiatieven is er veel aandacht voor functionaliteit, maar te weinig voor de nieuwe digitale risico's die de innovaties inherent met zich

meebrengen. Het is noodzakelijk meer rekening te houden met veiligheid en te vereisen dat nieuwe digitale technologie *secure-by-design*, *resilient-by-design* is en privacy borgt. Dit betekent ook dat het cybercluster actiever betrokken moet zijn bij deze initiatieven en helpt de digitaliseringsinitiatieven integraal te laten bijdragen aan een duurzame en digitaal weerbare economie.

Cyberinnovatie moet de economische sectoren helpen cyberweerbaarheid makkelijker (en goedkoper) te maken. Bedrijfssystemen digitaal veilig en weerbaar maken en houden is momenteel te ingewikkeld. Dit geldt niet alleen voor informatietechnologie (IT), maar vooral ook voor operationele technologie (OT), zoals we die zien in de haven, in de tuinbouw, in de maakindustrie. Vooral in de IT stapelen de cybersecurityoplossingen zich op en is het niet makkelijk vast te stellen met welke architecturen en welke oplossingen de risico's het best kunnen worden afgedekt. In de OT is de aandacht voor cybersecurity nog relatief nieuw, omdat oorspronkelijk OT-netwerken op zichzelf stonden en niet met het internet verbonden waren. Dat is nu vaak wel zo, met alle gemakken en risico's van dien. Cyberinnovatie ten behoeve van de Zuid-Hollandse economie moet zich vooral focussen op het eenvoudiger en goedkoper maken van oplossingen om de cyberweerbaarheid van bedrijven, zowel IT als OT te borgen. Overigens is het door de provincie en gemeente Den Haag gesteunde *Automated Security Operations Consortium* (*ASOC*) met TNO, HSD en verschillende bedrijven een goed voorbeeld in deze richting.[lxxxviii] Om cyberweerbaarheid te verbeteren is het nodig goed begrip te hebben van de specifieke bedrijfsprocessen van economische sectoren. Het cybercluster moet daarom meer een integraal onderdeel worden van het netwerk van innovatie-initiatieven van die sectoren, zoals de haven, glastuinbouw, defensie en veiligheid, air & space, biotech en hightech instrumentation.

Nederland moet haar cyber kerncompetenties en productontwikkeling borgen en dat is goed voor de regio. Nederland is te afhankelijk van import van essentiële technologieën om ons land veilig en weerbaar te houden. Dat is een risico, want die technologie kan niet gegarandeerd beschikbaar zijn, zeker als die van buiten Europa komt. Denk hierbij aan post-quantum cryptologie, netwerktechnologie, hoog beveiligde datacentra. R&D en innovatie uitgevoerd in deze regio zal geen windeieren leggen en versterkt de positie van het cybercluster.

Er liggen kansen voor innovatie als meer met defensie en veiligheidsdiensten wordt samengewerkt. Defensie en veiligheidsdiensten, maar ook NAVO en Europol investeren veel in cybersecurity oplossingen en innovaties. Die oplossingen zijn breder bruikbaar, bijvoorbeeld voor vitale diensten of bedrijven met waardevolle IP. De veiligheidsorganisaties zien het nut in samenwerken met jonge innoverende bedrijven, maar om tal van redenen lukt dit niet goed. Defensie heeft daarom besloten een Cyber Innovatie Hub in Den Haag te starten. Deze zal zich niet afscheiden van het Haagse security cluster, maar moet er juist middenin komen te staan zodat kennisoverdracht van de hoog beveiligde domeinen naar de 'gewone' ICT oplossingen kan plaatsvinden en tegelijkertijd innovatieve oplossingen uit de markt bij defensie en de diensten kan worden getoetst. Ook blijkt internationaal dat cyberclusters die hecht samenwerken met defensie en veiligheidsdiensten tot de meest productieve worden gerekend. Een voorbeeld is CyberSpark in Israël.

Er is geld beschikbaar voor cybersecurity R&D en innovatie, maar het komt niet vanzelf naar de regio. De regering investeert fors in R&D en innovatie. Een nieuw cybersecuritysamenwerkingsplatform van het Ministerie van Economische Zaken en Klimaat gaat zich richten op een handvol thema's voor cybersecurity R&D en innovatie. De overheidsmiddelen voor R&D zullen vooral naar die thema's gaan. Het is dus zaak dat de regio thema's aandraagt, relevant voor de regionale economie. Actief inbrengen van relevante onderwerpen is van belang, zoals de regio eerder heeft gedaan met het *ASOC.* Ook is er

Europees geld voor R&D en innovatie, waarvan Nederland en Zuid-Holland mee kan profiteren als de complexe procedures beter begrepen worden en de lobby goed is georganiseerd. Als de overheid en het bedrijfsleven meer meewerkt aan valorisatie van regionale producten en vaker *launching customer* wordt, beïnvloedt dit de aantrekkelijkheid voor private investeringen in regionale cyberbedrijven. Kortom: het is de moeite waard startups en scale-ups actief te helpen bij het vinden van middelen en dit goed te organiseren.

Voorkomen van digitale ontwrichting vergt aandacht. De zorgen die de Wetenschappelijke Raad voor het Regeringsbeleid uit over het gebrek aan voorbereiding om digitale ontwrichting van de economie van Nederland te voorkomen, geldt helaas ook voor de provincie Zuid-Holland. Niet alleen is de provincie de grootste economie van Nederland, ook is ze al in hoge mate gedigitaliseerd en heeft de terechte ambitie digitale technologie verder uit te buiten. De regio vergt effectief watermanagement om droge voeten te houden en heeft veel industrieën die bij een incident, ook een cyberincident negatieve impact kunnen hebben op maatschappelijk welzijn. Ook is het nog eens heel druk op wegen, waterwegen en in het luchtruim; alles is digitaal aangestuurd. Daarnaast is een belangrijk deel van de economie, met name het MKB kwetsbaar. Dat vergt goed beoefende crisismanagementplannen, die up-to-date zijn voor digitale incidenten en ontwrichting. Plannen van bedrijven, die de lokale samenwerking met (digitale) hulpverlening verzekeren; van steden en veiligheidsregio's; plannen die zijn afgestemd met nationale inzet. Er is nog een weg te gaan om dit te realiseren.

Waarom is het verbeteren van cyberweerbaarheid vooral een probleem van het bedrijfsleven? Moet de overheid geen groter rol nemen? Natuurlijk is elk bedrijf of organisatie zelf verantwoordelijk om adequate maatregelen te nemen tegen de risico's die een bedrijf loopt. Dat geldt voor brand, voor diefstal en ook voor digitale risico's. Een bedrijf kan technische maatregelen nemen, mensen opleiden, diensten inhuren, zich verzekeren of een risico bewust accepteren. Voor bepaalde sectoren is dit niet alleen een economische keus, omdat wet- en regelgeving bepaalde eisen stelt. Voor vrijwel iedereen geldt de Algemene Verordening Gegevensbescherming (AVG). Voor nationaal essentiële dienstverleners (AED), digitale dienstverleners, maar ook verschillende andere sectoren zoals defensie-industrie, geldt daarnaast dat zij verplicht zijn bepaalde maatregelen te nemen (zorgplicht). De overheid ondersteunt die ruim honderd bedrijven en organisaties dan ook om aanvallen te voorkomen en bij het reageren op incidenten.

De regering wenst niet verder in te grijpen in de markt door van een grotere groep bedrijven meld- en zorgplicht te eisen om de cyberweerbaarheid van de economie te borgen, tenzij daar goede redenen voor zijn. Zo zijn in verband met de COVID-pandemie organisaties uit de zorgsector tijdelijk toegevoegd. Vanuit nationaal en economisch perspectief is er veel voor dit beleid te zeggen.

Maar nu vertegenwoordig je een bedrijf of organisatie die vitaal is voor de provincie of de regio. Je bent een grote werkgever. Je bent geen AED en je wordt aangevallen. Je staat er alleen voor. Er is geen CSIRT van het NCSC die leverplicht heeft; je kan dus niet van ondersteuning uitgaan. Je hebt ook geen ervaring met cyberaanvallen, want zo vaak komt het nu ook weer niet voor. Wie ga je bellen? In het weekend, want cyberaanvallers die echt kwaad willen doen dit op onverwachte momenten. Als er brand is, bel je de brandweer; als er gewonden vallen, bel je de eerste hulp en krijg je iemand aan de lijn die je helpt bij de acties die je snel moet nemen om erger te voorkomen. Bij diefstal bel je de politie. Waarheen kunnen we bellen bij een cyberincident?

De rijksoverheid vindt dat het bedrijfsleven dit zelf moet organiseren, en dus ook zelf betalen. Vandaar de oproep om het landelijk dekkend netwerk te verdichten, door het bedrijfsleven zelf te financieren. Sommige initiatieven kunnen 200k euro subsidie krijgen voor de eerste twee jaar. Maar het blijkt heel lastig te zijn om een goed businessmodel te ontwikkelen voor zo'n sectoraal Cybersecurity Centrum; het MKB staat (nog) niet in de rij om aan te sluiten en moet al van zoveel 'dingen' lid zijn. Een CSIRT of CERT-functie (de cyberbrandweer) is al helemaal niet te betalen; dat vereist een groep ervaren experts die daar een dagtaak aan hebben. Dus we zitten in een vicieuze cirkel: we wachten tot de brand geweest is; we dempen de put als het kalf verdronken is. Na een forse cyberaanval op onze economie komt er wel aandacht… zo hebben we in Rotterdam gezien.

