

Policy Research Corporation



Security Delta

Eindrapport



13 februari 2013

In opdracht van Gemeente Den Haag, HSD

© *Policy Research Corporation*

Copyright 2014

Kantoor Nederland:

Parklaan 40

3016 BC Rotterdam

tel: +31 10 436 03 64

fax: +31 10 436 14 16

e-mail : info@policyresearch.nl

website : www.policyresearch.nl

Kantoor België:

Jan Moorkensstraat 68

2600 Antwerpen

tel : +32 3 286 94 94

fax : +32 3 286 94 96

e-mail : info@policyresearch.be

website : www.policyresearch.be

Dit rapport waarop het auteursrecht van toepassing is, is bestemd voor eigen gebruik door de geadresseerde. Elke vorm van gebruik door derden van dit rapport, volledig of gedeeltelijk, vergt een voorafgaande schriftelijke toestemming van Gemeente Den Haag / HSD.

INHOUDSOPGAVE

TEN GELEIDE	ii
I. FOTO SECURITY DELTA	1
I.1. METHODOLOGIE	1
I.2. FOTO VEILIGHEIDSSECTOR 2012.....	2
I.2.1. Omvang en economische betekenis Regio Den Haag.....	2
I.2.2. Omvang en economische betekenis Nederland.....	3
I.2.3. Omvang en economische betekenis wereldwijd.....	4
II. FORESIGHT SECURITY DELTA.....	5
II.1. TRENDS EN ONTWIKKELINGEN	5
II.1.1. National security	6
II.1.2. Cyber security.....	7
II.1.3. Critical infrastructure	8
II.1.4. Urban security.....	8
II.1.5. Forensics	9
II.1.6. Education & Research.....	10
II.2. FORESIGHT VEILIGHEIDSSECTOR 2020.....	10
II.2.1. Groeiverwachting Regio Den Haag	10
II.2.2. Groeiverwachting Nederland	11
II.2.3. Groeiverwachting Europa en wereldwijd.....	11
III. STAPPEN VOORUIT.....	13
III.1. AMBITIE	13
III.2. NODIGE KWALITEITEN VOOR CLUSTERONTWIKKELING	14
III.3. EVALUATIE SECURITY DELTA VANDAAG	21
III.4. ACTIES VOOR EEN STERKE(RE) SECURITY DELTA.....	22
REFERENTIES	24
GECONTACTEERDE PERSONEN	27
BIJLAGE.....	29

TEN GELEIDE

Veiligheid is meer en meer een (complex) issue. Er is een evolutie van traditionele veiligheid (particuliere beveiliging, brandbeveiliging enz.) naar nieuwe veiligheid (terrorisme, cyber, natuurrampen enz.) en naast fysieke veiligheid zijn ook virtuele en data veiligheid key geworden. De veiligheidsdreigingen zijn met elkaar verbonden en kunnen niet geïsoleerd of puur politoneel-militair aangepakt worden. Een geïntegreerd beleid en strategie met inzet van verschillende instrumenten is vereist om een effectieve veiligheidsaanpak te realiseren.

Veiligheid is gelinkt aan ‘vrede en recht’. Den Haag staat al ruim een decennium op de wereldkaart als stad van ‘vrede en recht’, maar herbergt ook steeds meer wereldspelers op het vlak van ‘veiligheid’. The Hague Security Delta is het grootste netwerk van bedrijven, overheden en kennisinstituten in de Europese veiligheidssector. HSD is er als clusterorganisatie op gericht om economische groei en innovatie op het gebied van veiligheid te stimuleren. Om de positie van HSD te verstevigen en door te groeien tot koploper in het veiligheidsdomein, is het van belang om een geloofwaardig, goed onderbouwd beeld te krijgen van het economisch potentieel van de Security Delta.

In dit rapport geeft *Policy Research in Hoofdstuk 1* een overzicht van de huidige veiligheidssector in de regio Den Haag, Nederland en wereldwijd. Vervolgens wordt in *Hoofdstuk 2* een overzicht gegeven van de trends en ontwikkelingen in het veiligheidsdomein en een kwantitatieve foresight van het veiligheidscluster in 2020 op de drie niveaus regio Den Haag, Nederland en wereldwijd. *Hoofdstuk 3* gaat ten slotte in op de te nemen stappen voor de doorontwikkeling van de Nederlandse veiligheidssector. Naast de ambitie en de evaluatie van het veiligheidscluster vandaag komen in dit hoofdstuk ook de concrete acties aan bod om door te groeien tot koploper in het veiligheidsdomein.

I. FOTO SECURITY DELTA

I.1. METHODOLOGIE

Policy Research brengt de veiligheidssector in de regio Den Haag¹, Nederland en de wereld in kaart op vlak van werkgelegenheid, productiewaarde (omzet) en toegevoegde waarde voor de periode 2006 - 2012².

Binnen de bestaande statistische classificaties is de veiligheidssector maar voor een beperkt deel herkenbaar. Voor het maken van een foto van veiligheidscluster regio Den Haag werd door *Policy Research* daarom een bottom-up analyse uitgevoerd. Voor Nederland is de economische betekenis bepaald via semi-bottom-up analyse en voor Europa en wereld via top-down analyse (secundaire databronnen).

Voor de regionale economische parameters werd een lijst bedrijven en instellingen opgesteld die binnen de regio Den Haag actief zijn in het veiligheidsdomein. De basis was een eerdere foto in opdracht van HSD³, die werd aangevuld met (nieuwe) ledenbedrijven van HSD in de regio en met informatie uit andere netwerken⁴. Voor de bedrijven op deze lijst is via Stadgewest Haaglanden⁵ informatie opgevraagd uit het werkgelegenheidsregister LISA.

¹ Regio Den Haag betreft de optelsom van de COROP-gebieden 'Agglomeratie Den Haag' (COROP 26) en 'Delft en Westland' (COROP 27). Dit gebied behelst de regio's Den Haag, Wassenaar, Leidschendam-Voorburg, Zoetermeer, Rijswijk, Pijnacker-Nootdorp, Delft, Midden-Delftland en Westland.

² Cijfermateriaal voor 2013 is waar relevant en beschikbaar meegenomen in de foresight.

³ B&A Consulting (2011). *De veiligheidssector in de regio Den Haag en Nederland*.

⁴ Voorbeelden hiervan betreffen relevante partners genoemd in de HTSM Security Roadmap, Triarii rapportage 'De Nederlandse Defensie- en Veiligheidsgerelateerde industrie' NIDV-ledenlijst, aanwezige bedrijven bij netwerkevents zoals het matchmaking cyber security event door ICT-innovatieplatform 'Veilig Verbonden'.

⁵ Stadgewest Haaglanden is geconsulteerd als specialist inzake het vestigingsplaatsregister alsook inzake monitoring / ruimtelijk-economisch en arbeidsmarktonderzoek om het statistisch cijfermateriaal aan te leveren (werkzame personen, bedrijfsklasse en SBI-categorie).

Voor alle organisaties werd (waar relevant) gecorrigeerd voor bedrijfsgrootte en productiviteit die niet van toepassing is op het veiligheidscluster⁶. De aldus verkregen inzichten zijn uitgesplitst naar de door HSD onderscheiden deelsectoren national security, cyber security, critical infrastructure, urban security, forensics en education & research.

Met deze inzichten aangaande het aantal bedrijven (en hun SBI-categorisering) en het aantal werkzame personen werd de basis gelegd voor een adequate berekening van de parameters omzet en toegevoegde waarde per domein. Hiervoor werden de input-outputtabellen van het Centraal Bureau voor de Statistiek (CBS) aangewend. Deze werden ook gebruikt als input voor de omvangbepaling van het veiligheidscluster ‘Nederland’.

I.2. FOTO VEILIGHEIDSSECTOR 2012

I.2.1. OMVANG EN ECONOMISCHE BETEKENIS REGIO DEN HAAG

Het veiligheidscluster in de regio Den Haag⁷ bestaat in de kern uit een 400-tal vestigingen van bedrijven en (onderzoeks)instellingen. Samen stellen zij 13 400 werkzame personen te werk, verspreid over de deelsectoren national security, cyber security, critical infrastructure, urban security, forensics en education & research. In de schil eromheen zitten nog eens 12 200 werkzame personen bij gerelateerde onderdelen van ministeries, overige HSD partners en veiligheidsgerelateerde organisaties.⁸

Het veiligheidscluster in de regio Den Haag is goed voor een omzet van bijna 1.7 miljard euro op jaarbasis en realiseert daarmee een toegevoegde waarde van 820 miljoen euro.

Het veiligheidscluster is een vernieuwend cluster dat in de regio Den Haag sinds 2006 een bovengemiddelde jaarlijkse groei van 4.1% heeft gerealiseerd. De algemene Nederlandse economie vertoonde in de periode 2006 – 2012 een gemiddelde jaarlijkse groei van 0.6%. 85% van de omzet in de regio wordt gegenereerd *buiten* de traditionele veiligheidsdomeinen particuliere beveiliging en beveiliging via alarmsystemen (die vooral deel uitmaken van de deelsector *urban security*).

⁶ Met name voor grotere bedrijven (die vaak meerdere activiteiten hebben, binnen en buiten de veiligheidssector) is nagegaan - en ook getoetst via navraag bij de bedrijven zelf - welk deel (grootteorde) van de werkgelegenheid toe te rekenen is aan de veiligheidssector.

⁷ Regio Den Haag betreft de optelsom van de COROP-gebieden ‘Agglomeratie Den Haag’ (COROP 26) en ‘Delft en Westland’ (COROP 27).

⁸ Zie bijlage III.4.a/ *Overzicht werkzame personen en belangrijkste werkgevers per deelsector* voor nadere onderbouwing van het aantal werkzame personen per deelsector.

