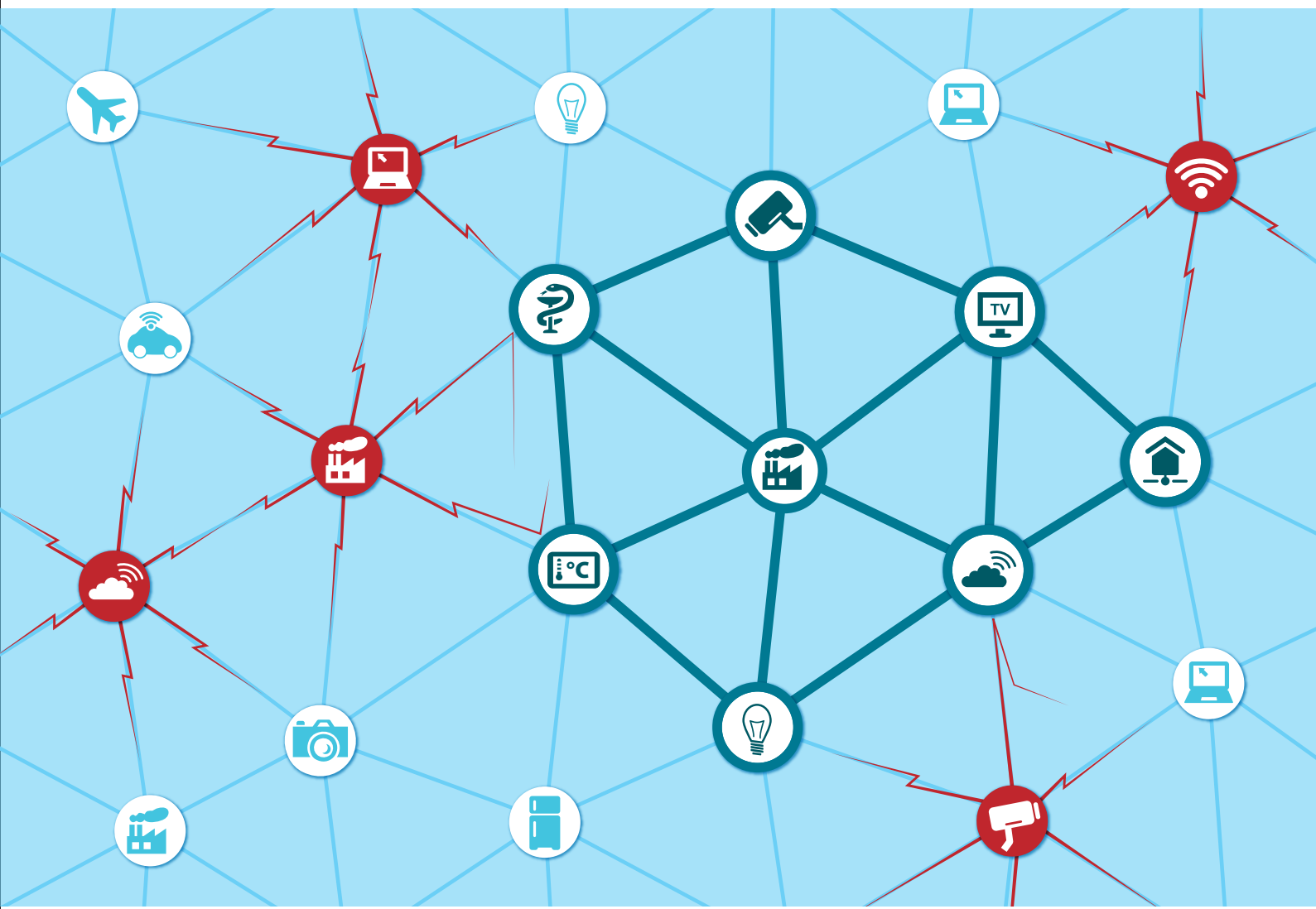
Verkenning van Nut, Noodzaak en Haalbaarheid van een Nationaal Cybertestbed



TNO innovation for life

HSD The Hague Security Delta

MRDH METROPOOLREGIO ROTTERDAM DEN HAAG

Verkenning van Nut, Noodzaak en Haalbaarheid van een Nationaal Cybertestbed

CONTENTS

1 INLEIDING

De wereld digitaliseert, iedereen en alles wordt dankzij het internet met elkaar verbonden. Dit biedt overheden, bedrijven en andere organisaties geweldige kansen om efficiënter en effectiever te kunnen communiceren en acteren, lokaal en globaal. De vitale infrastructuur in steden wordt 'slim' en kan met sensoren (het Internet of Things) de verkeersdoorstroming verbeteren. Het energienetwerk wordt 'slim', de sluis wordt op afstand bediend en patiëntgegevens worden real-time gedeeld tussen de hartslagmeter en de specialist. Stroomuitval, geblokkeerde ziekenhuisnetwerken, gegevensmanipulatie en platgelegde internetsites tonen aan dat diezelfde digitaliseringsslag ons kwetsbaar maakt.

De veiligheid en betrouwbaarheid van ons digitale domein is cruciaal en een randvoorwaarde om Nederland als 'Digital Gateway to Europe' te positioneren. Bezien de toenemende kracht van de internationale cybercriminaliteit kunnen we niet alles aan de markt overlaten. En als we niet alle cyber attacks kunnen voorkomen, is weerbaarheid (resilience) dan het nieuwe toverwoord? Liggen hier ook (internationale) economische kansen voor Nederland?