De vraag is gerechtvaardigd wat de rol van de overheid zou moeten zijn. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) [lxxxix] vraagt om een publiek debat over de toerusting van de Nederlandse samenleving met het oog op de mogelijkheid van een digitale ontwrichting en vindt dat de overheid een grotere rol moet nemen. Ze vindt de definitie van vitale diensten te eng, onder meer omdat vitale dienstverleners in ketens werken. Die ketenpartners, veelal MKB, vallen niet onder de definitie van AED. Ook TNO beveelt aan dat de overheid haar rol in het cyberveilig maken van de Nederlandse samenleving moet heroverwegen. [xc] De complexiteit van het domein en de daaraan verbonden cybersecurity-uitdagingen is zo groot dat de samenleving deze niet zelf kan adresseren. Ze beveelt aan, in lijn met onder andere de visie van het *World Economic Forum* (WEF) [xci], cybersecurity te beschouwen als een 'publiek goed'. Marcel Pfeiffer, hoogleraar aan de Universiteiten van Nyenrode en Leiden vindt ook dat de rol van de overheid wel wat groter mag, maar dan vooral op het gebied van voorlichting en bewustwording en het aanreiken van simpele en waar mogelijk goedkope oplossingen, dit ook als tegenwicht voor het optreden van commerciële organisaties die vooral dure adviezen en oplossingen aandragen, waarvan niet makkelijk beoordeeld kan worden in welke mate die echt nodig zijn. [xcii]

Kortom: het verdient aanbeveling dit onderwerp verder uit te diepen. Dit vergt een nationaal debat, publiek en privaat. Maar dat debat zou heel goed in Zuid-Holland, de grootste economie van Nederland kunnen starten.

BIJLAGE A: LIJST GEïNTERVIEWDE PERSONEN

Alexis Barron	Cyberweerbaarheidcentrum Brainport - Directeur
Jan Piet Barthel	Dcypher - Directeur
Colinda de Beer	InnovationQuarter – Senior Business Developer Horticulture
Bibi van den Berg	Leiden University – Hoogleraar Cybersecurity Governance
Raymond Bierens	Connect2Trust Foundation – Chairman of the Board
Fred Boekhorst	Dutch Digital Delta, team ICT - Directeur
Adri Bom – Lemstra	Provincie Zuid-Holland – Gedeputeerde Economie en Innovatie, Land- en Tuinbouw, Gezond en Veilig, Milieu en Bodem
Joris den Bruinen	Stichting The Hague Security Delta – Algemeen Directeur
Barbara Brunnhuber	Leiden University – General manager Business Activities Metabolomics BioPartner Center Leiden – Executive in Residence
Marly Coenders	Gemeente Rotterdam – Senior Strategic and Government Advisor
Eefje Dekkers	InnovationQuarter – Director Innovation
Wim van den Doel	Leiden-Delft-Erasmus Universities Alliance – Dean Leiden University – Professor of Contemporary History
Rob van Dort	Nederlandse Industrie voor Defensie en Veiligheid – Program Manager Cyber Resilience
Remco Duijverman	Hoogendoorn Growth Management – Product Owner Software Development
Sandro Etalle	Technische Universiteit Eindhoven – Full Professor and Chair of the Security Group
Tim Franken	InnovationQuarter – Business Developer Digital Technology
Edward Gilding	InnovationQuarter – Senior Business Developer Port & Maritime
Martin van Gogh	Batenburg Industriële Automatisering – Divisie Directeur Hoogendoorn Growth Management - Chief Executive Officer Economic Board Zuid-Holland – Member of the Board
Jos Griffioen	Hogeschool Leiden – Education Manager Informatics
Bert van Haarlem	Leiden University Medical Center – directeur ICT
Ida Haisma	Leiden Bio Science Park - Director
Elly van den Heuvel	Nationale Cybersecurity Raad - Secretaris
Pancras Hogendoorn	Leiden University Medical Center – Dean & Vice-Chairman of the Board, Professor of Pathology
Rick van Holsteijn	Rijk Zwaan – Project Adviseur (Cyber Security)
Liesbeth Holterman	Cyberveilig Nederland – Beleidsadviseur Novel-T – Projectleider Cybersecurity Centrum Maakindustrie
Martijn van Hoogenhuyze	InnovationQuarter – Senior Account Manager Safety & Security
Auke Huistra	Applied Risk B.V. - Partner
Martijn Jonk	Nationaal Cyber Security Center – Team Leader
Jelte van Kammen	Harvest House – Algemeen Directeur/Chief Executive Officer
Mick van Kappen	Innovation Quarter – Transition Manager Smart Digital Delta
Oscar Koeroo	KPN – Team Lead Government and External Relations to the CISO
Edwin Kok	Cocus Consult – Owner Samenwerkingsverband Cybersecurity i.o. - kwartiermaker
Sandra Konings	BDO Nederland – Equity Partner Cybersecurity Cyberweerbaarheidscentrum Brainport – Member Advisory Board

	FERM - Kwartiermaker
Jan Koudijzer	Festo NL – Market & Technology Development Manager
	Holland Instrumentation – Member of the Board
Bert Kremer	Provincie Zuid-Holland – Hoofd Eenheid Advies Gebruik Assets & Technisch Specialistisch Onderhoud (Wegen en Waterwerken)
Ras Lalmy	Yes!Delft – Managing Director The Hague
Rutger Leukfeldt	The Hague University of Applied Sciences – Director Centre of Expertise Cybersecurity
Andre van der Linden	Royal Flora Holland – Chief Information Officer
Woody Maijers	Greenport WestHolland – Innovationpact manager
Eric van Meijer	Airbus Defence and Space Netherlands – Head of Services
Rene Montenarie	ECP Platform voor de InformatieSamenleving – Directeur Operations
	Team Dutch Digital Delta – plv Directeur
Juriaan Rijnbeek	Leiden University Medical Center – Manager Architecture & Security
Kevin Scheid	NATO Communications & Information Agency – General Manager
Hans Schikan	Biotech Entrepreneur, Board member, Chair Pharma & Life Science
Arno Sevinga	VOPAK – Corporate Information Security Officer
Marcel Spruit	The Hague University – Professor Cyber Security
Maarten Tossings	TNO – Lid Raad van Bestuur / Chief Operating Officer
	Voorzitter Taskforce Digitale Economie / Economic Board Zuid-Holland
Kim van der Veen	Digital Trust Center - Relatiemanager
Michel Verhagen	Digital Trust Center - Programmamanager
Hans van der Vet	Gemeente Den Haag – Directeur Veiligheid
Berry Vetjens	TNO – Director Market TNO ICT
Jacco Vooijs	Glastuinbouw Westland - Voorzitter
Jeroen van der Vlugt	Ministerie van Defensie – Chief Information Officer
Eveline Vreede	Technische Universiteit Delft – Executive Manager Safety & Security Institute / Leiden Delft Erasmus Universities Cyber Security
Jaron Weishut	Nexero – consultant & owner
	TF Digital Economy – kwartiermaker Smart Digital Region
Delia Wind	Holland Instrumentation – Project manager
Annemarie Zielstra	TNO – Director Cyber Security & Resilience
	Momenteel: KPMG – Partner Cyber Security

BIJLAGE B: NATIONALE KADERS VOOR CYBERSECURITY

Wet beveiliging netwerk- en informatiesystemen (Wbni). Recent is een cyberwet in het Parlement aangenomen: Wet Beveiliging Netwerk- en Informatiesystemen [xciii]. De wet regelt onder andere de implementatie van Europese regelgeving zoals de *Regulation for Security of Network- and Information Systems.* De Wbni dicteert onder meer dat bepaalde organisaties 'passende technische en organisatorische maatregelen op het gebied van cyber security moeten nemen'. De wet geldt voor zogenoemde Aanbieders van Essentiële Diensten (AED's) en digitale dienstverleners. De overheid bepaalt welke bedrijven essentieel zijn. AED's bevinden zich in essentiële sectoren als energie, vervoer, bankwezen, infrastructuur voor de financiële markt, levering en distributie van drinkwater, en digitale infrastructuur. Onder digitale dienstverleners wordt verstaan online marktplaatsen, zoekmachines en clouddiensten. Deze laatstgenoemde organisaties kunnen zelf bepalen of zij onder Wbni willen vallen.

De wet legt AED's en digitale dienstverleners in essentie twee verplichtingen op:

- Een zorgplicht om de nodige technische en organisatorische maatregelen te nemen om de cybersecurity op orde te hebben, en
- Een meldplicht wanneer zich incidenten op het gebied van cybersecurity voordoen met (potentieel) aanzienlijke gevolgen.

Daarnaast regelt de wet de rol van het nationale Cyber Security Incident Response Team van het NCSC en het delen van (gerubriceerde) informatie over cyberrisico's of incidenten. Dit blijft voorbehouden aan bedrijven en organisaties die tot de bovengenoemde categorieën behoren of daartoe zijn geaccepteerd. Er is geen leverplicht voor het CSIRT aan andere sectoren, maar het staat open om hulp te vragen.