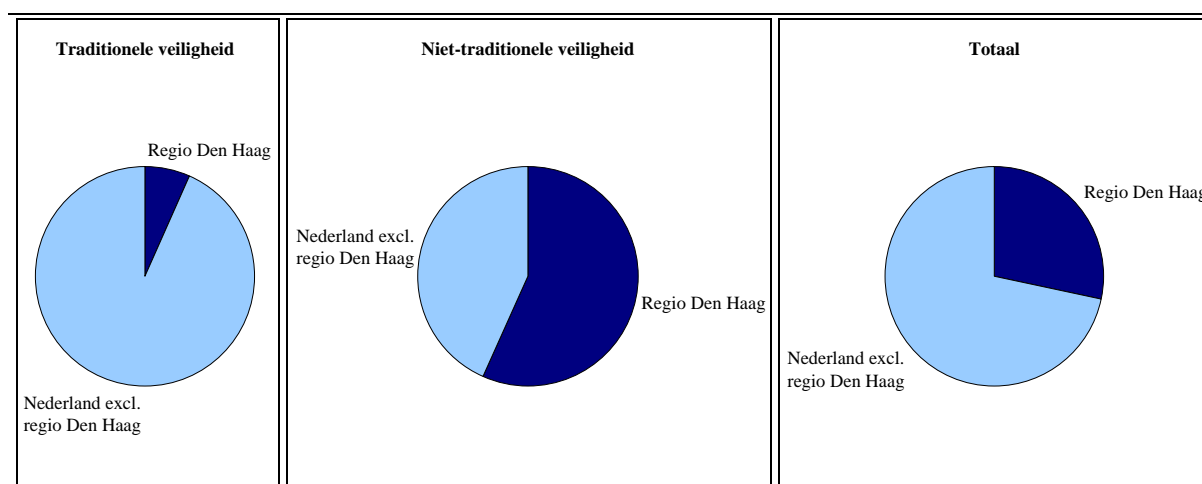
I.2.2. OMVANG EN ECONOMISCHE BETEKENIS NEDERLAND

Het veiligheidscluster ‘Nederland’ is in grootteorde goed voor 61 500 werkzame personen en een omzet van 6 miljard euro.

Het veiligheidscluster ‘Nederland’ is in belangrijke mate in transitie van een traditioneel (particuliere beveiliging en beveiliging via alarmsystemen) naar een niet-traditioneel (nieuwe veiligheid) veiligheidscluster. Momenteel wordt al ongeveer 45% van de omzet *buiten* de traditionele veiligheidsdomeinen gerealiseerd. Een belangrijk deel daarvan komt voor rekening van de regio’s Den Haag (HSD), Brabant (DITTS) en Twente (TSS).

Figuur 1 plaatst de regio Den Haag in perspectief tot Nederland op vlak van omzet in de veiligheid.

Figuur 1: De omzet van het veiligheidscluster in de regio Den Haag in perspectief tot de veiligheidssector in Nederland

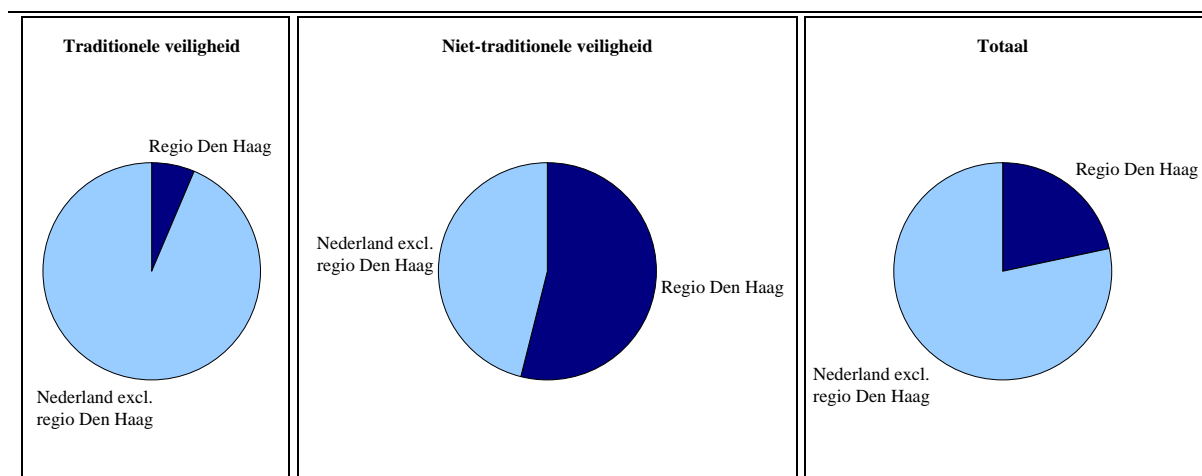


Bron : Policy Research Corporation

De regio Den Haag heeft in de traditionele veiligheid een aandeel van 7% in de Nederlandse omzet en in de niet-traditionele veiligheid een aandeel van 57%. Dit geeft een algemeen aandeel van het veiligheidscluster in de regio Den Haag van 28% in de omzet van het veiligheidscluster Nederland.

Figuur 2 plaatst de regio Den Haag in perspectief tot Nederland op vlak van aantal werkzame personen in de veiligheid.

Figuur 2: Het aantal werkzame personen in het veiligheidscluster in de regio Den Haag in perspectief tot de veiligheidssector in Nederland



Bron : Policy Research Corporation

De regio Den Haag heeft in de traditionele veiligheid een aandeel van 7% in het totale aantal werkzame personen in dit type veiligheid in Nederland. In de niet-traditionele veiligheid heeft de regio een aandeel van 54%. Dit geeft in termen van werkzame personen een algemeen aandeel van het veiligheidscluster uit de regio De Haag van 22% in het veiligheidscluster Nederland.

1.2.3. OMVANG EN ECONOMISCHE BETEKENIS WERELDWIJD

Het veiligheidscluster ‘wereldwijd’ vertegenwoordigt een omzet van ruim 180 miljard euro, waarvan om en nabij 45 miljard euro in West-Europa⁹. Tweederde deel daarvan komt voor rekening van activiteiten in het domein van traditionele veiligheid. Een derde deel betreft niet-traditionele veiligheidsactiviteiten (in bijzonder cyber security en forensics).

Het veiligheidscluster regio Den Haag heeft in de niet-traditionele veiligheid een aandeel van ruim 2% in de wereldwijde omzet, waar Nederland 4% van de wereldwijde omzet vertegenwoordigt. Het totale veiligheidscluster in de regio Den Haag heeft bijna 1% aandeel in de wereldwijde omzet. In het veiligheidscluster ‘Nederland’ wordt in totaal ruim 3% van de wereldwijde omzet gerealiseerd.

⁹ Inschatting op basis van informatie van Forensic Technology Market (2012), Freedonia Group (2013), G4S (2013) en MarketsandMarkets (2012).

II. FORESIGHT SECURITY DELTA

II.1. TRENDS EN ONTWIKKELINGEN

De veiligheidssector is onderhevig aan een aantal evoluties en trends die de concrete invulling van de sector in de komende jaren sterk zullen beïnvloeden.

Het belang van *samenwerking binnen de triple helix* om de veiligheidsuitdagingen aan te pakken wordt algemeen onderkend. Niet enkel HSD bouwt het veiligheidscluster in Nederland verder uit, maar ook andere regio's zoals Brabant (DITTS, Dutch Institute for Technology, Safety & Security) en Twente (TSS, Twente Safety & Security) doen – complementaire – inspanningen om de clusterontwikkeling op het vlak van veiligheid te stimuleren. De internationale trends binnen het veiligheidsdomein in combinatie met de complementariteit van de veiligheidsregio's zijn een ideaal kader om via *nauwere samenwerking* synergieën te creëren en het veiligheidscluster in de wereld op de kaart te zetten.

Globalisering, digitalisering, klimaatverandering, urbanisering en radicalisering verhogen de veiligheidsrisico's en maken de aanpak ervan meer complex. De samenhang tussen de verschillende veiligheidsdomeinen en –risico's vraagt een meer *geïntegreerde aanpak* om de risico's te beheersen en het veiligheidsgevoel te verhogen.

Veiligheidsbeleid en -maatregelen dringen steeds meer de *persoonlijke levenssfeer* van de bevolking binnen, waardoor het managen hiervan (inzake accepteerbaarheid door het publiek) steeds belangrijker wordt. Het *veiligheidsgevoel* is bijgevolg een van de meest belangrijke parameters voor het veiligheidsbeleid.

De evolutie van traditionele veiligheid naar nieuwe veiligheid legt nadruk op *innovatie*. Hierbij gaat het over een combinatie van innovatie op technologisch vlak en sociale innovatie. Het blijvend realiseren van innovatie vereist een integrale benadering, openheid en samenwerking tussen verschillende regio's, sectoren, disciplines en types organisaties.

De globale trend van automatisering zet zich ook door in het veiligheidsdomein. Meer en meer nadruk wordt gelegd op de *zachte aspecten van veiligheidssystemen* (software, datamanagement enz.) en er is een toename in vraag naar *geautomatiseerde systemen*. Dit leidt tot de vervanging of vermindering van het aantal werkzame personen. Verfijning van veiligheidsmateriaal promoot de high-end oplossingen met hoge toegevoegde waarde. *Technologische ontwikkelingen* met verwachte groei zijn digitale bewaking, smart cards, biometrische systemen en RFID (identificatie met radiogolven).

Niet onbelangrijk is ook dat technologie niet op zich staat maar dat ook de maatschappelijke en gedragskant, naast de privacy kant, meer geïntegreerd dient te worden om adoptie en adaptatie te realiseren (*sociale innovatie*)

Hoge instapbarrières in de veiligheidssector ontmoedigen MKB's en innovatie. Niet enkel zijn de investeringskosten verbonden aan de ontwikkeling van nieuwe (technologische) innovaties hoog, maar ook zijn er substantiële kosten verbonden aan de doorontwikkeling tot een commercieel product en de vermarkting ervan. MKB's actief in de ontwikkeling verkopen vaak patenten aan grotere ondernemingen of worden overgenomen om tot de fase van effectieve vermarkting te komen. Ook de consolidatie aan vraagzijde om de nieuwe veiligheidsrisico's te bestrijden (in het bijzonder terrorisme) leidt met grote aankoopcontracten vooral tot overeenkomsten met gevestigde grote spelers op de veiligheidsmarkt.