Tijdens bezoeken van diverse Nederlandse organisaties aan het Japanse Control System Security Center (CSSC) ontstond het initiatief voor een verkenning naar een soortgelijk cyber testbed in Nederland. Het CSSC is een voorbeeld hoe –in triple helix verband– wordt samengewerkt om de Japanse vitale infrastructuur veiliger te maken en daarmee meer weerbaar. Tegelijkertijd ondersteunt het de Japanse export door het certificeren van Japanse producten.

Is er een nut en noodzaak voor Nederlands cyber testbed? Welke functies zou het kunnen bieden? Wat is de focus en is het haalbaar? Om hierop een antwoord te geven heeft de gemeente Den Haag (vanuit de Metropoolregio Rotterdam Den Haag) aan The Hague Security Delta gevraagd om in samenwerking met TNO een verkenning te doen. De uitkomsten van de verkenning vindt u in deze publicatie en werden op 14 februari 2017 in een slotconferentie gepresenteerd.

2 AANPAK

Om nut, noodzaak en haalbaarheid van een Nationaal Cybertestbed te onderzoeken is gekozen voor een aanpak conform het voorstel uit de 'voorverkenning' uitgevoerd door HSD en TNO met de volgende fasen (en deliverables richting de subsidieverstrekker):

1. analyse stakeholders en behoeften (2de en 3de kwartaal 2016)
2. onderzoek bestaande initiatieven en internationale testbeds (2de en 3de kwartaal 2016)
3. uitwerken business case en commitment partijen (4de kwartaal 2016)
4. projectplan ter realisatie (4de kwartaal 2016)
5. slotevenement (1ste kwartaal 2017)

Het team bestond uit de door HSD aangestelde kwartiermaker en TNO experts en werd afhankelijk van de activiteiten aangevuld met andere inhoudelijke experts.

Het gehele traject is begeleid via een maandelijkse adviesraad met vertegenwoordigers uit de Metropoolregio Rotterdam Den Haag, TNO, HSD en de ministeries van Economische Zaken en Veiligheid & Justitie (op persoonlijke titel). Ook werd de status gepresenteerd en besproken in het bestuur van HSD.

Om inzicht te krijgen in de behoefte zijn er in het 2de kwartaal van 2016 naast deskresearch interviews gehouden met vertegenwoordigers uit de vitale sectoren, de overheid, kennisinstellingen en security- en ICT bedrijven. Ook zijn bestaande testfaciliteiten bekeken en werd onderzoek gedaan naar (internationale) testbeds. Tegelijkertijd vond een inventarisatie plaats van bestaande cybersecurityleveranciers in Nederland. Ook vond een meta-analyse plaats van bestaande marktonderzoeken om meer gevoel te krijgen over de grootte van de markt en de te verwachten trends. De belangrijkste conclusies zijn meegenomen in deze verkenning.

Naast motieven voor een Nationaal Cybertestbed (de 'waarom' vraag) werd onderzocht naar 'wat' het testbed zou moeten leveren. Het 'wat' werd vormgegeven in een menukaart van functies in het 3de kwartaal van 2016. Tijdens een workshop in september met vertegenwoordigers van vitale-infrastructuurpartijen, de overheid en andere experts is de menukaart aangevuld en is een eerste aanzet gegeven tot de invulling van het testbed (het 'hoe'). Parallel werd met security providers en securityafdelingen van vitale-infrastructuurorganisaties gesproken over een mogelijke rol in het testbed. In verband met de aandacht voor cyberweerbaarheid van steden vonden ook diverse overleggen plaats met betrokkenen van gemeenten, resilient city organisaties, (lucht-)havens en de metropoolregio (in het kader van de zgn. Rifkin's Next Economy roadmap MRDH).

Na de verdere focussering, is er vanaf het 4de kwartaal van 2016 met experts gewerkt aan de technische invulling van het testbed en heeft het team een inschatting gemaakt van de investeringen, de operationele kosten en mogelijke opbrengsten. De haalbaarheid draait uiteindelijk om een harde vraag enerzijds en investeringen anderzijds om tot een haalbare business case te kunnen komen.

Op 14 februari werden op uitnodiging van de subsidieverstrekker de resultaten bekend gemaakt over het nut, de noodzaak en de haalbaarheid tijdens een slotconferentie op de HSD campus.

3 OMGEVING

Nut en noodzaak van een Nationaal Cybertestbed zijn vanuit een economisch en vanuit een veiligheidsperspectief bekeken.

3.1 VEILIGHEID

Cybersecurity is een voorwaarde voor de doorontwikkeling van de huidige gedigitaliseerde maatschappij en het realiseren van economische groei. Barack Obama, voormalig president van de VS zei hierover: “America’s economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.”

Dit geldt ook voor de Nederlandse situatie, zoals blijkt uit de door het NCSC geproduceerde Cybersecuritybeelden van de laatste jaren. Vanuit verschillende kanten worden overheden, private organisaties en burgers bedreigd. Cybersecuritybeeld Nederland 2016 benadrukt nog specifiek de zorgelijke situatie voor het MKB: Het MKB is belangrijk voor Nederland. Veel ketens bevatten bedrijven uit het MKB, zo ook ketens binnen de vitale processen. Qua cybersecuritymaatregelen blijft deze groep achter. Dat betekent een risico voor de vitale processen en daarmee voor de Nederlandse samenleving.