<u>Consequenties</u>:

- Alleen de nationale AED's en digitale diensten in de provincie kennen meld- en zorgplicht en worden ondersteund; Die van belang voor maatschappelijke veiligheid en economische weerbaarheid van provincies en regio's niet.
- Het gros van het MKB wordt niet met zekerheid ondersteund vanuit het NCSC omdat die geen leverplicht heeft.
- Het gros van het MKB krijgt geen dreigingsinformatie, tenzij ze deel uitmaakt van een regionaal of sectorale organisatie die daartoe is geautoriseerd. Dit kan een weerbaarheidscentrum zijn.

Baseline Informatiebeveiliging Overheid [xciv] Om de veiligheid verder te vergroten, is sinds 1 januari 2019 de Baseline Informatiebeveiliging Overheid van kracht, afgekort BIO. Tot 2019 hadden alle bestuurslagen een eigen baseline, de BIR (Rijk), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Deze baselines zijn (met uitzondering van de BIR2017) voor een groot deel nog gebaseerd op de ISO-normering uit 2005 en lopen achter op de actuele ISO-normen. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Deze baseline wordt nu geïmplementeerd bij de provincie, inbegrepen provinciale diensten. Ook gemeenten zijn gehouden aan deze nieuwe norm. Naast de BIO gelden voor de overheid en haar toeleverende bedrijven het Voorschrift Informatievoorziening Rijksdienst (VIR) en de regeling Algemene Beveiligingseisen Defensie Opdrachten (2019). De VIR regelt de omgang met gevoelige informatie. ABDO zijn verplichtingen voor het bedrijfsleven om deel te kunnen nemen aan defensieopdrachten. De versie 2019 stelt heldere eisen aan de cyberweerbaarheid van deelnemende bedrijven.

Consequenties:

- Deze regelingen gelden voor overheidsorganisaties en niet voor het bedrijfsleven.
- De regelingen zijn van belang voor bedrijven die producten of diensten leveren aan de overheid; die moeten aan die cybersecurity eisen voldoen.

Nationale Cybersecurity Strategie [xcv] en Nederlandse Cybersecurity Agenda.[xcvi] De Nationale Cybersecurity Strategie 2 van 2013 is een verdere ontwikkeling van de eerste strategie. Ze legt nadruk op publiek, private participatie, focus op netwerken en strategische coalities, verduidelijkt de onderlinge verhouding tussen stakeholders en richt zich op capaciteitsopbouw, met name bij de overheid. De strategie benadrukt het belang van risico-analyse: het vinden van een balans tussen bescherming en bedreiging van belangen en de mate waarin we risico maatschappelijk willen accepteren. In 2018 is besloten tot een verdere uitwerking in de Nederlandse Cyber Security Agenda. De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.

1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

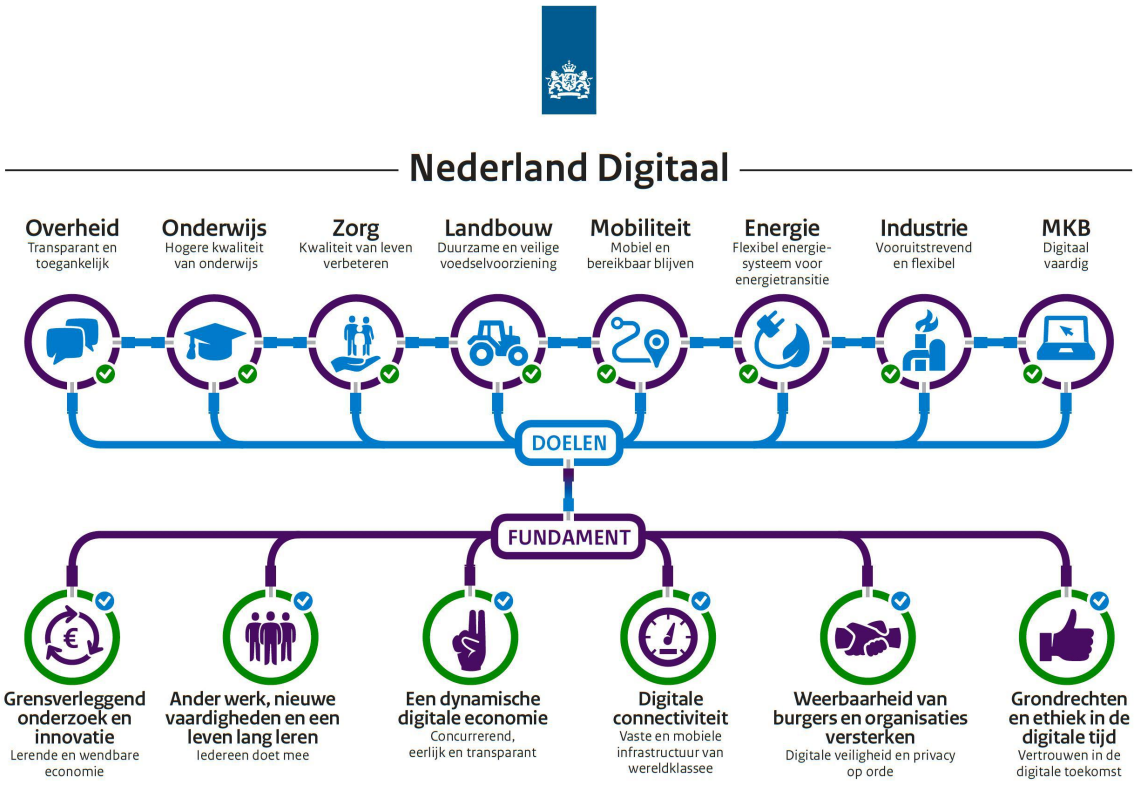
De NCSA wordt geïmplementeerd met aanvullende middelen van M€95, die voor een belangrijk deel worden gebruik voor het versterken van het NCSC, de veiligheidsdiensten en politie. Ook is een Digital Trust Center opgericht ter ondersteuning van het MKB. Het DTC stimuleert een landelijk netwerk van publiek/private weerbaarheidscentra. De NCSA wordt ondersteund door een actuele Nationale Cybersecurity Research Agenda, met daaraan gekoppelde onderzoeksgelden.

Consequentie:

- De strategie heeft vooral landelijke impact, met uitstraling naar de provincies, maar is niet afgestemd op specifieke aspecten van de Zuid-Hollandse economie, tenzij deze behoren tot bedrijven en diensten met een erkend nationaal belang.
- De aandacht voor weerbare digitale infrastructuur ondersteunt zeker ook de provincie en haar digitaliseringsinitiatieven.
- Aangezien de politie en het OM nationaal is opgehangen profiteert de provincie n regio mee met de extra investeringen in de aanpak van cyber crime.
- Dit geldt ook voor de ambities op het gebied van cybersecuritykennisontwikkeling. Juist omdat veel activiteiten in Zuid-Holland plaatsvinden (Dcypher, HSD, Universiteiten) profiteert Zuid-Holland en met name de Haagse regio wellicht extra.

Nederlandse digitaliseringsstrategie.[xcvii] De scope van de Nederlandse Digitaliseringsstrategie is breed: van digitalisering in domeinen als agro en zorg tot het overheidsdomein, van digitale vaardigheden tot cybersecurity. En van grensverleggend onderzoek tot ethische vraagstukken. In 2019 is de NDS geactualiseerd en heeft het kabinet aangegeven welke thema's en acties in 2020 prioritair zijn. Dat zijn: 1. Artificiële Intelligentie 2. Data delen en -toegang 3. Digitale vaardigheden en inclusie 4. Digitale overheid 5. Digitale connectiviteit 6. Digitale weerbaarheid.

De digitaliseringsstrategie onderkent dat extra stappen nodig zijn voor digitale weerbaarheid. Het richt zich op het versterken van toezicht en interventiemogelijkheden voor vitale infrastructuur, inbegrepen telecom netwerken. Omdat 100% veiligheid niet mogelijk is, wordt in de komende periode de oefenagenda verder ingevuld. Er is gestart met een bewustwordingscampagne voor IoT apparaten, ook voor de burger. Er is een roadmap Digitaal Veilige Hard- en Software opgesteld met daarin aangepast inkoopbeleid ICT voor de overheid. Daarnaast stimuleert de strategie het uitwisselen van informatie tussen publieke en private organisaties voor vitale en via het DTC voor niet vitale organisaties. Tot slot vraagt ze aandacht voor bescherming van persoonsgegevens.