In elk van de door HSD onderscheiden deelsectoren – national security, cyber security, critical infrastructure, urban security, forensics en education & research – doen zich specifieke trends en ontwikkelingen voor.

II.1.1. NATIONAL SECURITY

Binnen national security vormen vooral de *transnationale (georganiseerde) criminaliteit en klimaatveranderingen* een belangrijke trend. De grootste bedreigingen in de transnationale criminaliteit zijn vooral cyberaanvallen, biologische wapens en nucleaire wapens. Ook *demografische ontwikkelingen* (verstedelijking, migratie, bevolkingsgroei) hebben een impact op het nationaal veiligheidsbeleid. Militaire of humanitaire operaties moeten worden voorbereid binnen een meer en meer complexe stedelijke context.

Er is sprake van een *gefragmenteerde Europese markt*, zowel aan vraag- als aanbodzijde. Het Europees veiligheidsbeleid moet de trigger zijn om tot verdere defragmentatie te komen en inefficiënties weg te werken in zowel de vraag als het aanbod. Hiervoor zijn de eerste stappen al gezet¹⁰.

¹⁰ Directives on defence procurement (2009/81) and transfers (2009/43) en de communicatie "Towards a more competitive and efficient defence and security sector" (2013).

II.1.2. CYBER SECURITY

Nederland neemt een prominente positie in de cybermarkt in met enkele *leader firms* die internationaal geconsulteerd worden¹¹.

De *afhankelijkheid van ICT* voor individuen, organisaties, ketens en de maatschappij neemt sterk toe door ontwikkelingen als *hyperconnectiviteit*, *cloud computing* en het gemak waarmee internet wordt ingezet. De potentiële impact van incidenten wordt daardoor groter. Omdat Nederland sterk heeft ingezet op de elektronische dienstverlening, kunnen cyberincidenten ook een grote impact hebben.

Het aantal (cyber)dreigingen is toegenomen. Deze gaan vooral uit van staten (*digitale spionage*) en beroepscriminelen (overname van ICT via ‘malware’ en ‘ransomware’ infecties en manipulatie van informatie (fraude)) tegen overwegend overheden, private organisaties en burgers. De *aanvallen worden minder zichtbaar* en nestelen zich voor lange tijd in stilte in organisaties voor ze worden ontdekt.

Afgelopen jaren is een *criminele cyberdienstensector* – waarin hulpmiddelen via ‘cybercrime-as-a-service’ commercieel beschikbaar worden gesteld – nadrukkelijk zichtbaar geworden. Enkele voorbeelden hiervan zijn Youtube filmpjes waarin hack-les wordt gegeven, de verkoop van online buitgemaakte creditcardgegevens, persoonsgegevens en emailadressen, witwasconstructies voor digitaal gestolen geld¹² of het gebruik van de Bitcoin voor criminele activiteiten. De Nederlandse cyberdienstensector wordt internationaal geconsulteerd om de aanvallen vanuit deze criminele sector te vermijden en bestrijden.

De *eindgebruiker krijgt grote verantwoordelijkheid toegedicht voor beveiliging*, maar wordt vaker geconfronteerd met kwetsbaarheden in apparaten / diensten waar hij beperkte invloed op heeft. Daarenboven brengen cloud diensten, mobiele diensten enz. nieuwe kwetsbaarheden met zich mee waar gebruikers zich minder tegen beschermen dan bij gebruik van de traditionele hardware.

Publieke en private partijen nemen, afzonderlijk en gezamenlijk, verschillende initiatieven om de digitale weerbaarheid te vergroten; de effectiviteit hiervan op lange termijn is nog niet in te schatten. De inherente dynamiek van cyber security vereist een *vernieuwende aanpak*. Statische informatiebeveiligingsmaatregelen zijn niet meer voldoende, organisaties hebben meer inzicht nodig in dreigingen (*detectie*) en hebben capaciteit nodig om te handelen bij dreigingen (response).

¹¹ Daartegenover staat dat onder andere door de concentratie van dataverkeer (Nederland als European gateway) Nederland in de top 10 staat van de ‘malicious activity’ cyber dreiging. Nederland is in 2012 van de 20e naar de 6e plaats gegaan in de algemene ranking wereldwijd van ‘malicious activity’ cyber dreiging. De Nederlandse gateway functie inzake dataverkeer maakt Nederland een target voor phishing & malware mails.

¹² Bijvoorbeeld het geval waarbij een Nederlandse moeder en zoon op een vooraf afgesproken tijdstip voor hackers geld pinden (2013).

Met de oprichting van *cyber security afdelingen* binnen een divers scala van ondernemingen (bv. Accenture, Deloitte, E&Y, KPN, PwC, Shell) en organisaties als NCSC¹³, NCTV¹⁴, ENCS¹⁵ enz. wordt getracht hier antwoord op te bieden.

Een hele nieuwe markt betreft de ontwikkeling van een verzekeringsmarkt, die zich meer en meer positioneert inzake het ontwikkelen van producten en diensten voor brede cyberrisico's.

II.1.3. CRITICAL INFRASTRUCTURE

Een *holistische aanpak* met focus op *weerbaarheid* eerder dan bescherming tegen dreigingen is noodzakelijk om respons te bieden aan de *toenemende kwetsbaarheid* van critical infrastructure. De kwetsbaarheid zal nog verder stijgen aangezien (1) critical infrastructure meer en meer deel uitmaakt van een netwerk en onderling met elkaar verbonden is, (2) computers en andere technologieën (cyber) steeds meer geïntegreerd worden in infrastructuur¹⁶, (3) terroristische dreiging (en evolutie hiervan) grote impact heeft op het beheer en de beveiliging van critical infrastructure en (4) de klimaatverandering en haar impact een extra uitdaging inhouden om voldoende bescherming te blijven bieden.

Verschillen en gelijkenissen tussen critical infrastructure bepalen het complexe speelveld van het veiligheidsbeleid. De verschillen betreffen de types critical infrastructure, spelers op de markt, veiligheidsstrategieën en juridische kaders. De gelijkenissen zijn de risico's gelinkt aan terrorisme, de toenemende dreiging van cyberaanvallen, de behoefte aan uitwisseling van best practices en de nood aan samenwerking tussen organisaties (publiek / privaat, intergouvernementeel).

Een nauwere *samenwerking tussen overheid en private sector* in de bescherming van vitale infrastructuur is een vereiste in een markt waar meer en meer private investeringen komen in vitale infrastructuur die historisch door overheden wordt gefinancierd.

II.1.4. URBAN SECURITY

De algemene trend van *doorgedreven verstedelijking* houdt een veiligheidsrisico in: dit kan zowel een negatieve impact (honger, armoede, criminaliteit) als een positieve impact (welvaartsverhoging) hebben. Globalisering heeft daarenboven een (betere) samenwerking tussen georganiseerde misdaad en terrorisme mogelijk gemaakt.

¹³ National Cyber Security Center.

¹⁴ Nationaal Coördinator Terrorismebestrijding en Veiligheid.

¹⁵ European Center voor Cyber Security.

¹⁶ 'Cyber-physical infrastructure'(bijv. smart grids) bij transportinfrastructuur, water infrastructuur en gezondheidszorg infrastructuur.

De belangrijkste *types van bedreiging* voor stedelijke veiligheid zijn geweld en criminaliteit, verblijfsonzekerheid¹⁷ en natuurrampen of ongelukken veroorzaakt door menselijke tussenkomst.

Urban security gaat vooral over het *veiligheidsgevoel* en de perceptie. De verbetering van statistieken is een middel om de perceptie te verbeteren, maar onvoldoende op zich. Het veiligheidsbeleid gaat dan ook niet meer enkel over politie of justitie, maar vereist een inzet op (1) aanpassingen van de fysieke ruimte (urban design), (2) verhoging van de maatschappelijke betrokkenheid, (3) minimalisering van risico's door te focussen op kwetsbare groepen en (4) versterking van het sociaal kapitaal. Steden kiezen hierbij meer en meer voor een *proactieve aanpak* van veiligheid¹⁸.

Technologische ontwikkelingen zijn essentieel om risico's en bedreigingen beter te anticiperen (o.a. energie efficiëntie verbeteren, risico op natuurrampen inschatten / verminderen), maar ook *kennisonwikkeling rond menselijk gedrag* levert een grote bijdrage aan een betere urban security.

II.1.5. FORENSICS

De forensics sector ondergaat een evolutie van reactieve forensics naar meer *actieve (digitale) forensics*¹⁹, naar meer *virtuele en mobiele forensische instrumenten* en naar een hogere *klantenfocus* dan in het verleden: sneller, meer, betrouwbaar en aan lagere gemiddelde kost opleveren.

Er is een enorme *groei* merkbaar, meer dan gemiddeld in het veiligheidsdomein. Deze groei is onder meer te danken aan nieuwe technische capaciteiten (biometrisch, IT, chemisch), een grotere awareness bij de klant en een nieuw type klanten buiten de scope van traditioneel forensisch onderzoek, zoals gemeentelijke organisaties, defensie ministeries, transportbedrijven, belasting onderzoekers, geheime diensten... Er ontstaat een groeiende nood aan *training en opleiding*²⁰.

De grote uitdaging is om (wereldwijd) als forensics sector om te gaan met de hoge *fragmentatie* op vlak van expertise en geografie. Deze leidt tot inefficiëntie, kwetsbaarheid, backlog/capaciteitsproblemen en (te) weinig innovatie. Nederland is binnen de forensics sector een uitzondering omdat binnen NFI juist alle expertise gebundeld is.

¹⁷ Inclusief basisbehoeften zoals water-, voedsel- en energie(on)zekerheid.

¹⁸ 1) preventie, 2) bescherming, 3) reactie.

¹⁹ Business Intelligence principes toepassen op de forensics gerelateerde (big) data.

²⁰ Opleiding Forensics opgestart in Amsterdam.