Betere publiek-private samenwerking en meer aandacht voor innovatie zijn essentieel voor het behouden van een veilige infrastructuur in Nederland. Dit laatste wordt ook benoemd in de Nationale Cyber Security Strategie 2: De technologische ontwikkelingen in het digitale domein gaan snel. Om daarop te kunnen anticiperen, is innovatiebeleid cruciaal. Innovatie ontstaat daar waar creatieve en kundige mensen elkaar ontmoeten. Dat alleen is niet voldoende. Meer coördinatie op vraag en aanbod is gewenst. Dit wordt bereikt door bestaande innovatie-initiatieven en het topsectorenbeleid aan elkaar te verbinden. Hieraan is inmiddels invulling gegeven door het oprichten van Dcypher, het Nederlandse platform voor onderzoek en educatie op het gebied van cybersecurity. Een platform dat bedrijven en overheden ondersteunt bij het testen, certificeren en veilig implementeren van nieuwe innovaties in de operationele praktijk is er echter nog niet.

Het Nationaal Cybertestbed kan hier een belangrijke rol vervullen. Het Nederlandse cyberlandschap is momenteel nog sterk gefragmenteerd. Door meerdere partijen is aangegeven dat het noodzakelijk is dat de samenwerking en kennisdeling wordt geïntensiveerd. Binnen de Information Sharing and Analysis Centres (ISAC's) vindt wel kennisdeling plaats, maar dat gaat beperkt over sectoren heen en is voornamelijk gericht op actuele dreigingen en kwetsbaarheden. Er is ruimte voor een nieuw platform waar kennisinstituten, vitale infrastructuur managers, ICT-bedrijven en startups samenwerken om innovatie rondom nieuwe cybersecuritytechnologieën en methodes te versnellen en door (zelf)regulering en het toetsen van eisen de maatschappelijke risico’s worden geminimaliseerd.

3.2 ECONOMISCHE KANSEN

Nederland staat bekend om haar uitstekende logistiek en infrastructuur en haar strategische positie binnen de Europese Unie, en wordt daarom ook wel 'Gateway to Europe' genoemd. Dit geldt ook voor de digitale variant. Aangezien Nederland een goede positie heeft opgebouwd met goed functionerende en state-of-the-art digitale infrastructuur, een levendige IT sector die toponderzoek doet, samenwerking tussen bedrijven, overheid en kennisinstelling op gebied van innovatie en een samenleving die nieuwe ICT ontwikkelingen in hoog tempo omarmt. De Nederlandse overheid zet in op het zijn van de 'Secure Digital Gateway to Europe'. Deze gunstige omstandigheden hebben er voor gezorgd dat vele IT (Security) bedrijven zich in Nederland hebben gevestigd of zijn ontstaan.

De omvang en groei van de cybersecuritymarkt is moeilijk in te schatten. De belangrijkste redenen zijn de relatieve nieuwheid, niet eenduidige definities van cybersecurity, en het rapporteren van cybersecurity als onderdeel van bestaande ICT uitgaven. Geschat wordt dat de huidige uitgaven aan cybersecurity in Nederland liggen tussen de 0,9 en 1,8 miljard euro. Dit is tussen de 0,13% en 0,26% van het BNP en tussen de 1,3% en 2,6% van de jaarlijkse ICT uitgaven in Nederland door de overheid en het bedrijfsleven.

Nederland verdient zo'n 4,5% van het BNP (rond de 30 miljard euro) aan ICT. Dit is vergelijkbaar met de landen om ons heen. Andere landen waar hardware wordt geproduceerd hebben een hoger percentage. Hetzelfde geldt bv.. voor Ierland en India waar ICT dienstverlening hard is gegroeid. Nederland importeert relatief veel ICT hardware en diensten (50 miljard euro waarvan 88% hardware en 12% diensten) en exporteert relatief weinig. De ICT markt Nederland zelf bedraagt rond de 70 miljard euro (capex en opex).

In het rapport "Digitaal Droge Voeten"[1] wordt gepleit om 10% van het ICT budget uit te geven aan cybersecurity. Dit percentage is gebaseerd op benchmarks van onder meer Singapore en Duitsland. In de praktijk zou dit een uitgave van 3 a 7 miljard euro per jaar betekenen. Internationale rapporten wijzen op een verlies van 1,5% van het BNP door toedoen van cybercrime, oftewel 10 miljard euro in Nederland. Deloitte bepaalt de 'cyber value at risk' in Nederland op 7,5 miljard euro.

Er lijkt een mismatch lijkt te zijn tussen wat we uitgeven en wat we zouden moeten uitgeven. Waar we tussen de 0,9 en 1,8 miljard euro uitgeven zou dit tussen de 3 en 10 miljard euro moeten zijn om de cyber risico's onder controle te hebben. Waaraan we dit bedrag moeten uitgeven is ook onderhevig aan gebrek aan helderheid in de statistieken. Wel zien we globale trends die –bezien de Nederlandse digitaliseringsagenda– ook in Nederland van toepassing zijn. De security services markt op zich verwacht een samengestelde jaarlijkse groei van 16% tot en met 2020. Qua samengestelde jaarlijkse groei is de cybersecuritymarkt voor het Internet of Things (IoT) de grootste met 33%.

Omdat cybersecurity geen standaard onderdeel is van de meeste MBO, HBO en WO opleidingen, is awareness en kennis over dit onderwerp vaak beperkt. Er is daarom behoefte aan het verbeteren van awareness, zowel bij burgers als binnen bedrijven en overheden. Ook zien we dat er een groot tekort aan ICT professionals is (11.000 in 2016) en dat het aantal niet ingevulde vacatures in cybersecurity verder rap zal toenemen (meer dan 1.500 vacatures verwacht in 2016).