De digitaliseringsstrategie stimuleert digitaliseringsinnovaties via publiek-private *living labs* en proeftuinen. Voor dit ICT-onderzoek en innovaties zijn per jaar rond de M€300 overheidsgeld beschikbaar. Er wordt geen specificatie gegeven voor cybersecurity-activiteiten. De provincie Zuid-Holland kent vele van dergelijke innovatie initiatieven voor digitalisering, zoals benoemd in deze nationale strategie[xcviii]:

Bennekom/Leidschendam - Connect2Trust | Cyberweerbaarheidsnetwerk
Delft - DigiShape | Data benutten
Delft - Do IoT Fieldlab | 5G Fieldlab
Delft - Dutch Optics Centre | Smart Industry Fieldlab
Delft - Fieldlab UPPS (Ultra Personalized Products and Services) | Smart Industry Fieldlab
Delft - Geronimo AI | Digitale overheid
Delft - RoboHouse | Smart Industry Fieldlab
Delft - SAM|XL | Smart Industry Fieldlab
Delft - Stichting RoboValley | Artificiële intelligentie

Den Haag - 5G netwerk Den Haag | 5G Fieldlab
Den Haag - Digital Factory For Composites | Smart Industry Fieldlab
Den Haag - HI Cybersecurity Network | Cyberweerbaarheidsnetwerk
Den Haag - NIDV Cyberweerbaarheid DVI | Cyberweerbaarheidsnetwerk
Den Haag - Smart Industry Hub West, SMITZH | Smart Industry Hub
Dordrecht - Duurzaamheidsfabriek | Smart Industry Fieldlab
Rotterdam - BlockLab | Smart Industry Fieldlab
Rotterdam - Dutch Growth Factory | Smart Industry Fieldlab
Rotterdam - FERM | Cyberweerbaarheidsnetwerk
Rotterdam - RAMLAB | Smart Industry Fieldlab
Vondelingenplaat - Industrial 5G Fieldlab Shell Pernis | 5G Fieldlab
Zoetermeer - Big Data Innovatiehub | Big Data Hub
Zwijndrecht - Cyber Netwerk Drechtsteden | Cyberweerbaarheidsnetwerk

Consequenties:

- Zuid-Holland profiteert van de digitaliseringsstrategie ook door aanwezigheid van veel initiatieven in de provincie.
- Er ligt een kans voor het regionale cybersecuritycluster rondom HSD om bij te dragen aan *security-by-design*-oplossingen in al deze initiatieven.
- Subsidieverleners inb. de Provincie Zuid-Holland zouden moeten vereisen dat digitalisering 'secure by design' in de innovatie inbedt.

Topsectorenbeleid. De overheid stimuleert reeds geruime tijd 9 topsectoren in haar innovaties: agri&food; chemie; creatieve industrie; energie; hightech systemen en materialen; logistiek; Life Science & Health; Tuinbouw; Water & Maritiem. Er was geen sprake van een separate Topsector ICT of cybersecurity, omdat deze 'horizontale' capaciteiten van belang zijn voor alle topsectoren. Dat is per 1 januari 2020 veranderd; ICT krijgt dezelfde aandacht als een Topsector. De governance van die sector wordt ondersteund door Dutch Digital Delta (DDD)[xcix]. Team DDD identificeert, prioriteert en organiseert digitaal onderzoek & innovatie en creëert ecosystemen waarmee maatschappelijke en economisch vraagstukken aangepakt worden. Zij doet dat door publieke en private partijen bijeen te brengen in innovatie-coalities met enerzijds een focus op maatschappelijke uitdagingen, anderzijds een focus op sleuteltechnologieën. Cybersecurity is een van die sleutel technologieën. Opleiden van nieuw talent, kennisdisseminatie en internationale samenwerking vormen een belangrijk onderdeel van de missie van DDD.

Consequentie:

- Vrijwel elke Topsector is terug te vinden in de provincie Zuid-Holland; een aantal van de economisch sectoren is goed ingebed in dit beleid om regionale belangen te borgen.
- DDD borgt de belangen van ICT en cybersecurity namens de Topsector ICT. Deze regio kan profiteren van het stimuleren van cybersecurity als sleuteltechnologie en het opleiden van nieuw cybersecuritytalent. Het is van belang dat de economische belangen richting DDD goed worden geborgd.

BIJLAGE C: STAAT VAN CYBERSECURITY ECONOMISCHE SECTOREN

Haven Rotterdam en de maritieme delta. De haven van Rotterdam, momenteel in omzet vierde grootste haven ter wereld is een economische motor van Nederland en de regio. De havenindustrie en logistiek en distributie is enorm afhankelijk van digitalisering. Dat neemt verder toe met de komst van 5G die slimme toepassingen mogelijk maakt. De grote fabrieken en installaties maken gebruik van Operationele Technologie (OT) die steeds vaker gekoppeld wordt aan Informatie Technologie (IT) en het internet om efficiënter te kunnen werken. Dit brengt aanvullende risico's met zich mee, omdat OT niet altijd even goed is beschermd tegen cyberaanvallen, die dan via de aan het internet gekoppelde IT worden uitgevoerd.

In 2017 en 2018 is de haven verschillende keren opgeschrikt door grootschalige cyberaanvallen op haar bedrijven, waarvan de meest bekende de NotPetya-aanval was op Möller-Maersk, moederbedrijf van APM-terminals. De terminals zijn daardoor geruime tijd gesloten geweest, hetgeen niet alleen economische impact had op het bedrijf zelf, maar ook op de klanten in de logistieke keten. Er ontstond zelfs verkeerschaos, omdat de terminal de vele containervrachtwagens niet kon ontvangen. Deze aanvallen hebben de aandacht voor cybersecurity in de havensector enorm vergroot.

De belangrijkste bedreiging voor de haven is verstoring van bedrijfsprocessen, zoals bij de NotPetya aanval van 2017. Ook is manipulatie van OT een zorg, omdat die kan leiden tot uitval van productie en tot ongevallen. Natuurlijk is het lekken van persoons- en bedrijfsgegevens voor elke organisatie een zorg.

Er zijn in de havensector na de NotPetya-aanval verschillende maatregelen genomen om herhaling te voorkomen en incident response van ondernemingen te ondersteunen.

- De haven kent eenhoofdige leiding voor digitale weerbaarheid en heeft een port Cyber Resilience Officer (CRO) aangewezen. Dit is een neventaak van de havenmeester. Hij voert die taak uit namens de Politie, Deltalinqs[c], de Gemeente Rotterdam en het Havenbedrijf. De Port CRO is verantwoordelijk voor het realiseren van het Port CRO-programma. Het doel van dit programma is om gezamenlijk de cyber resilience in de haven te verhogen, de cyber security awareness te vergroten, de geoefendheid van organisaties te intensiveren en riskmanagement op dit vlak op te bouwen. Het Port CRO-programma wordt inhoudelijk uitgevoerd door werkgroepen op de thema's Organisatie & Communicatie, Juridisch Kader, Scholing, Oefenen & Awareness en Risk Management en wordt jaarlijks geactualiseerd.
- FERM is een onderdeel van het Port Cyber Resilience Programma. Het doel van FERM is het stimuleren van samenwerking tussen bedrijven in de Rotterdamse haven en het verhogen van het bewustzijn met betrekking tot cyberrisico's om zo de best digitaal beveiligde haven ter wereld te worden. FERM is een initiatief van het havenbedrijf, de gemeente Rotterdam en Deltalinqs. FERM biedt awareness testen aan, levert een basis cyber risicoscan en organiseert thematische informatie-uitwisseling. Ook deelt men technische informatie zoals een *storage spoofing blacklist* of dreigingsinformatie met een handelingsperspectief. FERM ontwikkelt zich verder als een Cyberweerbaarheidscentrum dat ook helpt bij incident response en is als zodanig erkend door het DTC.

Veel bedrijven in de haven vallen onder de door het NCSC geïdentificeerde Aanbieders Essentiele Diensten (AED). In geval van een incident worden zij door het NCSC ondersteund. Andere bedrijven kunnen steun en advies krijgen van FERM. Uiteindelijk zullen de meeste bedrijven bij incidenten

daarnaast terugvallen op commerciële dienstverleners zoals Fox-IT om hen te helpen bij het normaliseren van de situatie. Omdat geen meldplicht bestaat voor bedrijven die geen AED-status hebben, worden succesvolle aanvallen vaker wel dan niet gemeld, waardoor er een onvoldoende beeld bestaat van de mate waarin het cyberrisico daadwerkelijk de economie bedreigt. De haven voert maatregelen in om het meldgedrag verder te verbeteren.

De horticultuur bedrijven/Greenport. De horticultuur bedrijven in het Westland en andere delen van de provincie zijn sterk gedigitaliseerde bedrijven die veel investeren in innovatie. Greenport West-Holland is een triple-helix organisatie (ondernemers, overheden en kennis/onderzoeksinstellingen) die samenwerken aan een duurzame en vitale toekomst voor het regionale glastuinbouwcluster. Men zet zich ook in voor verbetering van digitale weerbaarheid van het cluster. Kassen staan immers vol met sensoren en meet- en regelsystemen. De systemen communiceren met elkaar via het internet om optimale groei van planten en bloemen te realiseren. De glastuinbouwbedrijven, vaak in coöperaties verenigd, zijn digitaal verbonden om groenten, fruit en bloemen rechtstreeks of door tussenkomst van een veiling te verkopen aan groothandels, supermarkten en winkeliers. Transporteurs distribueren de goederen in Nederland binnen 24 uur en in 72 uur wereldwijd. Ook hier zien we een convergentie van OT en IT met alle risico's van dien. Het is een groot digitaal netwerk dat veel economische waarde vertegenwoordigt: de *value at risk* is hoog. Zelfs een korte onderbreking leidt tot significante economische verliezen.

De belangrijkste cyberbedreiging is criminele activiteit: verstoring van bedrijfsprocessen door ransomware of DDOS aanvallen. Voor de zaadveredelaars speelt ook het stelen van *Intellectual Property* (IP) een rol. Daarnaast is voor elk bedrijf verlies van persoons- of bedrijfsgegevens een issue.