II.1.6. EDUCATION & RESEARCH

Er worden steeds meer *veiligheidsgerichte (master) opleidingen* georganiseerd door de kennis- en onderzoeksinstituten, gaande van bijvoorbeeld Crisis & Security Management aan de Universiteit Leiden tot de Cyber Security Academy als samenwerking tussen onderzoek en ondernemingen. Daarbij wordt voldoende aandacht besteed aan het afstemmen van de opleidingen aan de behoeftes van de bedrijven en op het flexibel kunnen inspelen op nieuwe trends en ontwikkelingen.

Zowel binnen als tussen onderzoeks- en onderwijsinstellingen wordt gewerkt aan de cross-over aanpak (tussen disciplines en in samenhang met de andere O's).

II.2. FORESIGHT VEILIGHEIDSSECTOR 2020

II.2.1. GROEIVERWACHTING REGIO DEN HAAG

Het aantal werkzame personen in het veiligheidscluster regio Den Haag zal naar verwachting met een kwart toenemen in de periode tot 2020. De omzet zal in dezelfde periode met de helft toenemen. Dit vertaalt zich in 2020 in circa 17 000 werkzame personen (+ 6 000) en een omzet van naar verwachting 2.5 miljard euro (+ 800 miljoen euro). De toename in de periode tot 2020 valt voor meer dan de helft voor rekening van de deelsectoren *cyber security* en *forensics*.

Specifiek in het cyber domein zijn er vele berichten van aanwerving van extra werknemers de komende jaren. Er is sprake van 40 extra werkzame personen in 2014 bij het Nationaal Cyber Security Center, 90 extra werkzame personen de komende drie jaren bij het European Cyber Crime Center en zelfs 350 extra werkzame personen de komende jaren bij de Joint SIGINT Cyber Unit (Symbolon).

Voor de komende jaren lijkt op basis van deze aantallen binnen het cyberdomein alvast een groei van meer dan 10% per jaar (200 wzp of meer) gegarandeerd.

National security heeft geen hoger groeipercentage dan de andere domeinen, maar heeft als grootste domein toch een relatief grote toename van het aantal werkzame personen. Een lichte krimp wordt verwacht in de werkgelegenheid bij urban security als gevolg van de toename in vraag naar geautomatiseerde systemen (vervanging werkzame personen). In de domeinen critical infrastructure, forensics en education & research) zal de werkgelegenheid toenemen met in totaal een 500tal werkzame personen.

II.2.2. GROEIVERWACHTING NEDERLAND

Ook het veiligheidscluster ‘Nederland’ zal groei kennen in de periode tot 2020.

De traditionele veiligheidsactiviteiten die – op Nederlands niveau – in termen van werkgelegenheid momenteel het overgrote deel uitmaken van het cluster zullen een verdere transitie kennen van personen naar technologie. Er is er een verschuiving van werkgelegenheid van traditionele veiligheid naar niet-traditionele veiligheid en in termen van werkgelegenheid zal de groei op Nederlands niveau dan ook minder uitgesproken zijn dan in de regio Den Haag.

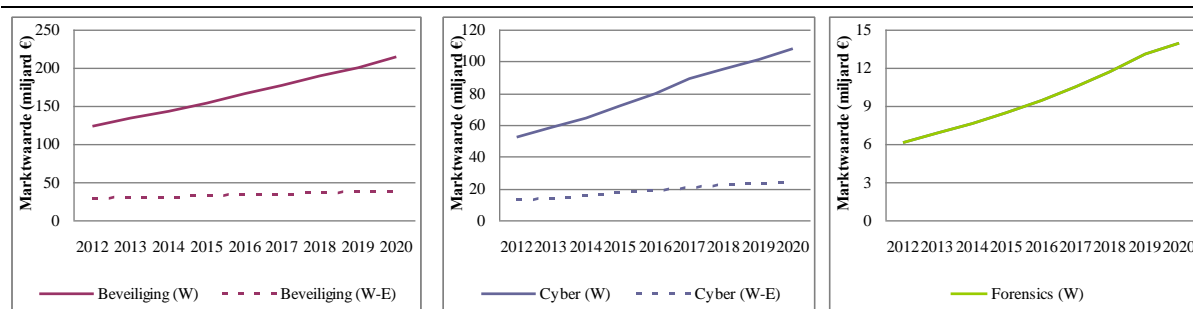
In Brabant en Twente wordt vanuit DITTS en TSS sterk ingezet op het via living labs aanpakken van praktische veiligheidsvraagstukken zodat technologische, juridische en gedragswetenschappelijke aspecten kunnen opgepakt worden.

Ook in termen van omzet zal de groei op Nederlands niveau minder uitgesproken zijn. De omzetgroei cumuleert in belangrijke mate in de ‘security delta’ regio’s – Den Haag, Brabant en Twente – waar de nieuwe, niet-traditionele, veiligheidsactiviteiten vooral plaats hebben.

II.2.3. GROEIVERWACHTING EUROPA EN WERELDWIJD

Het veiligheidscluster ‘wereldwijd’ zal tegen 2020 aangegroeid zijn tot 300 à 350 miljard euro, waarvan ongeveer 70 miljard euro in West-Europa wordt gegenereerd. De groeiverwachting van de beveiligings-, cyber security en forensics markt is voorgesteld in *Figuur 3*.

Figuur 3: Groeiverwachting veiligheidssector wereldwijd (W) en in West-Europa (W-E)



Bron: Policy Research Corporation op basis van Forensics Technologies Market (2012), Freedonia Group (2013), G4S (2013) en MarketsandMarkets (2012)

De traditionele veiligheid heeft in waarde de grootste omvang met een relatief lage groei. Het verwachte gemiddelde jaarlijkse groeipercentage bedraagt wereldwijd 7.5% tot 2016 en 6.6% daarna tot 2020. De groeipercentages voor de West-Europese markt zijn iets lager en bedragen respectievelijk 4.0% en 3.3%.

In dit domein vindt (vooral in de geïndustrialiseerde gebieden) een transitie plaats van manbeveiliging naar geautomatiseerde beveiliging. Er is bijgevolg wel omzettoename in combinatie met werkgelegenheidsafname.

De grootste procentuele groei – zowel wereldwijd als in West-Europa – wordt volgens de Europese Commissie verwacht in cyber security en forensics. Het verwachte gemiddelde jaarlijkse groeipercentage voor de cyber markt bedraagt 11.3% wereldwijd en 10.1% voor West-Europa. Voor de forensics markt wordt wereldwijd ongeveer hetzelfde groeipercentage verwacht, namelijk gemiddeld 11.4% tot 2020.

De groeiverwachting in Azië en de Pacific regio is groter dan in Amerika en West-Europa. Het marktaandeel van Europa in de security sector wordt verwacht te dalen van 25% naar 20%.

III. STAPPEN VOORUIT

In dit hoofdstuk wordt eerst de ambitie van HSD inzake veiligheidsclusterontwikkeling in de regio Den Haag toegelicht (zie *III.1 Ambitie*). Vervolgens worden de succesfactoren voor clusterontwikkeling besproken (zie *III.2 Nodige kwaliteiten voor clusterontwikkeling*) en het veiligheidscluster vandaag geëvalueerd (zie *III.3 Evaluatie Security Delta vandaag*). Ten slotte komen enkele concrete actiepunten aan bod (zie *III.4 Acties voor een sterke(re) Security Delta*).

III.1. AMBITIE

Het bestaan van HSD als organisatie is cruciaal om de Security Delta als veiligheidscluster te versterken en verder uit te bouwen. Naast een faciliterende rol, waarin onder andere infrastructuur ter beschikking wordt gesteld en praktische adviezen worden gegeven aan MKB's, is er ook een inhoudelijke / procesmatige rol weggelegd voor HSD waardoor effectieve resultaten geboekt kunnen worden.

De ambitie van HSD inzake veiligheidsclusterontwikkeling in de regio Den Haag is:

- *De Security Delta internationaal op de kaart zetten als kernregio voor veiligheid*
De Security Delta niet enkel positioneren binnen Nederland en Nederlands kapitaal aantrekken, maar als veiligheidscluster op wereldvlak naam maken (naast bv. New York en Singapore);
- *Gericht zoeken naar nieuwe vormen van samenwerking binnen de triple helix*
Vanuit de clusterorganisatie een brug maken tussen vraag en aanbod door een actieve rol te spelen om de vraagarticulatie te verbeteren en de juiste aanbieders aan te trekken; in parallel ook structurele publiek/private samenwerking realiseren;
- *Lange termijn visie in functie van maatschappelijke veiligheid*
Integraal veiligheidsbeleid ontwikkelen en uitvoeren met nadruk op vooruitkijken en anticiperen; dit beleid moet op het juiste niveau verbonden worden met de nationale veiligheidsagenda;

- *Nieuwe concepten ontwikkelen*
Inzetten op innovatie en ontwikkeling in de nieuwe veiligheid en op de technologische ontwikkelingen in de traditionele veiligheid; dit gaat meer bepaald over high-end beveiligingsinnovaties, big data, (secure) cloud, forensic innovaties enz.;
- *Brede inzet op de Security Delta*
Nauwere samenwerking opzetten en synergieën creëren tussen in bijzonder regio Den Haag (HSD), regio Brabant (DITTS) en regio Twente (TSS).

Verschillende initiatieven zijn de voorbije jaren door HSD opgestart om deze ambitie te verwezenlijken, zoals bijvoorbeeld de oprichting van de HSD Campus, de selectie van innovatieprojecten die gefinancierd worden door het HSD Stimuleringsfonds, de oprichting van de Cyber Security Academy en de organisatie van ASIS European Security Conference & Exhibition. HSD speelt hierbij vooral een governance en faciliterende rol. In Brabant is DITTS²¹ de trekker om met de veiligheidssector economische spin-off te realiseren. In Twente is TSS²² de evenknie van HSD en DITTS.