[1] Nederland Digitaal Droge Voeten, Herna Verhagen, in opdracht van de Cyber Security Raad, 2016.

Duidelijk is dat veel bedrijvigheid kan ontstaan op al deze onderwerpen. Een Nationaal Cybertestbed kan hierbij als katalysator functioneren door partijen bij elkaar te brengen en op termijn een internationaal podium te bieden.

4 FOCUS

Cybersecurity is een breed thema met grote verschillen tussen systemen en gebruikscontexten. De bouw en inrichting van een Nationaal Cybertestbed vraagt daarom uit overwegingen van realiseerbaarheid om specifieke keuzes. In dit hoofdstuk onderzoeken we met welke keuzes een Nationaal Cybertestbed van start zou moeten gaan. We kijken hierbij naar verschillende functies, doelsystemen en naar contexten van gebruik.

4.1 FUNCTIES

In de opzet voor een Nationaal Cybertestbed onderscheiden we vijf potentiele categorieën van dienstverlening. In de workshop die is gehouden met stakeholders zijn deze verder uitgewerkt:

1. Testen
    a. Testen en valideren van hard- en/of software
    b. Testen en valideren van cybersecuritytechnologie
    c. Geïsoleerde testomgeving voor risicovol testen (bijvoorbeeld malware)
2. Zelfregulering en certificeren
    a. Bijdragen aan zelfregulering door middel van het opstellen van requirements en normering
    b. Certificering van hard- en/of software
3. Innoveren
    a. Open CyberLab
    b. Verbinden kennispartijen, vitale infra managers en ICT
    c. Samenwerking met MKB en start-ups
4. Trainen en opleiden
    a. Praktijkopdrachten voor trainingen
    b. Opleiden voor nieuwe technologieën
    c. Sector/keten-breed oefenen
5. Awareness
    a. Awareness bij overheid, bedrijfsleven en publiek
    b. Loketfunctie voor MKB en overheid

Een testbed richt zich op de eerste categorie. De interviews en de workshop laten zien dat er ook behoefte is aan de diensten in de andere vier categorieën. Een testbed biedt een platform waarop deze diensten aanvullend op de testactiviteiten kunnen worden ontwikkeld en aangeboden. De focus zal met name worden gelegd op de functies zelfregulering en certificering, het versnellen van innovaties, en het uitvoeren van testen die hiervoor nodig zijn. Als kennisplatform kan een Nationaal Cybertestbed bijdragen aan projecten en een platform bieden aan andere partijen voor dienstverlening op de andere functies.

4.2 DOELSYSTEMEN

Een onderverdeling van doelsystemen waar een Nationaal Cybertestbed zich op kan richten is:

- Kantoorautomatisering/bedrijfsnetwerken
- SCADA/Industrial Control Systems
- Telecom infrastructuren
- Online dienstverlening en transacties
- Internet of Things (IoT)

Om te bepalen voor welke doelsystemen een Nationaal Cybertestbed de meeste meerwaarde kan creëren zijn deze vijf kwalitatief beoordeeld door experts van TNO aan de hand van vier criteria:

1. Marktbehoefte: zijn er partijen die behoefte hebben aan securitydiensten die worden geleverd door het testbed?
2. Right-to-play: levert een Nationaal Cybertestbed diensten die niet worden aangeboden door bestaande commerciële dienstaanbieders?
3. Investeringsnoodzaak: is een substantiële investering nodig voor het inrichten van een testbed, waardoor het voor individuele partijen niet haalbaar is om een dergelijke investering te doen (aanbodbundeling).
4. Technische realiseerbaarheid testbed: is het mogelijk om een representatieve laboratoriumomgeving in te richten (hardware, configuraties, netwerk/systeem activiteit) die breed inzetbaar en herbruikbaar is voor meerdere partijen en projecten.

In tabel 1 zijn de doelsystemen aan de hand van deze criteria beoordeeld. Hoewel voor alle doelsystemen toepassingen denkbaar zijn waar een Nationaal Cybertestbed een zinvolle bijdrage kan leveren, geeft deze classificatiewijze een goed beeld van de doelsystemen waar de toegevoegde waarde het grootst is.

Tabel 1: Afwegingskader doelsystemen

	Marktbehoefte	Right to play	Investeringsnoodzaak	Realiseerbaarheid
Kantoorautomatisering	++	--	-	++
SCADA/Industrial Control Systems	+	+	++	--
Telecom infrastructuren	--	+	+	+/-
Online dienstverlening en transacties	++	--	-	++
Internet of Things	++	+	+/-	++/+

Er is geen right-to-play voor een Nationaal Cybertestbed bij kantoorautomatisering. Hetzelfde geldt voor systemen gericht op online dienstverlening. Dit zijn in het algemeen vrij standaard wereldwijd gebruikte systemen waarvoor voldoende commerciële aanbieders bestaan die zich richten op cybersecurity. Een testbed lijkt hier weinig toegevoegde waarde te bieden.

Telecominfrastructuren (mobiele netwerken en andere draadloze communicatieprotocollen als WIFI en Bluetooth) zijn een specifieke niche waarop veel grote internationale spelers en belangen zijn, maar waarvoor relatief weinig marktvraag wordt verwacht.