De cyberrisk awareness varieert. De telersverenigingen zijn grote ondernemingen die jaarlijks risicoanalyses doen en audits ondergaan door accountantsfirma's. Het cyberrisico staat de laatste jaren steevast op de lijst van 10 belangrijkste risico's en krijgt aandacht. Er wordt nagedacht over alternatieve netwerken en datasets om continuïteit bij uitval te verzekeren. Immers, ook korte uitval leidt tot grote verliezen. De verenigingen zijn nog niet actief bezig met het risico in de *supply chain*; men stelt geen eisen aan of monitort de cybergereedheid van de toeleveranciers (tuinders) of andere ketenpartners. Ook de zaadveredelaar, multinationals die wereldwijd zakendoen, hebben de nodige aandacht voor het onderwerp en monitoren de status van hun netwerken actief.

Er is steeds meer sprake van clustering van glastuinbouwbedrijven. Er zijn van de 4000 tuinders nu zo'n 400 grotere bedrijven die een middenmanagement en IT-professionals hebben. Die grotere ondernemingen vormen globaal 80% van de omzet. Dit zal verder convergeren naar minder maar grotere bedrijven met vrijwel gelijk verbouwingsoppervlakte. Deze bedrijven worden daardoor professioneler, ook op het gebied van informatiebeveiliging. Door de besturen te maken afwegingen over digitaal risico in de bedrijfsvoering kan meer aandacht krijgen door onbekendheid met de materie.

Veel kleinere glastuinbouwbedrijven behoren tot de categorie onwetend en onbekwaam aangaande cybersecurity: het is immers niet hun *core business*. Men valt terug op de dienstverlener of leverancier van meet- en regelapparatuur, netwerken of datacenters die zo goed als mogelijk proberen de risico's technisch in te dammen. Zo ontkoppelen zij thuiscomputers, bewakingscamera's en meet- en regelnetwerken; proberen de wachtwoorddiscipline technisch te verbeteren en helpen de klant met aanvullende maatregelen.

Experts geven aan dat er wel degelijk digitale aanvallen plaatsvinden, maar dat die niet openlijk bekend worden gemaakt. In veel gevallen wordt *ransom*/losgeld betaald om de operationele bedrijfsvoering te herstellen. Er wordt weinig informatie gedeeld opdat anderen kunnen leren en mogelijke schade kunnen voorkomen.

De brancheverenigingGlastuinbouw Nederland/Westland ziet het belang van cybersecurity, maar draagt niet actief bij aan oplossingen. Het onderwerp heeft geen prioriteit en moet concurreren met energie, water en specifieke tuinbouwproblemen.

Incident response in de sector varieert. Kleinere familiebedrijven vinden het een lastig onderwerp. Om die reden loopt er een bottom-up initiatief in eerste instantie om de cyber awareness te vergroten. Een kleine groep voortrekkers (VTM, Nethgrow en Hoogendoorn) werkt samen met IQ en de Lentiz onderwijsgroep om een risicoscan bij glastuinbouwbedrijven te gaan doen. Vanuit stichting Greenport is er de wens om ook top-down te werken en een Cyberweerbaarheidscentrum te starten. Hiervoor wordt subsidie van de provincie gevraagd. Deze activiteiten zijn nog niet opgestart.

High Tech Systemen en Materialen (HTSM) industrie. Zuid-Holland kent de hoogste concentratie hightech maakbedrijven in Nederland, met meer dan 16.000 bedrijven en bijna 104.000 medewerkers.[ci] Veel van deze innovatieve bedrijven zijn verenigd in Holland Instrumentation (HI), een platform dat de samenwerking stimuleert tussen bedrijven, opleiding en onderzoek en overheden. Ook werkt en innoveert men samen op het gebied van automatisering en digitalisering bij SMITZH, Smart Manufacturing Industriële Toepassingen Zuid-Holland. Dit is een loket voor ondernemers in samenwerking met acht fieldlabs, IQ, TNO, Metropool Rotterdam Den Haag (MRDH), gemeente Den Haag en de provincie.

Hightech maakindustrie is bij uitstek een gedigitaliseerde industrietak waar het managen van cyberrisico steeds belangrijker wordt. De grootste dreiging wordt gezien in criminele activiteit (ransomware), het lekken van persoonsdata en het stelen van Intellectual Property (IP).

De industrie kent bedrijven in vrijwel alle categorieën zoals eerder genoemd, met verschillende volwassenheid van digitaal risicomanagement. Er zijn topbedrijven, zoals Airbus Defence and Space, Fokker Technologies, Damen Shipyards, die ook aan defensie leveren en onder meer daarom digitaal volwassen zijn en veel aandacht hebben voor cyberincident response. Ook Batenburg is een voorbeeld van een groot bedrijf dat niet alleen veel aandacht besteedt aan cyberweerbaarheid van de bedrijfsvoering, maar ook haar hightech producten cyberveilig maakt volgens de laatste normen voor Operationele Technologie. Er is bij een grote groep hightech maakbedrijven wel awareness voor het belang van het onderwerp, maar dit bereikt niet altijd het bestuur of wordt vertaald in concrete maatregelen. Een risicoafweging voor digitaal risico voor de bedrijfsvoering staat bij veel bedrijven nog in de kinderschoenen. Voor kleinere bedrijven is de directeur vaak de enige die besluiten neemt en ondersteuning voor risicomanagement van zijn digitale infrastructuur ontbeert.

HI heeft een subsidieaanvraag gedaan bij het DTC voor een Cyberweerbaarheids (CW)-centrum; deze aanvraag is niet goedgekeurd. Men werkt samen met een kleine groep enthousiaste bedrijven zoals HTC, Promolding, met InnovationQuarter en HSD. Dit CW-centrum HI zou moeten bijdragen aan het verbeteren van de awareness, het leveren van een risicoscan en delen van best practice, ook op het gebied van preventie en incident response. Er bestaat verschil van inzicht of een dergelijke activiteit

door de overheid gesubsidieerd moet worden of dat dit een verantwoordelijkheid van het bedrijfsleven zelf is.

Ruimte- en luchtvaartcluster. Bedrijven dit cluster zijn gewend aan kwalitatief hoogwaardige bedrijfsprocessen en hebben mede daardoor ook aandacht voor digitale risico's. Veel bedrijven leveren daarnaast ook aan defensie, die op dit gebied ook hoge standaarden vereist.
De grootste zorg van de bedrijven is het stelen van IP en daarnaast stilleggen van bedrijfsprocessen. Vooral de grotere bedrijven zijn volwassen en maken ook deel uit van een ISAC gesteund door de overheid. De kleinere bedrijven en startups zijn vaak niet volwassen en geven aan ondersteuning nodig te hebben bij incident respons. Er zijn vaak geen plannen of ze zijn niet beoefend. Grote bedrijven geven aan kleinere toeleveranciers te willen helpen vanuit het belang van het beveiligen van digitale ketens.

Medical Delta en de BioScience industrie. Medical Delta is een samenwerkingsverband tussen drie universiteiten twee universitair medische centra, vier hogescholen, overheden, bedrijven, zorginstellingen en andere partijen in Zuid-Holland. Men werkt samen in twaalf verschillende consortia aan technologische oplossingen voor duurzame zorg. Medical Delta geeft een impuls aan de life sciences & health sector in Zuid-Holland.

Een belangrijk deel van de Biotech Industrie bevindt zich in het Leiden Bio Science Park. Hier zijn bij elkaar zo'n 153 life science en health organisaties en 103 biomedische bedrijven gevestigd. De focus ligt met name op het ontwikkelen en produceren van medicijnen; ook wordt gewerkt aan biodiversiteit (o.a. Naturalis). Het park kent bedrijven van multinationals tot start-ups en organisaties gericht op onderwijs, onderzoek, musea, maar ook dienstverleners zoals hotels of horeca.[cii]

De Life- en BioScience sector is in hoge mate gedigitaliseerd en maakt gebruik van enorme datasets, veelal ook te relateren aan individuen. De toepassing van Artificial intelligence (AI) neemt sterk toe om de data beter te ontsluiten. Met deze verregaande digitalisering is er behoefte aan een goede digitale infrastructuur (netwerk, mobiel, datacenters), maar ook aan een digitaal veilige omgeving. De universitaire ziekenhuizen hebben nog aanvullende complexiteit. Zij moeten continuïteit van zorg borgen in een uiterst digitale omgeving, patiënten moeten bij hun digitale gegevens kunnen; studenten en onderzoekers moeten kunnen inloggen vanuit buiten de universiteit; onderzoeker moeten internationaal kunnen samenwerken met andere universiteiten, onderzoekscentra en bedrijven.

Als belangrijkste cyberdreiging wordt gezien het stelen van IP en het lekken van persoonsdata. Het IP is zeer waardevol, vanwege de lange ontwikkeltijd van medicijnen en vaccinaties en grote investeringen in onderzoek. Daarnaast is de sector mogelijk doelwit van criminele activiteit, zoals ransomware aanvallen.

De sector kent alle vormen van volwassenheid van digitaal risicomanagement. De grote multinationals zijn gereguleerde, vaak in het buitenland beursgenoteerde ondernemingen waar strenge beveiligingsmaatregelen vaak vanuit het hoofdkantoor worden genomen. Ook de grote academische ziekenhuizen hebben de nodige aandacht voor digitale weerbaarheid, maar tegelijkertijd een zeer complexe ICT-architectuur. Bij een groep middelgrote ondernemingen, opleidings- en onderzoeksinstellingen wordt er zeker gewerkt aan digitale veiligheid, maar bereikt aandacht voor digitaal risicomanagement niet altijd het bestuur. Incident response wordt in veel gevallen ad hoc geregeld. Tot slot is er een groep kleiner MKB waaronder startups voor wie aandacht voor IT en cybersecurity in de bedrijfsvoering op een laag peil staat, ondanks dat men het risico wel begrijpt. Die groep bedrijven vraagt om ondersteuning.