III.2. NODIGE KWALITEITEN VOOR CLUSTERONTWIKKELING

Hoewel er een verschil blijkt te zijn tussen hoe clusters zich kenmerken (bijvoorbeeld kleine ondernemingen versus grote trekkers)²³, zijn er toch een aantal generieke succesfactoren waarvan de invulling, samenhang en onderlinge impact bepalend is voor het succes van de cluster. Een kader van 10 succesfactoren zal worden gehanteerd voor de evaluatie van de Security Delta als cluster vandaag (zie *III.3 Evaluatie Security Delta vandaag*) en zal als basis dienen voor de prioritering van acties om het veiligheidscluster verder uit te bouwen (zie *III.4 Acties voor een sterke(re) Security Delta*).

De 10 succesfactoren voor clusterontwikkeling zijn voorgesteld in *Figuur* .

²¹ Tilburg heeft binnen DITTS een initiatief gelanceerd om innovatieprojecten financieel te ondersteunen (vergelijkbaar met het HSD Stimuleringsfonds). Bij dit programma – ‘Uitvraag Tilburg’ – werden drie concrete veiligheidsvragen voorgelegd aan diverse stakeholders in workshops. Met deze aanpak is niet alleen vanuit de clusterorganisatie invulling gegeven aan de vraagarticulatie, maar ook werd zo een faciliterende rol opgenomen om van de veiligheidsvraag en vage ideeën tot concrete oplossingsrichtingen te komen. Een jury heeft dan in een tweede fase een selectie gemaakt en aan een van de voorstellen per vraag budget toegewezen.

²² Veiligheidsregio Twente heeft bijvoorbeeld de ambitie om in Triple helix verband met Twente Security & Safety (inter)nationaal de veiligheidsagenda mede te bepalen en uit te voeren. De centrale doelstellingen van het programma TS&S zijn:

1. Pak samen met publieke en private partijen veiligheidsproblemen aan met innovatieve oplossingen en realiseer een veilig woon- en leefklimaat tegen acceptabele kosten;
2. Ontwikkel en test deze hoogwaardige kennis en innovaties in de praktijk en toets naast technologie ook het gedrag bij hulpverleners en betrokkenen dat leidt tot effectief gebruik van de innovatie;
3. Pak door op succesvolle veiligheidsinnovaties, ontsluit deze voor de markt en stimuleer zo economie en werkgelegenheid;
4. Positioneer Twente met partners stevig in nationale en internationale arena's en verwerf gezamenlijk fondsen voor onderzoek en ontwikkeling.

²³ Zie bijlage *b/ Benchmark andere clusters* voor overzicht van enkele andere succesvolle clusters.

Figuur 4: 10 succesfactoren voor clusterontwikkeling



Bron : Policy Research Corporation

Om het snelgroeiend internationaal economisch cluster rond Den Haag op het gebied van veiligheid verder uit te bouwen, heeft HSD een Masterplan 2013 - 2014 uitgewerkt. In dit Masterplan zijn meerdere concrete initiatieven opgenomen om de clusterontwikkeling te verzekeren en versnellen. Met deze initiatieven speelt HSD in op de succesfactoren voor clusterontwikkeling.²⁴

De (door)ontwikkeling van lokale veiligheidscluster tot Security Delta van Nederland is zeer kansrijk, zeker nu in samenhang met andere regio's (Brabant, Twente) ingezet wordt op het samenbrengen van expertise en het (cross-sectorieel en cross-regionaal) bundelen van krachten. Er zijn al veel positieve stappen gezet en successen geboekt (zie ✓ hierna). Om de clusterontwikkeling verder te faciliteren is het niettemin zaak om een aantal concrete werkpunten (zie ✗ hierna) ter harte te nemen. Onderstaand worden de initiatieven en werkpunten per succesfactor weer gegeven.

1 *Beleid*

Prioriteit geven aan en het realiseren van een integrale veiligheidsaanpak

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ Intentie van HSD om een rol als katalysator op te nemen voor het verbinden en versterken van verschillende (inter)nationale initiatieven (incubator);

²⁴ In bijlage III.4.c/HSD Masterplan 2013-2014 worden de initiatieven uit het Masterplan toegelicht.

- ✓ Aanwezigheid (en gedeeltelijk actieve rol) van Nederlandse overheid en organisaties als NCSC (Nationale Cyber Security Raad), AIVD (Algemene Inlichtingen- en Veiligheidsdienst), NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid), KLPD (Korps Landelijke Politiediensten),...²⁵;
- ✓ Aanwezigheid van internationale publieke instanties zoals NATO, Internationaal Strafhof, Internationaal Gerechtshof, Europol, OPCW (Organisation for the Prohibition of Chemical Weapons),...

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

Werkpunten voor HSD:

- ✗ Clusterbeleid op basis van kleine nicheclusters (door middel van deelsectoren ‘Innovatiehuizen’) die toch onderling met elkaar overlappen; integrale veiligheidsaanpak minstens even belangrijk als visie en strategie per deelsector;
- ✗ Vooral kansrijk voor HSD in het cyber domein is de inzet op publiek-private vraagstukken die de Overheid (NCTV, NCSC, ..) niet getackled krijgt juist omdat de overheid daar in de lead zit²⁶;
- ✗ Smart, dynamische aanpak van HSD en lobbyen om politieke besluitvorming te versnellen.

Werkpunten voor overheid in samenwerking met de veiligheidsclusters:

- ✗ Een betere omschrijving van de vraag / betere afstemming tussen vraag en aanbod geeft de veiligheidsondernemingen meer richting en een beter afnamepotentieel (bv. nationale innovatieagenda voor maatschappelijke veiligheid).

Werkpunten voor de overheid:

- ✗ De overheid zou als ‘launching customer’ een grotere rol kunnen opnemen in de stimulering van de Nederlandse veiligheidssector²⁷;
- ✗ Via beleid en vraagarticulatie een positieve invloed uitoefenen op het aantrekken van kapitaal (bv. nationale veiligheidsinvesteringsagenda);
- ✗ Innovatie van inkoopproces om het doel van inkoop beter mee te nemen in de selectie en zo het risico te minimaliseren dat het resultaat niet is wat initieel werd beoogd;
- ✗ Interne (binnen overheidsdiensten) en externe sensibilisering over het belang van de nieuwe (virtuele/digitale) veiligheid.

²⁵ Gelieerd aan het feit dat Den Haag dé vestigingsplaats in Nederland is voor Nederlandse regering, parlement, ministeries en buitenlandse ambassades en organisaties.

²⁶ Vraagstukken waarbij organisaties niet graag gegevens uitwisselen vanwege WOB-verplichting van de overheid.

²⁷ Een type voorbeeld voor economische waarde creatie en de rol van de overheid als launching customer is het Nationaal Forensisch Instituut NFI.

2 Internationalisatie

Internationaliseer alle acties en organiseer profilerende events

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ Opstellen van het Internationaal Acquisitieprogramma voor het aantrekken en betrekken van internationale security bedrijven, congressen en andere netwerken;
- ✓ Security Acquisitie Platform (SAP) waarbij onder meer de focus ligt bij het aantrekken van buitenlandse partijen;
- ✓ Nuclear Security Summit 2014, European Security Conference & Exhibition 2014 en International Cyberspace Conference 2015 brengen internationale toporganisaties naar Nederland en bieden opportuniteit voor de Security Delta om zich internationaal te profileren; ook afvaardiging vanuit de Security Delta naar buitenlandse conferenties zoals de Cyber Summit 2015 in USA ondersteunt de internationale positionering;
- ✓ Internationale samenwerkingscontacten en verbanden met ASIS, Homeland Security (USA), Ottawa Invest (Canada), UKTI (Engeland) en landen zoals Duitsland, India, Singapore, Zweden, Zuid-Afrika, België.

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ Minstens één referentieproject nodig dat de Security Delta internationaal op de kaart zet (zogenaamde white pearl project). Dit moet op korte termijn gebeuren om echt als veiligheidscluster een doorstart te maken;
- ✗ Organisaties als bijvoorbeeld EU en NATO nog niet aan boord;
- ✗ Den Haag heeft 131 internationale instituties, waarvan een groot deel (zoals Europol en Interpol) gevestigd zijn in de Internationale Zone; de betrokkenheid van leader firms op vlak van veiligheid (wereldspelers en nichespelers in de nieuwe veiligheid) bij de clusterontwikkeling kan echter nog verbeterd worden.

3 Samenwerking

Organiseer een draagvlak dat de kracht heeft de veiligheidssector te stimuleren en aan te sturen

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ Intentie van HSD om als verbindende factor tussen innovatieregio's in Den Haag, Twente (TSS) en Brabant (Tilburg/Eindhoven - DITTS) actief te zijn;
- ✓ Internationale samenwerkingscontacten en -verbanden met ASIS, Homeland Security (USA), Ottawa Invest (Canada), UKTI (Engeland)... en landen zoals België, Duitsland, India, Singapore, Zuid-Afrika en Zweden.

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ Duidelijkere rolverdeling tussen verschillende types van organisaties om dubbelwerk en overlap van activiteiten te vermijden (bv. in het cyberdomein rol HSD vs. ENCS vs. NCSC...);
- ✗ Architectuur voor samenwerking binnen de triple helix²⁸ verder uit te bouwen en te stimuleren;
- ✗ Vertrouwen tussen triple helix organisaties versterken (nu gedragscode);
- ✗ Verruiming van HSD Board (TU Delft, KPN, Brabant, Twente,...).

4 Kennisinstellingen

Positioneer onderzoek- en kennisinstellingen als trekker voor de uitbouw van onderwijs en onderzoek in het veiligheidsdomein

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ Aanwezigheid universiteiten (TU Delft, ULeiden), hogescholen (Haagse Hogeschool) en onderzoekscentra (bv. TNO, NFI, Clingendael, HCSS) in de Haagse regio;
- ✓ Oprichting Cyber Security Academy;
- ✓ HSD Cyber Security Traineeship;
- ✓ Kennisinstellingen betrokken bij HSD projecten (Real Time Intelligence Lab, Serious Gaming Lab, Crisis simulatiecentrum, ENCS, Living Lab Sociale Veiligheid en CSI The Hague II).