SCADA lijkt in eerste instantie wel een interessant doelsysteem. Vitale partijen in Nederland maken hier in cruciale systemen gebruik van, zoals bij sluizen en gemalen, het energienetwerk, of de watervoorziening. Hierdoor wordt een groot maatschappelijk en economisch belang gediend. Het nadeel is dat elk SCADA systeem vrijwel uniek is, waardoor voor elk initiatief een nieuw en uniek testbed moet worden ingericht. Ervaringen bij andere testbeds hebben laten zien dat hergebruik vaak niet mogelijk is. Voor sommige toepassingen kan het interessant zijn een specifiek systeem na te bouwen. In Singapore is dit bijvoorbeeld gedaan met een waterzuiveringssysteem. Om dit voor meerdere toepassingen te doen is zeer kostbaar. Het kan voor bepaalde omgevingen zeker nuttig zijn, maar lijkt minder goed te passen in het concept van een breed inzetbaar Nationaal Cybertestbed.

In oktober 2016 is door grote aantallen Internet of Things apparaten tegelijkertijd data te laten sturen een grote DDoS aanval uitgevoerd op een service provider in de verenigde Staten. Hierdoor waren een groot aantal websites lange tijd onbereikbaar. . Veel van deze IoT apparaten blijken slecht beveiligd. Er is echter geen incentive voor de producent of de consument om daar kosten voor te maken. Dit wordt door velen als een vorm van marktfalen gezien[2]. Voor een Nationaal Cybertestbed ligt hier een right-to-play uit veiligheidsoverwegingen. Maar ook de enorme vlucht die IoT de komende jaren zal nemen betekent dat hier veel economisch activiteit kan ontstaan. Afhankelijk van het gekozen IoT-apparaat (thermostaat versus auto) zal het meer of minder moeilijk en kostbaar zijn om een realistisch testbed te ontwikkelen. Speciaal op IoT gerichte telecom infrastructuren (zoals ZigBee of een LPWAN) kunnen als onderdeel van het doelsysteem meegenomen worden.

Op basis van deze analyse, die tot stand is gekomen op basis van de marktanalyse, gesprekken en de werksessie met stakeholders uit het domein, is gekozen voor IoT als primaire doelsysteem om mee te starten. Afhankelijk van hoe de vraag uit het veld zich ontwikkelt kan deze focus later worden bijgesteld of uitgebreid.

4.3 TOEPASSINGSDOMEINEN

Vanuit het maatschappelijke belang ligt een focus voor het Nationaal Cybertestbed op vitale infrastructuur voor de hand[3]. Het Ministerie van Veiligheid en Justitie heeft een lijst van vitale infrastructuren gemaakt op basis van de criteria: economische impact, aantal slachtoffers, maatschappelijke impact en keteneffecten. IoT speelt in vrijwel alle toepassingsgebieden inmiddels een rol, of zal daar de komende jaren een rol gaan spelen. Een specifiek voorbeeld van een omgeving waar IoT een vlucht neemt is Smart Cities. In vrijwel alle grote steden, zowel in Nederland als wereldwijd, lopen projecten om steden smart te maken zodat ze veiliger, duurzamer, gezonder, prettiger en bereikbaarder worden[4]. In deze transitie is een grote rol voorzien voor IoT en vooral voor de data die deze IoT levert. Vanwege de grote publieke belangen en de complexe vraagstukken kan het niet alleen aan de markt worden overgelaten om hiervoor veilige systemen te bouwen. Naast het bedrijfsleven is

[2] Bruce Schneier: “Your Wifi-connected thermostat can take down the whole internet. We need new regulations”, Washington Post, November 3, 2016
[3] Zie ook *Securing Critical Infrastructures in the Netherlands*, HSD rapport, 2015
[4] NL Smart City Strategie: the future of living: https://gsc3.city/smart-city-strategie/

een rol voor overheid en kennisinstituten essentieel. Het Nationaal Cybertestbed kan hier een verbindende en faciliterende rol vervullen.

4.4 CONCLUSIE FOCUS

Het Nationaal Cybertestbed richt zich in eerste instantie op de functie van testen, zelfregulering en certificering. Als primair doelsysteem is het zogenaamde Internet of Things gekozen binnen de context van de vitale infrastructuur in steden. Daar waar ‘cyber’ en het ‘Internet of Things’ samenkomen lijkt er behoefte aan een neutraal testbed.

5 TWEE SCENARIO'S

5.1 AMBITIE

De hiervoor beschreven bevindingen maken meer dan aannemelijk dat er ruimte is voor de ambitie om te komen tot wat we een Nationaal Cybertestbed noemen. De focus - *het cybersecure maken van IoT-systemen waar deze de kwetsbaarheid in Nederlandse steden raken*- wordt eveneens voldoende onderbouwd. Tegelijkertijd moeten vraag en financiële onderbouwing nog verder uitgewerkt worden.

Ambitie Nationaal Cybertestbed:
Het Nationaal Cybertestbed levert een grote bijdrage aan het cybersecure maken van IoT-systemen en het verminderen van de kwetsbaarheid van Nederlandse steden. Het NCT fungeert als kenniscentrum en verbindt partijen die IoT-systemen willen implementeren met kennisinstituten, universiteiten en bedrijven. Het Nationaal Cybertestbed is een samenwerkingsplatform voor bedrijven en overheden die met dit onderwerp aan de slag gaan. Het Nationaal Cybertestbed ontwikkelt zich tot een gezaghebbende speler op dit thema en is aanjager voor de zelfregulering en certificering van IoT cybersecurity. Het werkt nauw samen en deelt kennis op dit onderwerp met de beleidsmakers bij de Rijksoverheid en internationale partijen.