Voor de zorg bestaat stichting Z-CERT[ciii], een expertisecentrum voor cybersecurity. Z-CERT heeft specifieke kennis van medische hard- en software en ondersteunt zorginstellingen bij een digitaal incident en vergroot daarmee de weerbaarheid van de medische sector. Het levert diensten op het gebied van dreigingsinformatie, kennisdeling en advies, monitoring IP-adressen, afhandeling en coördinatie van incidenten en werkt aan ontsluiten van digitale kwetsbaarheden in software.

De onderwijs en onderzoeksinstellingen werken op het gebied van cybersecurity samen in SURFnet en maken gebruik van een gezamenlijke CERT-organisatie voor incident response. De recente hack bij de Universiteit van Maastricht heeft aangetoond dat dit geen vrijwaring is voor cyberincidenten.

Een belangrijk deel van de MKB-bedrijven in de Medische en Biotech sector worden echter niet bereikt, kampen met een lage awareness, beperkte kennis van risicomanagement en grote afhankelijkheid van leveranciers. Kennis van leveranciersmanagement voor IT- en cyberdiensten ontbreekt veelal.

Industrie voor defensie en veiligheid. Zuid-Holland kent een groot aantal producenten van uitrusting voor defensie- en veiligheidsdoeleinden. Dit betreft onder meer schepen (o.a. Damen Shipyards), communicatieapparatuur, drones en vliegtuigonderdelen (o.a. Fokker, Airbus) ook cybersecuritydienstverlening (crypto apparatuur en sleutels). Om producten of diensten aan defensie te kunnen leveren moeten bedrijven voldoen aan de Algemene Beveiligingseisen Defensie Opdrachten (ABDO). De versie 2019 vereist uitgebreide cybersecuritymaatregelen waaraan bedrijven moeten voldoen om vooral spionage te voorkomen. Deze verplichting geldt ook voor de toeleveranciers van de bedrijven die als hoofdaannemer een contract hebben gewonnen. Bij de aanbesteding moet bewijsvoering voor het voldoen aan ABDO worden overlegd. Ook NAVO-contracten vereisen deze strenge toelatingsvoorwaarden, die overigens net als bij defensiecontracten door de MIVD worden beoordeeld. Mocht een bedrijf voor de EU, bijvoorbeeld European Space Agency willen werken, waarbij gerubriceerde informatie moet worden gebruikt, dan verzorgt de AIVD *clearance* van zowel de individuen als het bedrijf.

Als gevolg van deze maatregelen heeft de defensie- en veiligheidsindustrie een hoge standaard voor cybersecurity en digitale weerbaarheid. Het is immers gewoon een verplichting om contracten te kunnen winnen. Men voert risicoanalyses uit op basis waarvan de nodige maatregelen worden genomen. De uitvoering wordt gecontroleerd bij aanbestedingen. Daarom is over het algemeen ook incident response op orde. De bedrijven hebben een gedegen veiligheidscultuur; het is geen financiële afweging om maatregelen te nemen, maar een voorwaarde.

Voor kleinere toeleveranciers van defensiebedrijven en startups is voldoen aan ABDO wel een uitdaging; men heeft geen keus. Wil een bedrijf defensie als klant, dan moet het meer inspanning doen om de beveiliging, fysiek en digitaal op orde te hebben. Doet een bedrijf dat, dan is er een nieuwe markt beschikbaar. Anderzijds is het moeilijker voor defensie om toegang te krijgen tot innovaties van jonge startups. Die hebben vaak niet de energie om aan de strakke vereisten te voldoen.

Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV) heeft via het DTC een subsidie ontvangen om een ABDO-register op te zetten. Dit register bevat alle bedrijven, ook toeleveranciers, die aan de ABDO-verplichting voldoen en dus een hoge mate van cyberweerbaarheid hebben. Een dergelijk register helpt de defensie-industrie haar toeleveranciers te vinden waarvan ze redelijk zeker zijn dat die aan de ABDO-verplichting voldoen. Via het register heeft de toeleverancier meer kans op toekomstige

contracten. NIDV overweegt in de toekomst wellicht een certificering in te voeren, maar regelgeving van de overheid staat dit momenteel in de weg.

Telecom en digitale dienstverlening. Een digitale dienstverlener, een *Digital Service Provider* (DSP), is een rechtspersoon die een of meer van de volgende diensten levert: een online marktplaats, een clouddienst of een zoekmachine. Men valt onder de Wbni als het bedrijf heeft een hoofdvestiging of vertegenwoordiging in Nederland heeft, 50 of meer medewerkers, heeft en het balanstotaal of de jaaromzet meer is dan € 10 miljoen. In die gevallen heeft het bedrijf zorgplicht om zich te beveiligen tegen cybercriminaliteit en voorkomen dat de netwerksystemen en informatiesystemen beschadigd raken. Ook hebben deze bedrijven meldplicht bij cybercriminaliteit bij het NCSC, het Agentschap Telecom voor essentiële dienstverleners en het CSIRT-DSP van het ministerie van EZK voor digitale dienstverleners.

De digitale dienstverleners, met name de grotere DSPs hebben uitgebreide en moderne cybersecurityteams om de dagelijkse risico's maar ook crises tegemoet te komen. Cyberincidenten zijn dagelijkse kost. Vaak leveren ze ook cyberdiensten aan haar klanten.

BIJLAGE D: BEST PRACTICE CYBERSECURITYCENTRUM

In het netwerk van het Digital Trust Center zitten verschillende interessante voorbeelden van opstartende cybersecurity- of cyberweerbaarheidscentra. Op basis van literatuurstudie en gesprekken met onder andere vertegenwoordigers van FERM, Cyberweerbaarheidscentrum Brainport, Cybersecurity Centrum Maakindustrie zijn een aantal *best practices* vast te stellen. Als hulp bij verdere ontwikkeling worden deze in deze bijlage besproken.

Ervaring met andere centra in het land en een recent onderzoek van de Haagse Hogeschool over *best practices* voor het delen van cyberinformatie [civ] leert het volgende:

- Zorg voor een businessplan van een cyber centrum dat ook zonder subsidies kan werken.
- Ga uit van een groeimodel: de ambitie past bij de beschikbare middelen; win vertrouwen en groei gestaag verder. Het Cybersecurity Centrum Maakindustrie toont aan dat je al kan starten met 0,4 fte en een beperkt budget.
- Kies een tarievenstructuur die past bij de sector: lidmaatschap met basisdiensten en/of pay-per-use diensten; grote bedrijven betalen meer dan kleine; werk aan sponsoring van grote bedrijven die belang hebben bij een veilige keten.
- Expertise van de deelnemers en relevante kennis van de bedrijfstak is nodig; daarom heeft sectorale aanpak met kennis van de sector en ketens de voorkeur.
- Streef ernaar geaccrediteerd te worden als informatiepunt door NCSC; de informatie uit het Nationaal Detectie Netwerk is van grote toegevoegde waarde. Dit stelt overigens eisen aan de organisatievorm.
- Onderling vertrouwen – hoe groter en meer divers de groep is, hoe lastiger de samenwerking.
- Structurele opzet – zorg voor een kleine vaste kern, werkgroepen met regelmatige, vaste schema's en thematisch samenwerkingsbijeenkomsten; de grootste waarde is de inbreng van bedrijven.
- Sluit aan bij bestaande structuren en bestaande netwerken; lift mee op administratieve organisatie van die organisaties.
- Lidmaatschapeisen: stel eisen – onder andere aan eigen inbreng, ook in kennis en kunde. Hierbij geldt ook vertrouwelijk omgaan met de verkregen data.
- Leiderschap: zorg dat een centrum gesteund en uitgedragen wordt door invloedrijke senior executives in de sector; kies niet alleen voor expertgroepen; maar ook voor een samenwerkingsvorm die gericht is op bestuurders en bedrijfsleiding.

Taken die een cybersecuritycentrum op zich kan nemen, in volgorde van prioriteit; indicatieve kosten ($-$$$$)

- Risicoscan voor bedrijven - $
- Awareness trainingen voor bestuur en bedrijfsleiding - $$
- Kennisdeling sessies met experts - $
- Awareness trainingen voor personeel - $$
- Uitgeven informatiebulletins (best practice; kwetsbaarheden in producten; cyberdreiging) specifiek voor sector - $$
- Basis *Cyber Security Incident Response Team* (CSIRT) functie (helpdesk voor eerste hulp, bij voorkeur 24/7) - $$/$$$

- *Information Sharing & Analysis Center* (ISAC) functies, voor bedrijven die zelf informatie kunnen inbrengen; waardevol na accreditatie door NCSC zodat informatie uit het Nationaal Detectie Netwerk beschikbaar komt - $$$
- Gezamenlijke inkoop van cyberdiensten; evaluatie van producten; due diligence - $$
- Gezamenlijk opzetten van cybercrisis oefeningen voor de sector - $$
- Gezamenlijke *Security Operations Center* (SOC) functie (team van experts dat netwerken 24/7 monitort) - $$$
- *Cyber Security Incident Response Team* (CSIRT)/*Computer Emergency Response Team* (CERT); deze functie vergt een team van hoogwaardige specialisten die de sectorale architecturen goed begrijpen en als brandweer optreden (eerste hulp bij cyberaanval). Een mobiel team heeft speciale apparatuur nodig om systemen door te kunnen lichten. - $$$$

Over de auteur:
Koen Gijsbers heeft zich na een langdurige operationele carrière bij defensie toegelegd op digitale vraagstukken. Zo was hij initiator van de eerste Defensie Cyber Strategie (2012) als CIO van het Ministerie van Defensie en heeft hij het agentschap van de NAVO geleid dat verantwoordelijk was voor het ontwikkelen, in dienst houden en beveiligen van de netwerken en informatietechnologie voor de hoofdkwartieren en voor militaire operaties van de Alliantie. Vanaf 2017 helpt hij start- en scaleups in cybersecurity, traint hij boards en adviseert hij overheden en bedrijven.