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ TU Delft (nog) onvoldoende betrokken;
- ✗ Draagvlak bij kennisinstellingen op bestuurlijk niveau, maar uitdaging om ook de hoogleraren actief te betrekken en enthousiasmeren;
- ✗ Kennis creatie binnen de cluster verder stimuleren;
- ✗ Opleidingsniveau en –inhoud nauw laten aansluiten bij de behoeften van vraag en aanbod.

5 Innovatie en R&D

Creëer, faciliteer of verwerf high-profile projecten

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ HSD Innovatiehuizenprogramma, MKB Innovatieprogramma waarbij HSD MKB's begeleidt in netwerkvorming, clustervorming en doorontwikkeling;
- ✓ MKB Connect, voor persoonlijk advies aan MKB's;

²⁸ Soms wordt ook gesproken over een quadruple helix: hierin staat de (maatschappelijke) vraag centraal binnen de 30's.

- ✓ MKB Desk, voor advies i.v.m. innovatieprojecten;
- ✓ Oprichting van het Nationaal Veiligheidsinnovatie Centrum (Real Intelligence Lab, Cyber Incident Experience Center, Serious Gaming Lab, Crisis simulatiecentrum, ENCS);
- ✓ Living Lab (o.a. CSI The Hague II).

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ Vele initiatieven bevinden zich in de opstartfase, een verdere realisatie is nodig om innovatie en R&D écht te ondersteunen en stimuleren;
- ✗ High-profile projecten beter te ondersteunen zodat deze ook als marketingtool kunnen worden ingezet.

6 Ondernemers / rolmodellen

Stimuleer de vestiging en ontwikkeling van leader firms

Initiatieven die de clusterontwikkelingen al stimuleren:

- ✓ Voortrekkende rol / rolmodel door grote ondernemingen zoals Fox-IT, KPN, Siemens, Thales en Trigion;
- ✓ Ondernemingen vestigen zich in de regio (bv. 3M, speler in de forensics markt);
- ✓ Betrokkenheid ondernemers bij Cyber Incident Experience Center, Cyber Security Academy, HSD Cyber Security Traineeship, CSI The Hague II.

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ Trekkers zijn door HSD aangesteld per deelsector, maar dit zijn voornamelijk kennisinstellingen (geen goede mix van triple helix);
- ✗ Relatief weinig grote (internationale) ondernemingen (wereldspelers en nicheorganisaties nieuwe veiligheid), voornamelijk (lokale) MKB's.

7 Kapitaal & investeringen

Lanceer een stimuleringsfonds en trek kapitaal aan

Initiatieven die de clusterontwikkelingen al stimuleren²⁹:

- ✓ HSD Stimuleringsfonds, waarbij partners zicht geboden wordt op financieringsbronnen voor onder meer onderzoek, prototypes, business development en marketing;

²⁹ Een Brabants voorbeeld van structurele en substantiële kapitaalbreng voor R&D is ASML. Als bedrijfsconcept investeren klanten / afnemers mee in de R&D activiteiten van de onderneming. Op deze manier worden voldoende middelen vrij gemaakt voor onderzoek, wordt het risico gespreid, zijn de innovaties afgestemd op de concrete markt vraag en vinden de nieuwe ontwikkelingen ook effectief hun weg naar de markt.

- ✓ Oprichting Innovation Quarter, actief in business development, marketing & acquisitie en het beheer van het regionaal ontwikkelingsfonds en met Safety & Security als een van de kerndomeinen;
- ✓ Horizon 2020 programma van de Europese Commissie;
- ✓ HSD Ontwikkelingsmaatschappij;
- ✓ MKB Desk;
- ✓ HSD Office (acquisitie + PR).

Concrete werkpunten om de clusterontwikkeling te optimaliseren:

- ✗ Beschikbaarheid van kapitaal en toegang tot kapitaal te verbeteren (stapeling van fondsen lokaal, regionaal en nationaal; bv. nationale veiligheidsinvesteringsagenda);
 - Ten behoeve van kennisontwikkeling, innovatie en R&D;
 - Ten behoeve van het realiseren van een doorstart van projecten (van ontwerp en succesvolle tests naar vermarkting brengen);
- ✗ Relatief weinig beursgenoteerde ondernemingen aanwezig;
- ✗ Relatief weinig investeringen via venture capital.

8 Levenskwaliteit

Zorg voor een aantrekkelijk vestigingsklimaat in de regio

Initiatieven die de clusterontwikkelingen al voldoende stimuleren:

- ✓ Reeds hoge levenskwaliteit in Den Haag;
- ✓ Verhogen van ‘quality of life’ met nieuwe voorzieningen als Spuiforum en een expatdesk;
- ✓ Nieuwe investeringen in bereikbaarheid;
- ✓ Living Lab Integrale Gebiedsbeveiliging;
- ✓ Living Lab Sociale Veiligheid.

9 Human Capital

Trek talent aan om de stijgende vraag aan werknemers in te vullen

Initiatieven die de clusterontwikkelingen al voldoende stimuleren:

- ✓ Strategische partnership met International Community Platform voor optimaal woon- en werkklimaat van internationale werknemers en hun gezinnen;
- ✓ Opzet Human Capital agenda in 2014;
- ✓ Portal via HSD site voor opleidingen en leerlijnen, aanbieden van (online) trainingen, oefeningen en games;
- ✓ Aanwezigheid van kennisinstellingen en opleidingscentra.

10 Infrastructuur

Voorzie de nodige infrastructuur om de andere succesfactoren te kunnen realiseren

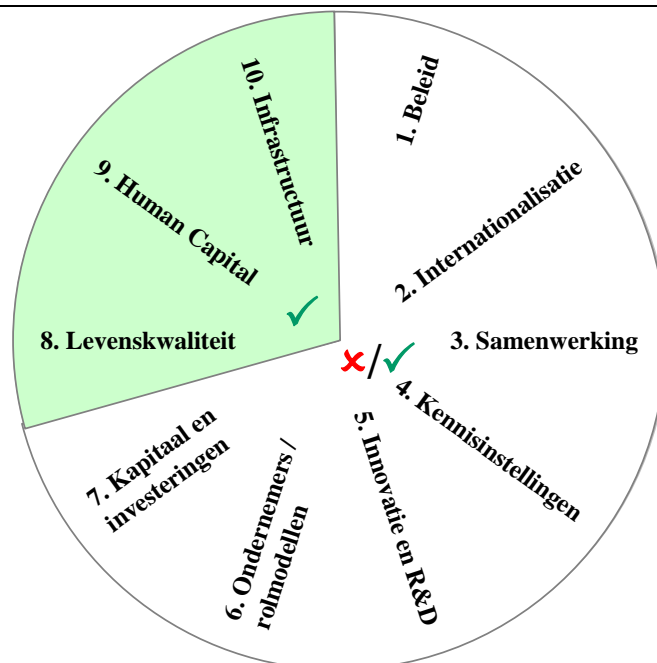
Initiatieven die de clusterontwikkelingen al voldoende stimuleren:

- ✓ Uitbouw HSD Campus, met aanwezigheid van Nationaal Veiligheidsinnovatiecentrum, kantoorruimtes, opleidings- en vergaderfaciliteiten, Incubator faciliteiten, een bedrijfsverzamelgebouw, Living Labs;
- ✓ Versterken van de security in de Internationale Zone.

III.3. EVALUATIE SECURITY DELTA VANDAAG

Figuur 5 geeft de evaluatie zoals *Policy Research* die maakt voor wat betreft de ‘as is’ situatie rond de Security Delta (regio Den Haag). Het teken ✗ / ✓ geeft aan dat er nog concrete werkpunten (✗) zijn om de clusterontwikkeling optimaal te stimuleren, naast positieve punten (✓). Het teken ✓ geeft aan dat voor een bepaalde succesfactor de huidige initiatieven de clusterontwikkelingen al voldoende stimuleren.

Figuur 5: Evaluatie succesfactoren Security Delta Regio Den Haag vandaag



Bron : *Policy Research Corporation*

Op vlak van beleid, internationalisatie, samenwerking, kennisinstellingen, innovatie en R&D, ondernemers / rolmodellen en kapitaal en investeringen is er bijkomende actie nodig om van de Security Delta een internationaal succesverhaal te maken. Acties om dit te realiseren worden toegelicht in de volgende paragraaf.

III.4. ACTIES VOOR EEN STERKE(RE) SECURITY DELTA

De Security Delta heeft vandaag nog een aantal werkpunten om zich optimaal als cluster te kunnen (door)ontwikkelen. Deze vertalen zich samengevat in een aantal concrete acties om als veiligheidscluster het groeipad naar 2020 slagvaardig te kunnen realiseren.

De concrete acties zijn:

Beleid

- i. Overheid ondersteunen bij beleidsontwikkeling, vraagarticulatie, inkoopinnovatie en aligering met lange termijn visie (veiligheidsbeleid, stadsontwikkeling, vestigingscondities enz.);
- ii. Als overheid de rol opnemen van 'launching customer' ter stimulering van de Nederlandse veiligheidssector;
- iii. Integraal veiligheidsbeleid en algemene visie op veiligheid (maatschappelijk rendement en sociale innovatie) om de deelsectoren te aligieren en synergieën tussen de deelsectoren te benutten;

Internationalisatie

- iv. Optimaal benutten van de aanwezigheid van de internationale markt in Nederland ter gelegenheid van Nuclear Security Summit 2014, European Security Conference & Exhibition 2014 en International Cyberspace Conference 2015; naast conferenties ook handelsmissies opzetten en ondersteunen om deuren te openen en bedrijven aan te trekken; eigen events een internationaal karakter geven;

Samenwerking

- v. Vertrouwen creëren en een nieuwe architectuur voor samenwerking ontwikkelen en implementeren;

Kennisinstellingen

- vi. Kenniscreatie stimuleren en opleidingen beter afstemmen op vraag en aanbod in het veiligheidsdomein;

Innovatie en R&D

- vii. 'White pearl voor HSD': high profile referentieproject(en) die als visitekaartje voor HSD kunnen gelden;

Ondernemingen / rolmodellen

- viii. Aantrekken van wereldspelers en nicheorganisaties nieuwe veiligheid naar de regio;

Kapitaal en investeringen

- ix. Beschikbaarheid van en toegang tot kapitaal verbeteren (investeringsagenda);
- x. Als katalysator voor innovatieprojecten de juiste (financiële) ondersteuning bieden.