Het hebben van die ambitie is één, het realiseren ervan vraagt het een en ander. De hiervoor genoemde bevindingen maken aannemelijk dat HSD met haar partners een rol kan gaan spelen bij het cybersecure maken van IoT-ecosystemen. Daarvoor worden twee scenario's voorzien:

- Scenario 1: Het Nationaal Cybertestbed als Kenniscentrum
- Scenario 2: Het Nationaal Cybertestbed als Kenniscentrum en Facilitator

In het eerste scenario beschikt het Nationaal Cybertestbed niet over een eigen testfaciliteit, maar is vooral een kenniscentrum en samenwerkingsverband. Voor projecten en initiatieven waar technische faciliteiten nodig zijn zal gebruik worden gemaakt van bestaande testbeds bij andere organisaties.

In het tweede scenario worden door het Nationaal Cybertestbed voorzieningen ontwikkeld dan wel georganiseerd, waarop IoT-apparaten en systemen zelf kunnen worden getest op cybersecurityaspecten. Voor IoT bestaat een dergelijk testbed nu niet en voor individuele organisaties is de inrichting ervan niet haalbaar.

Voor beide scenario's geldt dat met concrete casuïstiek die wordt aangeboden door bijvoorbeeld KPN en de gemeente Den Haag snel de eerste stappen kunnen worden gezet.

5.2 HET NATIONAAL CYBERTESTBED ALS KENNISCENTRUM

Het Nationaal Cybertestbed verbindt vragende en aanbiedende partijen en fungeert als kennispartner. Het draagt in die rol bij aan de vijf genoemde functies: testen, zelfregulering en certificering, opleiding, innovatie en awareness. Om deze rol goed in te kunnen vullen zal het Nationaal Cybertestbed zelf een gezaghebbende speler moeten zijn die op basis van haar neutrale positie de functie van verwijzer kan vervullen. Het Nationaal Cybertestbed helpt vitale infrastructuurpartijen en steden bij het opstellen van

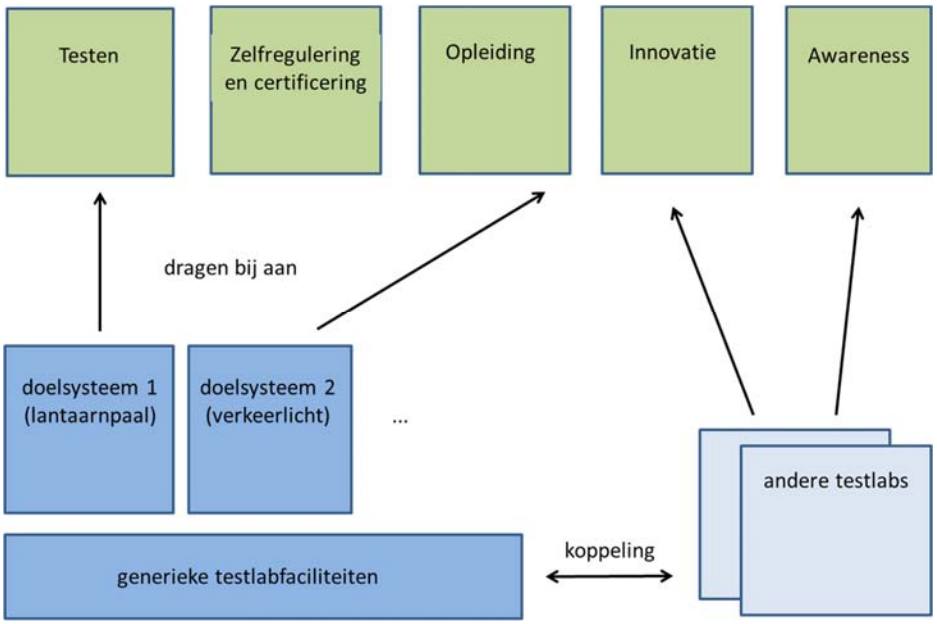
normen voor zelfregulering. Voor projecten en initiatieven waar technische faciliteiten nodig zijn zal gebruik worden gemaakt van bestaande testbeds bij andere organisaties.

5.3 HET NATIONAAL CYBERTESTBED ALS KENNISCENTRUM EN FACILITATOR

In het tweede scenario vervult het Nationaal Cybertestbed al deze rollen ook, maar heeft het daarnaast de beschikking over een eigen IoT cybersecuritytestbed waar partijen gebruik van kunnen maken om IoT-apparaten of -systemen te ontwikkelen, testen, certificeren, of om trainingen aan te bieden. Een dergelijke faciliteit bestaat momenteel niet in Nederland. Er zal een generiek testbed worden ontwikkeld dat een aantal basisfaciliteiten biedt, zoals:

- Simulatie van netwerken, systemen en activiteiten.
- Test tooling om relevante tests te kunnen uitvoeren.
- Gesimuleerde aanvallen op de IoT-systemen om kwetsbaarheden in kaart te brengen en cybersecuritymaatregelen te toetsen.
- Mogelijk een Kooi van Faraday om de opstelling te isoleren van de omgeving.

De testfaciliteit wordt beheerd door een neutrale organisatie. Op dit testplatform zullen verschillende IoT communicatieprotocollen worden aangeboden, zoals WIFI en LPWAN. Specifieke IoT-apparaten en -systemen kunnen (tijdelijk) worden toegevoegd aan dit basistestbed, bijvoorbeeld: intelligente lantaarnpalen, luchtvervuilingssensoren, camera's, verkeerslichten enzovoort. In een gecontroleerde laboratoriumomgeving kunnen deze worden onderzocht op verschillende cybersecurityaspecten.