ENDNOTES

[i] Lees meer hierover: Nationaal Cybersecurity Centrum: Cybersecuritybeeld 2019. Den Haag, juni 2019
[ii] Ontwikkeld met toestemming van Hathaway Global Strategies LLC.
[iii] Cyber Readiness Index 2.0 - a Plan for Cyber Readiness: a Baseline and an Index, Potomac Institute for Policy Studies, Arlington, Va, USA, November 2015.
[iv] Provincie Zuid-Holland: Begroting 2020. Vastgesteld door Provinciale Staten op 13-11-2019 door Provinciale Staten.
[v] Zo is er landelijk de directeur cybersecurity bij het NCTV, in de haven van Rotterdam de cyber resilience officer (havenmeester) en bij grotere gemeenten een Chief Information Security Officer.
[vi] Besluit Risico Zware Ongevallen. https://brzo.nu/wat-is-een-brzo-bedrijf/
[vii] Centraal Planbureau: Risicorapportage cyberveiligheid 2019. Blz 37 en 38, para 4.5.3 Risico's van een decentrale aanpak. Den Haag, 17 oktober 2019, https://www.cpb.nl/risicorapportage-cyberveiligheid-2019#docid-160018
[viii] Den Haag: Staat van de Stad 2020.
https://denhaag.raadsinformatie.nl/document/9006849/1/RIS305530_Bijlage
[ix] Den Haag: Strategisch Beleidskader Informatieveiligheid Gemeente Den Haag 2019-2022.
https://denhaag.raadsinformatie.nl/document/8308173/1/RIS304162_Bijlage
[x] Den Haag: Den Haag Resilience Strategie 2019.
https://denhaag.raadsinformatie.nl/document/7613029/1/RIS302023_bijlage_Den_Haag_Resilience_Strategie
[xi] Gemeente Den Haag: Integraal Veiligheidsplan Den Haag 2019-2022.
https://denhaag.raadsinformatie.nl/document/7515618/1/20190404-RIS301821_GEAMENDEERD_BIJLAGE_Integraal_Veiligheidsplan
[xii] Gemeente Rotterdam: begroting 2020.
https://www.watdoetdegemeente.rotterdam.nl/begroting2020/programmas/openbare-orde-en-veilighe/opnebare-orde-en-veilighe/
[xiii] Zie: https://www.economicboardzuidholland.nl/wat-doet-ebz/
[xiv] Nationaal Cybersecurity Centrum: Cybersecuritybeeld 2019. Den Haag, juni 2019
[xv] NIST Cybersecurity Framework (US National Institute of Standards and Technology)
[xvi] ISIDOOR: cyber oefening georganiseerd door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) met ruim 200 spelers uit de private en publieke sector.
[xvii] De Algemene Verordening Gegevensbescherming is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
[xviii] Notté, van 't Hoff – de Goede, Leukfeldt: Cybersecurity in de metaalsector. De ontwikkeling van een praktisch cybersecurity risicomodel voor het MKB in de metaalsector. Den Haag, Mei 2019.
[xix] M. Hathaway et all: The Netherlands Cyber Readiness at a glance, pagina 20. Arlington, VA, 2017
[xx] Secondant: 'Er gebeurt zoveel, dat kan de politie nauwelijks bijbenen'. Utrecht, 19-08-2019.
https://hetccv.nl/nieuws/secondant-er-gebeurt-zoveel-dat-kan-de-politie-nauwelijks-bijbenen/
[xxi] Security.nl. Utrecht, 13 maart 2020.
https://www.security.nl/posting/647924/Eerste+Nederlandse+cyberdriehoek+bespreekt+impact+cybercrime
[xxii] Bureau Boekhoorn Sociaal Wetenschappelijk Onderzoek: De aanpak van cybercrime door regionale eenheden van de politie – van intake van cybercrime naar opsporing en vervolging. Nijmegen, oktober 2019
[xxiii] Zie Wbni, hoofdstuk 5. https://wetten.overheid.nl/BWBR0041515/2020-07-15
[xxiv] Zie: https://www.digitaltrustcenter.nl
[xxv] NCSC, Nationaal Detectie Netwerk – Nederland samen digitaal veilig. Publicatie-nr. 113593. Den Haag, juli 2018.
[xxvi] Zie: https://www.misp-project.org
[xxvii] Zie NCSC: Start een ISAC: handreiking Sectoraal samenwerken. Den Haag, oktober 2018.
[xxviii] Overigens is vanwege COVID-19 middels een tijdelijke wet de zorgsector als essentiële dienst aangewezen.
[xxix] Naast Z-CERT en SURF zijn dat CERT-Watermanagement (Waterschappen) en de Informatie Beveiligingsdienst IBD-CERT (gemeenten)
[xxx] Zie: https://www.connect2trust.nl
[xxxi] Zie: https://www.risklens.com/cyber-risk-management

[xxxii] In de VS is dit meer gemeengoed. Zo werkt het FAIR Institute samen met universiteiten en het bedrijfsleven aan dit onderwerp met als missie: *Establish and promote risk management best practices that empower risk professionals to collaborate with their business partners on achieving the right balance between protecting the organization and running the business.* https://www.fairinstitute.org

[xxxiii] "Tijd voor een Deltaplan Cyber Security", Inge Bryan en Bibi van den Berg, 2019, https://www.deloitteforward.nl/cyber-security/tijd-voor-een-deltaplan-cyber-security/

[xxxiv] Een uitgebreide arbeidsmarktanalyse is te vinden in de Human capital Agenda Security (2019-2022), https://www.thehaguesecuritydelta.com/news/newsitem/1283-launched-human-capital-agenda-security-2019-2022; De laatste trends in vacatures zijn te zien op securitytalent.nl, https://securitytalent.nl/career/dashboard

[xxxv] Zie: Human Capital Agenda Security, pag. 24.

[xxxvi] https://www.dcypher.nl/sites/default/files/uploads/documents/NCSEA.pdf

[xxxvii] Zie: dcypher: landkaart cybersecurity hoger onderwijs. https://www.dcypher.nl/landkaart-cybersecurity-hoger-onderwijs

[xxxviii] https://online-learning.tudelft.nl/courses/cybersecurity-for-managers-and-executives/

[xxxix] Zie: https://www.summerschoolcybersecurity.org

[xl] https://securitytalent.nl/education

[xli] https://www.economicboardzuidholland.nl/projecten-hca/

[xlii] Binnen iFlow worden hoger opgeleiden met uiteenlopende achtergronden binnen een jaar omgeschoold tot ICT'er voor het Rijk. Op dit moment lopen de voorbereidingen voor een eerste pilot met de Hogeschool van Amsterdam en de Haagse Hogeschool. Tijdens de pilot, die in februari van start gaat, krijgen de studenten de eerste vijf maanden intensief les in Software Engineering, Cyber Security of Business Analystics. Hierna volgt een inwerkperiode van zes maanden en gaan de nieuwe ICT'ers een dag per week naar school om hun kennis toe te spitsen op hun specifieke vakgebied. https://www.ubrijk.nl/actueel/nieuws/2017/10/31/project-iflow-aan-de-slag-op-ict-gebied-bij-het-rijk

[xliii] https://cyberwerf.nl

[xliv] Zie: https://www.lentiz.nl/mbo-westland/digitale-gevaren-worden-getackeld-door-studenten-horti-technics-management-en-bedrijfsleven-in-de-tuinbouw/

[xlv] Platform voor Informatiebeveiliging: beroepsprofielen Informatiebeveiliging 2.0. 1 januari 2017. https://www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging

[xlvi] NCSC Certified Training. https://www.ncsc.gov.uk/information/certified-training

[xlvii] Video of life stream lessons learned cyber attack symposium Maastricht University. https://www.youtube.com/watch?v=ik-ZVvZ2-xU

[xlviii] Een voorbeeld: https://www.mycyberhygiene.com is een gratis generieke cursus gemaakt door een bedrijf uit Estland; is ook in het Nederlands beschikbaar. https://e-estonia.com/free-cyber-hygiene-training-in-12-languages/

[xlix] Cyber Central (Rotterdam) is een initiatief van KPN Security Services, Cisco en McAfee. Cyber Central wil cybersecurity weer 'gewoon' maken en richt zich met name op MKB. https://www.cybercentral.nl