De verantwoordelijkheid voor het oppakken en uitvoeren van de werkpunten en acties ligt bij alle triple helix partijen. Een gezamenlijke inzet zal Nederland langdurig internationaal als veiligheidscluster op de kaart zetten. HSD, in samenwerking met DITTS en TSS, zal hiervoor als clusterorganisatie de nodige begeleiding geven aan de triple helix partijen, zowel in een faciliterende rol als via een procesmatige ondersteuning.

Regio's Den Haag, Brabant, Twente en Nederland hebben het potentieel om een Security Delta met wereldbetekenis te zijn. De combinatie van de volledigheid van het cluster, de ontwikkelingen in de niet-traditionele veiligheid, de historische als 'stad van vrede en recht' en de aanwezigheid van de (internationale) triple helix vormt een uniciteit en voordeel tegenover andere regio's in de wereld.

Het kader en potentieel voor de succesvolle uitbouw van het veiligheidscluster zijn aanwezig om door te groeien tot wereldwijde koploper en dé referentie in het (nieuwe) veiligheidsdomein.

REFERENTIES

- AGB Masterplan Houthalen-Helchteren (2009). *Visie voor de Limburgse Cleantech Toekomst*
- Antonenko, O., Giegerich, B., Inkster, N., Pantucci, R. & Roy-Chaudhury, R. (2008). *FORESEC Deliverable 2.3: Global Trends and Actors Shaping European Security*
- Atlantic Council & Stimson Center (2013a). *Foreign Policy for an Urban World: Global Governance and the Rise of Cities*
- Atlantic Council & Stimson Center (2013b). *The Security of Cities: Ecology and Conflict on a Urbanizing Planet*
- B&A Consulting (2011). *De Veiligheidssector in de regio Den Haag en Nederland*
- Crisis and Risk Network (CRN), Center for Security Studies (CSS) – ETH Zürich (2009). *Focal Report 2: Critical Infrastructure Protection*
- CSIS (2012). *European Defense Trends 2012: Budgets, Regulatory Frameworks, and the Industrial Base*
- Decisio (2011). *Den Haag internationale stad van vrede en recht: Economische impact internationale organisaties*
- Decisio (2013). *Economisch belang intergouvernementele organisaties in Nederland*
- Den Haag Centrum voor Strategische Studies (2012). *Internationale clusters in vergelijkend perspectief – best practices voor de opzet van The Hague Security Delta*
- Ecorys (2009). *Study on the Competitiveness of the EU security industry*
- EIM (2008). *De Nederlandse defensiegerelateerde industrie: Actualisering van de kwantitatieve kenmerken*
- European Commission (2012). *Security Industrial Policy: Action Plan for an innovative and competitive Security Industry*
- Federal Emergency Management Agency (2011). *Critical Infrastructure: Long-term Trends and Drivers and their Implications for Emergency Management*
- Forensic Technologies Market (2012). *Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2013-2019*
- Freedonia Group (2013). *World Security Services: Industry Study with Forecasts for 2016 & 2021*
- G4S (2013). *Our Markets*

- Gemeente Den Haag (2013). *The Hague Security Delta ontwikkelt campus voor innovatie en veiligheid*
- GlobeScan & MRC McLean Hazel (2007). *Megacity Challenges: a Stakeholder Perspective*
- Hinoult M. (2007). *The Leuven Knowledge Economy Region*
- Holland High Tech (2013). *Roadmap HTSM Security*
- HSD (2012). *Masterplan 2013 – 2014*
- HSD (2013). *Ledenlijst*
- ICT-Innovatieplatform ‘Veilig Verbonden’ (2013). *Bundel Matchmaking Cyber Security Onderzoek (deelnemerslijst)*
- ICT Office (2012). *Cyber Security Manifest 2012*
- Kaspersky (2013). *Special Report on Espionage: Who’s spying on you? No business is safe from cyber-espionage*
- Kaspersky (2013). *Global IT Risks Survey 2013: IT Security Fighting the Silent Threat*
- Kaspersky (2013). *The Threat Landscape, A practical guide from the Kaspersky Lab Experts*
- Marketsandmarkets (2012). *Cyber-Security Market: Advanced Technologies, Geographical Analysis and Worldwide Market Forecasts*
- Ministerie van Veiligheid en Justitie (2013). *De Nationale Cybersecurity Strategie (NCSS2)*
- National Defense Magazine (2012). *Top Five Threats to National Security in the Coming Decade*
- National Forensic Institute (2013). *Trends, Challenges and Strategy in the Forensic Science Sector*
- NATO Emerging Security Challenge Division (2012). *The World in 2020 – Can NATO Protect Us? The Challenges to Critical Infrastructure*
- Nederland Ondernemend Innovatieland (2008). *Maatschappelijke Innovatie Agenda Veiligheid*
- Nederland Ondernemend Innovatieland (2008). *Maatschappelijke Innovatie Agenda Veiligheid: Bijlagen*
- NIDV (2013). *Ledenlijst via <http://www.nidv.eu/nl-NL/pages/1176/Deelnemers-overzicht.aspx>*
- Onderzoeksraad voor de Veiligheid (2012). *Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt – rapport*
- Onderzoeksraad voor de Veiligheid (2012). *Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt – aanbevelingen*
- Panteia, Rotterdam School of Management, Erasmus Universiteit (2013). *Innovatie- en Concurrentiemonitor 2012*
- PwC (2011). *Cyber Security M&A*
- RAND Corporation (2013). *Demographics and the Changing National Security Environment*
- Sempere, C.M. (2011). *EUSECON: A survey of the European security market*
- Symantec (2013). *The Northon Cyber Report*
- Symantec (2013). *Security Threat Report 2013 – Volume 18 Threat Activity Trends*
- Symantec (2013). *Security Threat Report 2013 – Volume 18 Threat Activity Trends Appendix*
- Sturgeon T.J., Industrial Performance Center, Massachusetts Institute of Technology (2000). *How Silicon Valley came to be*
- Strubinger, R. (2012). *Trends in Digital Forensics & Incident Response*

- The Hague Security Delta (2013). *Jaarplan – Concept 1.5: The Hague Security Delta 2014*
- TNO (2012). *Stedelijke Veiligheid*
- TNO (2013). *Roadmap HTSM Security, revised version 2013*
- Toffler Associates (2008). *Five Critical Threats to the Infrastructure of the Future*
- Transparency Market Research (2013). *Forensic Technologies Market: Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2013-2019*
- Triarii (2012). *De Nederlandse Defensie- en Veiligheid gerelateerde industrie*
- UN-Habitat (2007). *Enhancing Urban Safety and Security: Global Report on Human Settlements*
- Van Drunen M., Erasmus Universiteit Rotterdam (2007). *Samen werken aan succes? De praktische werking van de Triple Helix binnen Brainport*

GECONTACTEERDE PERSONEN

a/ Overheid

Ministerie van Defensie	Erik Akerboom	Secretaris Generaal
Ministerie van EL&I	Pieter Taal	Commissioner Military Production
	Heleen de Brabander-Ypes	Senior Advisor Industrial Participation
Ministerie van V&J	Pieter Cloo	Secretaris Generaal
	Wil van Gemert	Directeur Cyber Security
Gemeente Den Haag	Henk Kool	Wethouder
Gemeente Enschede	Peter den Oudsten	Burgemeester, voorzitter veiligheidsregio Twente
	Erdo Smit	Bestuursadviseur, samenwerking ministerie en HSD
	Herman Meuleman	Secretaris, programmamanager veiligheidsregio Twente
Gemeente Tilburg	Peter Noordanus	Burgemeester
Innovation Quarter	Rinke Zonneveld	Algemeen Directeur

b/ Onderwijs en onderzoek

Haagse Hogeschool	Rob Brons	Voorzitter College van Bestuur
TU Delft	Karel Luyben	Rector magnificus en vice-voorzitter College van Bestuur
	Pieter van Gelder	Professor ‘Safety and Security Science’
	Jan van den Berg	Professor ‘Cyber Security’
Universiteit Leiden	Carel Stolker	Rector magnificus en voorzitter College van Bestuur
	Jouke de Vries	Decaan Campus Den Haag
TNO	Kees d’Huy	Businessline Manager Security & Protection

c/ Ondernemingen & organisaties

Deloitte	Dick Berlijn	Senior Board Advisor
DITTS	Guus Sluijter	Directeur
	Pieter Tops	Lid College van Bestuur
	Menno van der Marel	Directeur en medeoprichter
Fox-IT	Eelco Blok	CEO
KPN / Cyberraad	Bob Toetenel	Directeur Executive Relations
	John van Vianen	Directeur Zakelijke Markt, lid Executive Team KPN en CEO KPN Business Market
	Pieter Cobelens	Liaison Manager
M4B (Military Talent for Business Solutions)		
NFI	Marcel van der Steen	Directieadviseur
	Elise van den Heuvel	Programmamanager CSI Innovations
Siemens NL	Ab van der Touw	CEO
	Max Remerie	Business Development Manager
Thales	Aart Jan Smits	Directeur Nationale Veiligheid, Business Development Director
Trigion	Richard Franken	Commercieel directeur

BIJLAGE

a/ Overzicht werkzame personen en belangrijkste werkgevers per deelsector³⁰

Security Triple Helix: 13 400 werkzame personen

- National Security (6 000 WZP):
 - AIVD, Europol, Min V&J, MIVD, Nationale Politie, Nato (incl C3 Agency), NCTV, OPCW, TNO Defensie en Veiligheid,...
- Cyber Security (2 100 WZP):
 - Alcatel Lucent, Centric Software Engineering, Deloitte, Fox-IT, Getronics, KPMG, KPN, NCI, NCSC,...
- Critical Infrastructure (1 000 WZP)
 - Deltares, Onderzoeksraad vd Veiligheid, Rijkswaterstaat, Siemens, TNO, Verebus Engineering,...
- Urban Security (3 400 WZP)
 - SBI-80 bedrijven (onder andere Capricorn, Securitas, Trigion, enz.) en overige partijen als Applicom, Lobeco,...
- Forensics (700 WZP)
 - NFI, Politie Forensische Opsporing,...
- Education & Research (200 WZP)
 - Haagse Hogeschool, HTU Delft, UL – Campus Den Haag,...