Figuur 1: Functionele architectuur van het testbed

Daarnaast kan dit cybertestbed worden verbonden met fieldlabs waar deze IoT-systemen staan opgesteld, zodat deze ook in een meer realistische omgeving kunnen worden onderzocht. Het securitytestbed kan ook aan andere IoT-testbeds worden gekoppeld waar de focus ligt op functionaliteit (zoals mobiliteit in Helmond) of reeds specifieke toepassingen zijn gebouwd, zoals bij Rijkswaterstaat. In plaats van het opnieuw bouwen van zo'n omgeving, kunnen cybertests dan op afstand worden uitgevoerd.

We voorzien een testomgeving waar meerdere partners gezamenlijk projecten uitvoeren. Om deze reden is het realistisch om uit te gaan van een ongerubriceerde omgeving of van een rubricering die maximaal departementaal of commercieel vertrouwelijk is. Ook maakt een laag rubriceringsniveau hergebruik van systemen voor meerdere onderzoeken en projecten haalbaar. Voor meer vertrouwelijke testen of innovaties is een ander testbed nodig in een beveiligde omgeving.

6 HAALBAARHEID

Dit hoofdstuk beschrijft de scenario's in financiële zin. wat de te verwachten investeringen, kosten en opbrengsten zijn en hoe het gefinancierd kan worden. Voor verdere detaillering en onderbouwing verwijzen we naar de bijlage. Het eindigt met een voorstel voor vervolgstappen om de haalbaarheidsfase af te ronden.

6.1 NATIONAAL CYBERTESTBED SCENARIO'S

Zoals aangegeven zijn er twee scenario's uitgewerkt voor het nationaal cyber testbed: als 'Kenniscentrum' zonder eigen testfaciliteit en als 'Kenniscentrum en Facilitator' met een eigen testfaciliteit. Voor beide scenario's zijn aannames gemaakt rondom te verwachten investeringen, kosten en opbrengsten. De aannames en berekeningen zijn opgenomen in de bijlagen.

6.2 HET NATIONAAL CYBERTESTBED ALS KENNISCENTRUM

Het Nationaal Cybertestbed beschikt niet over een eigen testfaciliteit maar is vooral een kenniscentrum en samenwerkingsverband. Voor projecten en initiatieven waarvoor technische faciliteiten nodig zijn zal gebruik worden gemaakt van bestaande testbeds bij andere organisaties. De bemensing bestaat uit 2 fte (business development/operationeel management en kennismedewerker), de benodigde ruimte is beperkt (20m^2).

Behalve voor personeel en ruimte wordt er rekening gehouden met benodigde marketing uitgaven. De totale jaarlijkse uitgaven liggen rond de € 350.000. De initiële investering is beperkt (€ 50.000).

De operationele opbrengsten bestaan uit:

- Lidmaatschappen partijen voor toegang tot het kenniscentrum voor vragen en verbinden.
- MRDH lidmaatschap voor toegang tot het kenniscentrum voor andere partijen betrokken bij bv. Resilient/Smart City initiatieven voor vragen en verbinden.

De aanname is dat de opbrengsten van lidmaatschappen in het totaal zullen oplopen door de jaren heen maar dat er exploitatie tekorten blijven bestaan tussen de €100.000 en €200.000. Naast commitments voor lidmaatschappen is er zodoende mininaal € 500.000 nodig voor de initiële investering en voor de dekking van de exploitatie tekorten in jaar 1 t/m 3.

6.3 HET NATIONAAL CYBERTESTBED ALS KENNISCENTRUM EN FACILITATOR

Het Nationaal Cybertestbed beschikt naast het kenniscentrum en samenwerkingsverband over een eigen testbed waarop IoT-apparaten en -systemen kunnen worden getest op cybersecurityaspecten. Dit IoT-cybersecurity-testbed zal functioneren als schakelpunt van een federatie van bestaande testfaciliteiten van partners.

De bemensing bestaat uit 5 fte (business development/operationeel management, kennismedewerker, technici en administratie). De benodigde ruimte is 100m^2 en beschikt over technische infrastructuur, werkplekken en een loketfunctie.

Naast personeel en ruimte worden uitgaven gedaan voor marketing, het up-to-date houden van de technische infrastructuur, afschrijvingen en eventuele financieringskosten. De totale jaarlijkse uitgaven liggen rond de € 1.000.000. De initiële investering is rond de € 800.000 voor technische infrastructuur en opstartkosten.

De operationele opbrengsten zullen bestaan uit:

- Lidmaatschappen partijen voor toegang tot het kenniscentrum voor vragen en verbinden.
- MRDH lidmaatschap voor toegang tot het kenniscentrum voor andere partijen betrokken bij bv. Resilient/Smart City initiatieven voor vragen en verbinden.
- Afname voor testen:
  a. Vitale infrastructuursectoren Transport en Telecom.
  b. MRDH voor Resilient/Smart City initiatieven en als launching customer.
  c. Kennisinstellingen.
- Projecten en overige inkomsten (testen IoT apparatuur, inhuren faciliteit, resources, e.d.).

Voor lidmaatschappen zijn dezelfde aannames als in scenario 1 gemaakt. Voor afnames is uitgegaan van een significante groei richting het derde jaar. De project inkomsten zullen ook door de jaren heen stijgen.

O.b.v. deze aannames zijn er exploitatie tekorten aflopend van € 600.000 euro in het eerste jaar naar € 100.000 euro in het derde jaar. Naast commitments voor lidmaatschappen en afname is er zodoende minimaal rond de € 1.200.000 financiering nodig voor de initiële investering en voor de dekking van de exploitatie tekorten in jaar 1 t/m 3 om dit scenario haalbaar te maken.