[l] Regeerakkoord kabinet Rutte III: Vertrouwen in de Toekomst. https://www.rijksoverheid.nl/regering/regeerakkoord-vertrouwen-in-de-toekomst/2.-zekerheid-en-kansen-in-een-nieuwe-economie/2.4-economie-innovatiebeleid-en-vestigingsklimaat

[li] Miljoenennota 2020-2021. Tweede Kamer, vergaderjaar 2020-2021, 35 570, nr. 1, pg. 44 - 45

[lii] Dcypher, NCSRA III. Den Haag, 2018. https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf

[liii] https://www.dcypher.nl

[liv] KIA Veiligheid, oktober 2019. https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/KIA%20Veiligheid%20-%2020191015%20definitief_0.pdf

[lv] Ministerie van Economische Zaken en Klimaat, kamerbrief: Resultaten verkenning en vervolgaanpak cybersecurity kennisontwikkeling en innovatie. Den Haag, 9 april 2020. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/04/09/kamerbrief-over-resultaten-verkenningen-en-vervolgaanpak-cybersecurity-kennisontwikkeling-en-innovatie

[lvi] TNO-rapport | TNO 2019 R10769 – Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity

[lvii] The Third Industrial Revolution Consulting Group LLC: TIR Roadmap Next Economy. Bethesda, MD, USA, 4 november 2016.
[lviii] Zie: https://www.thehaguesecuritydelta.com
[lix] Policy Research Corporation: Ontwikkeling veiligheidscluster HSD. Rotterdam, 16 februari 2016. https://www.thehaguesecuritydelta.com/media/com_hsd/report/84/document/Policy-Research-Ontwikkeling-veiligheidscluster-HSD-Rapport-DEF-16-02-2016.pdf
[lx] Policy Research Corporation: Update 2016 veiligheidscluster HSD. Rotterdam, 3 februari 2017. https://www.thehaguesecuritydelta.com/media/com_hsd/report/130/document/Policy-Research-Update-2016-veiligheidscluster-HSD-Rapport-DEF.pdf
[lxi] Zie: https://www.innovationquarter.nl
[lxii] ZieL https://www.innovationquarter.nl/item/dutch-security-techfund/
[lxiii] De *Defense Innovation Unit Experimental (DIUx)* van de Amerikaanse krijgsmacht heeft een proces ontwikkeld waarbij startups binnen 6 weken een contract kunnen krijgen bij de US Defensie; bij succes kan onbeperkt worden opgeschaald, zonder nieuwe aanbesteding.
[lxiv] Zie MinBuZa: factsheet cyberdiplomatie
[lxv] Zie MinBuZa: Digitale Agenda voor Buitenlandse Handel en Ontwikkelingssamenwerking.
[lxvi] Startup Delta is een overkoepelende stichting om de belangen van startups en innovatie te borgen; Innovatie Quarter is een van hun 8 partners. http://www.startupdelta.org/faq/what-is-startupdelta/
[lxvii] WRR, Den Haag 2019. Voorbereiding op digitale ontwrichting.
[lxviii] NCTV, Den Haag, februari 2020. Nationaal Crisisplan Digitaal.
[lxix] Het CSIRT-DSP heeft als taak om meldingen van incidenten bij digitale dienstverleners te ontvangen met het doel om de economische en eventueel maatschappelijke schade van een incident te beperken. Het CSIRT-DSP kan eventueel ook andere digitale dienstverleners waarschuwen als er zich een bepaald type incident voordoet. Verder deelt het CSIRT-DSP actuele dreigingsinformatie. https://www.csirtdsp.nl
[lxx] Berenschot Groep B.V., Utrecht, 1 mei 2020. Deel 1 en deel 2.
[lxxi] Als voorbeeld: Regionaal Crisisplan Haaglanden 2019 - 2023, vastgesteld op 30 januari 2019 benoemd de cyber- of digitale crisis niet; de crisisorganisatie gaat uit van 'plaats Incident' wat bij cybercrisis niet altijd relevant is. Is dat het bedrijf waar uitval is, het datacentrum, of het netwerk control centrum van de digitale dienstverlener?
[lxxii] Als voorbeeld: Regionaal Crisisplan Haaglanden 2019 - 2023, vastgesteld op 30 januari 2019 benoemd de cyber- of digitale crisis niet; de crisisorganisatie gaat uit van een fysieke 'Plaats Incident' wat bij cybercrisis niet altijd relevant is. Is dat het bedrijf waar uitval is, het datacentrum, of het netwerk control centrum van de digitale dienstverlener?
[lxxiii] https://www.security.nl/posting/670739/Veiligheidsregio+Noord-+en+Oost-Gelderland+getroffen+door+ransomware
[lxxiv] Instituut Fysieke Veiligheid, Cyberrisico's en veiligheidsregio's – Hoe beoordelen veiligheidsregio's cyberrisico's. Arnhem, februari 2020. https://www.ifv.nl/kennisplein/Documents/20200228-IFV-Factsheet-Cyberrisicos-en-veiligheidsregios.pdf
[lxxv] Zie: https://www.surf.nl/ozon-oefen-hoe-je-bij-een-cybercrisis-reageert/whitepaper-cybercrisisoefening-ozon?dst=n1242
[lxxvi] Zie: https://ferm-rotterdam.nl/nl/nieuws/cybernautics-2019-veiligheidsregio-rotterdam-rijnmond-en-divisie-havenmeester-rotterdam
[lxxvii] Zie: https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cybercriminaliteit-kost-nederlandse-organisaties-10-miljard-euro-per-jaar.html
[lxxviii] Ponemon Institute: Cost of Cybercrime – ninth annual cost of cybercrime study. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
[lxxix] Centraal Bureau voor de Statistiek: Cybersecuritymonitor 2019. https://www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019
[lxxx] http://www.seo.nl/pagina/article/economische-kansen-nederlandse-cybersecurity-sector/
[lxxxi] Centraal Plan Bureau: Risicorapportage cyberveiligheid 2019, p. 37. Den Haag, oktober 2019. https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf

[lxxxii] Haagse Hogeschool, Centre of Expertise Cybersecurity, Lectoraat Cybersecurity in het mkb: Cybersecurity in de metaalsector – de ontwikkeling van een praktische cybersecurity risicomodel voor midden- en kleinbedrijf in de metaalsector. Notté, van 't Hoff-de Goede en Leukfeldt. Den Haag mei 2019
[lxxxiii] https://cwbrainport.nl
[lxxxiv] https://ferm-rotterdam.nl
[lxxxv] https://cybersecuritymaakindustrie.nl/nl/
[lxxxvi] https://www.connect2trust.nl
[lxxxvii] Het DTC stimuleert het landelijk dekkend netwerk: Lijst met huidige initiatieven. https://www.digitaltrustcenter.nl/samenwerkingsverbanden
[lxxxviii] https://www.tno.nl/nl/over-tno/nieuws/2019/10/consortium-automated-security-van-start/
[lxxxix] WRR: Voorbereiden op digitale ontwrichting. Den Haag, 2019.
[xc] TNO-rapport | TNO 2019 R10769 – Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity
[xci] World Economic Forum: We must treat cybersecurity as a public good. Here's why. Geneva, 22 Aug 2019. https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/
[xcii] Marcel Pfeiffer: Op het gebied van cybersecurity mag de rol van de overheid wel wat groter worden. Financieel Dagblad, 27 sep 17. https://fd.nl/opinie/1220206/op-gebied-van-cybersecurity-mag-rol-van-overheid-wel-wat-groter-worden
[xciii] Wet beveiliging netwerk- en informatiesystemen van 17 oktober 2018, geldend van 15 juli 2020. https://wetten.overheid.nl/BWBR0041515/2020-07-15#Hoofdstuk4_Paragraaf1_Artikel5
[xciv] Ministerie van Binnenlandse Zaken en Koninkrijkstaken: Baseline Informatiebeveiliging Overheid. Den Haag, 2019
[xcv] Ministerie van J&V: Nationale Cyberstrategie: van bewust naar bekwaam. Den Haag, 2013
[xcvi] Ministerie van J&V: Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig. Den Haag, 2018
[xcvii] Ministerie van Economische Zaken en Klimaat: Nederlandse Digitaliseringsstrategie. Den Haag, juli 2020
[xcviii] Overigens is deze lijst niet compleet en zijn er meer van dergelijke initiatieven, zoals Yes!Delft, Unmanned Valley Valkenburg, Living Lab Scheveningen (IoT), Smart City Dordrecht of Living Lab Sensibel Sensor Rotterdam.
[xcix] Voor informatie: https://dutchdigitaldelta.nl
[c] Deltalinqs behartigt de gezamenlijke belangen van meer dan 95% van alle logistieke, haven- en industriële bedrijven in de mainport Rotterdam. Bij de ondernemersvereniging zijn ruim 700 bedrijven aangesloten uit veertien verschillende sectoren. Samen dragen zij 6,2% bij aan het Bruto Nationaal Product van Nederland en bieden zij direct en indirect werk aan ruim 385.000 mensen. Deltalinqs helpt ook bij security en veiligheid, inbegrepen cybersecurity.
[ci] Bron: https://www.innovationquarter.nl/htsm/
[cii] Bron: https://leidenbiosciencepark.nl/the-park
[ciii] Zie: https://www.z-cert.nl
[civ] https://www.ncsc.nl/onderzoek/onderzoeksresultaten/succesfactoren-voor-het-delen-van-cybersecurity-informatie