Overige: 12 200 WZP werkzame personen

- Overheid (6 600 WZP)
 - Gerelateerde afdelingen bij ministeries (Binnenlandse zaken, Defensie, Justitie), ...
- Veiligheidsdiensten (5 100 WZP)
 - Brandweerkazernes, politiebureaus,...
- Overig (500 WZP)
 - Ambassades, KvK's, Provincie Zuid-Holland, Stichtingen,...

³⁰ Opgemerkt dient te worden dat niet elk bedrijf / iedere organisatie in een enkele vaste categorie kan worden geplaatst.

b/ Benchmark andere clusters

Tabel 1 : Benchmark andere bekende clusters

Cluster	Regio, land	Sectoren	Aantal deelnemers	Centrumfunctie	Samenwerking (organisch vs regulering)
Aerospace Toulouse	Toulouse, Frankrijk	Aerospace	550 bedrijven (1 600 totaal)	Ja, triple helix; vooral Airbus, overheid etc.	Regels en voorwaarden voor sommige ondersteuning
Brainport	Eindhoven, Nederland	HTSM, lifesciences, agrifood	300 bedrijven	Ja triple helix; vooral Philips, in mindere mate ASML, NXP etc. TU/e, overheid	Projectbasis, met regels
DITSS	Eindhoven / Brabant, Nederland	HTSM, veiligheid	10 partners, 20 betrokken organisaties	Ja, triple helix; BP, Universiteiten, gemeenten / provincie	Organisch per project; binnen project regels vastgelegd
DPI	Eindhoven, Nederland	Chemie	30 bedrijven, 40 kennisinstellingen	Ja, triple helix	Vast
Leuven LRD	Leuven, België	HTSM (wetenschap)	Meerdere honderden (enkel al +100 spin-offs)	Ja, triple helix: sterk verankerd met horizontale en verticale netwerken zoals ECAE en DSP Valley	Projectbasis, met regels (zeer sterke regie op investeringsprogramma)
Oost NV	Gelderland / Overijssel, Nederland	Agrofood, High Tec, Life Sciences en grondbeleid	166 participaties (samenwerkingen) en 2 200 betrokken bedrijven	Ja, met name overheid	Vast; strenge regels voor financiering
Ottawa	Ottawa, Canada	Veiligheid	Ong. 200 (400 in directory)	Ja, zoals voormalige OCRI	Veelal organisch
San Diego	San Diego, Verenigde Staten	Veiligheid, maar deelnemers over sectoren heen	-	Ja, in vorm van adviesraad met daarin triple helix	Vast patroon in facilitatie
Signum	Berlijn / Brandenburg, Duitsland	Veiligheid	Ong. 127	Specifieke trekkers in subsectoren	Afhankelijk van subsector, soms los, soms meer gereguleerd
Silicon Fen	Cambridge, UK	HTSM (elektronica, software en biotechnologie)	> 1500 high tech firma's	Ja, triple helix	-
Silicon Valley	San Francisco, Verenigde Staten	HTSM (vooral ICT)	150 grotere, 7 000 kleine organisaties (niet allemaal deel van de cluster)	Ja, meerdere centra: Stanford University en een twintigtal grote organisaties	Veelal organisch

Bron : Policy Research Corporation

c/ HSD Masterplan 2013-2014

Om het snelgroeiend internationaal economisch cluster rond Den Haag op het gebied van veiligheid verder uit te bouwen, heeft HSD een Masterplan uitgewerkt. In dit Masterplan zijn concrete initiatieven opgenomen om de clusterontwikkeling te verzekeren en versnellen.

Tabel 2 : Initiatieven uit het HSD Masterplan 2013 – 2014 (1/2)

Project	Trekker	Omschrijving
Nationaal Veiligheidsinnovatie Centrum		
Real Time Intelligence Lab	Thales, TNO	In het Real Time Intelligence Lab worden door open innovatie en co-creatie door overheid, bedrijven en kennisinstellingen de concepten, technieken en innovaties bedacht, getest en beproeft ten behoeve van actuele en toekomstige veiligheids- en crisismanagementvraagstukken
Cyber Incident Experience Center	Fox-IT	Het Cyber Incident Experience Center is een setting waarbij operationele ervaring van hedendaagse dreigingen en incidenten binnen enkele weken inzichtelijk wordt gemaakt, zodat hier direct lessen uit kunnen worden getrokken
Serious Gaming Lab	HCSS	Het Serious Gaming Lab is een omgeving waarin rondom visie- en conceptontwikkeling en ramp- en crisismanagement het mogelijk wordt gemaakt om voor veiligheidsvraagstukken een concrete samenwerking tot stand te brengen (publiek-privaat, lokaal & regionaal, regionaal & bovenregionaal, nationaal & internationaal)
Crisis simulatiecentrum	Crisisplan	Het crisis simulatiecentrum heeft als doel bedrijven en (semi)publieke organisaties de gelegenheid te bieden te trainen op strategisch, tactisch en/of operationeel niveau met behulp van de state of the art technologie die ingezet wordt op het terrein van het ondersteunen van besluitvorming, het ontwikkelen van handelingsperspectieven, het duiden van informatie, communicatie, het analyseren van mediaberichtgeving en het visualiseren van deze data
ENCS	Alliander	Het European Network for Cyber Security is een nieuw kenniscentrum gericht op onderzoek, testen, kennisdelen en training op het gebied van cyber security voor vitale infrastructuur
Innovatiehuizen HSD PID project	HSD	De vijf innovatiehuizen van het HSD Pieken in de Delta (PID) project worden ten behoeve van de continuïteit geïntegreerd en geïncorporeerd in HSD en het Nationale Veiligheidsinnovatie Centrum
Onderwijs / Arbeidsmarkt (Human Capital)		
Cyber Security Academy	Gemeente Den Haag	Het doel is een brede Cyber Security Academy met een internationale hoogstaande reputatie, die zijn kracht ontleent aan een intensieve 'Triple Helix' samenwerking van overheid, bedrijfsleven en kennisinstellingen in Cyber Security
HSD Cyber Security Traineeship	Fox-IT	Het HSD Cyber Security Traineeship heeft als doel het op korte termijn opleveren van cyber security specialisten; het traineeship kent zowel een publiek (NCSC, Europol) als een privaat (Fox-IT, KPN en andere) onderdeel
Overige faciliteiten		
Incubator Faciliteiten	Fakton, HSD Office	Een incubatieomgeving in het Nationaal Veiligheidsinnovatie Centrum waarin ook kleine innovatieve partijen zich gemakkelijk kunnen aansluiten dan wel vestigen; diensten en technologische deeloplossingen kunnen er ontwikkeld en getest worden in een omgeving waar ook de eindgebruiker aanwezig is
Bedrijfsverzamelgebouw	Fakton, HSD Office	Hierin kunnen startups en MKB bedrijven die relatie hebben tot de veiligheidssector zich vestigen

Bron : Policy Research Corporation

Tabel 3 : Initiatieven uit het HSD Masterplan 2013 – 2014 (2/2)

Project	Trekker	Omschrijving
Living Labs		
CSI The Hague II	NFI	In 2011 heeft NFI een revolutionair CSI Lab in gebruik genomen; het is een demonstratie- en trainingsfaciliteit om virtueel een plaats delict te onderzoeken; de eerste resultaten zullen worden doorontwikkeld tot vermarktbaar producten en diensten
Living Lab Integrale Gebiedsbeveiliging	Gemeente Den Haag	De Internationale Zone in Den Haag wordt momenteel beveiligd met aparte fysieke veiligheidsmaatregelen voor elk gebouw en elk event; HSD zal de Internationale Zone inzetten als 'living lab' voor integrale gebiedsbeveiliging; bewezen technologische oplossingen zullen worden geïmplementeerd om de beveiliging efficiënter en met minder overlast voor de omgeving op te zetten
Living Lab Sociale Veiligheid	Twijnstra Gudde, TNO	Een nieuw instrument om innovatie in de sociale veiligheid in te zetten om problemen op te lossen; op de locatie in de openbare ruimte waar het probleem zich manifesteert, is een testomgeving gecreëerd voor experimentele maatregelen ter verbetering van veiligheid en leefbaarheid
HSD Office		
Communicatie & Public Affairs	HSD	HSD Office bouwt aan duurzame relaties van HSD-partners voor gezamenlijke belangen en doelstellingen; een HSD alignment- en communicatieplan is opgesteld
Internationale activiteiten / acquisitie	Gemeente Den Haag, HSD Office	Gezamenlijke initiatieven van partners om het veiligheidscluster internationaal op de kaart te zetten; het gaat hierbij bijvoorbeeld over het initiëren van een deelnemen aan inkomende en uitgaande handelsmissies of het werven van relevante conferenties en beurzen voor de regio
MKB Desk	HSD Office, Syntens	De MKB Desk staat ondernemers bij met praktische hulp en advies, met name op bedrijfskundig en financieel vlak en bij innovatietrajecten; adviseurs zoeken samen met de ondernemers naar de beste oplossing en begeleiden hen bij de zoektocht naar kapitaal; partner Syntens staat in voor de MKB Desk voor de gehele topsector HTMS
Ontwikkelingsmaatschappij / HSD Development	Gemeente Den Haag, HSD Office	In functie van te nemen beslissingen zal aansluiting georganiseerd worden met de Regionale Ontwikkelingsmaatschappij

Bron : Policy Research Corporation