6.4 FINANCIERING

Ter financiering van de initiële investering en aanvulling van eventuele exploitatie tekorten in de eerste 3 jaar zijn er diverse opties. Om diverse partijen in de Triple Helix op diverse manieren te kunnen betrekken en daarmee het draagvlak te verhogen, adviseert de verkenning om o.b.v een publiek-private variant de diverse partijen in staat te stellen in de hun passende vorm een bijdrage te kunnen leveren. Dit moet in de vervolgstap worden uitgewerkt.

Voorbeelden van mogelijke opties voor bijdragen -voor nu of in de toekomst- zijn:

- Bedrijfsleven/Vitale infrastructuur partijen:
  - Financiert mee met geld, apparatuur en resources (eventueel in ruil voor af te nemen diensten).
  - Koppelen eigen test lab aan Nationaal Cybertestbed in federatief model om capaciteit Nationaal Cybertestbed versneld op te bouwen en op termijn uit te breiden.
  - Doneren geld of apparatuur en stellen resources beschikbaar ‘om niet’ vanuit MVO.
- Gemeenten en/of MRDH en/of ministeries financieren en geven 3 jaar garantie op basisexploitatie via investeringen (mogelijk in vorm van subsidies).
- Kennisinstellingen leveren vraag met onderzoeksprogramma’s.

6.5 ADVIES

De totale investeringen incl. de operationele kosten in de eerste 3 jaar liggen bij het scenario ‘Kenniscentrum’ rond de 1 miljoen euro. O.b.v. te verwachten opbrengsten voorzien we een benodigde financiering van minimaal een half miljoen euro.

Bij het scenario ‘Kenniscentrum en Facilitator’ liggen de totale investeringen incl. de operationele kosten in de eerste 3 jaar rond de 4 miljoen euro. O.b.v. te verwachten opbrengsten voorzien we een benodigde financiering van minimaal 1,2 miljoen euro.

Het advies vanuit de verkenning is om o.b.v usecases te beginnen met het scenario ’Kenniscentrum’ en met een klein aantal partijen de rollen en de publiek-private financiering in te vullen. Ook dienen afspraken gemaakt te worden wiens testfaciliteiten beschikbaar worden gesteld aan het NCT. Dit houdt de optie open om aanvullend de mogelijke rol als ‘Facilitator’ (met eigen testfaciliteit) nader uit te werken en hier later alsnog toe te besluiten.

Als vervolgstappen adviseert de verkenning het volgende:

- Interesse polsen bij partijen, usecases inbrengen en commitments aangaan om de mogelijke haalbaarheid in te vullen.
- Met de partijen de haalbaarheid aannames, business case en financieringsbehoefte uitwerken.
- ‘Go/no go’ besluit met invulling rollen, commitments en plan van aanpak.

7 CONCLUSIE

De doelstelling van de verkenning was om te bepalen of er een nut en noodzaak is voor een nationaal cybertestbed en zo ja of het haalbaar is.

De toenemende cyberdreiging stelt de samenleving voor grote maatschappelijke uitdagingen. Er is vandaag te weinig kennis(deling), er zijn te weinig experts en er is te weinig awareness. Bovendien worden de afhankelijkheden in de vitale ketens en netwerken door de inzet van het Internet of Things alleen maar groter. Hierdoor worden ook sterke schakels kwetsbaar in de keten. De metastudie onderstreept dat gezien de mogelijke impact van cyber aanvallen er te weinig wordt geïnvesteerd in cybersecurity. Dit terwijl juist op het vlak van het Internet of Things de vraag enorm toe zal nemen.

De beschreven bevindingen maken meer dan aannemelijk dat er ruimte is voor de ambitie om te komen tot wat we een Nationaal Cybertestbed noemen. De focus –*het cybersecure maken van IoT-systemen waar deze de kwetsbaarheid in Nederlandse steden raken*–wordt eveneens voldoende onderbouwd. Het fungeert als kenniscentrum en verbindt partijen, het is een aanjager voor de zelfregulering en certificering van IoT cybersecurity met additionele werkgelegenheid als spin-off.

De vraag is of er genoeg vraag is voor een nationaal cyber testbed en daarmee of het ook haalbaar is. In de verkenning werden twee scenario's onderzocht: als 'kenniscentrum' en als 'kenniscentrum & facilitator' (met eigen testfaciliteit). Voor beide scenario's zijn inschattingen voor kosten en opbrengsten gemaakt.

De verkenning adviseert met het eerste scenario van start te gaan en om de rol van faciliator (eigen testfaciliteit) later en nader te onderzoeken. Voor de financiering van het NCT adviseren we een PPS-constructie om bijdragen van diverse partijen en daarmee draagvlak hand in hand te laten gaan.

Als vervolgstap stellen we voor dit advies te bespreken met geïnteresseerde partijen om tot commitments te komen aangaande de vraagstelling o.b.v. usecases, de invulling van het testbed en de financiering. Hierna kan worden overgegaan tot de concrete uitwerking en implementatie.

De stip op de horizon is de rol van aanjager en verbinder in het cybersecure maken van IoT-systemen in steden. Hiermee zal het nationaal cyber testbed economische activiteit ondersteunen: enerzijds als enabler van een cybersecure digitale infrastructuur (ook passend in de ambitie van Nederland als 'Digital Gateway to Europe'). Anderzijds direct als een eigen activiteit resulterend in werkgelegenheid en indirect als aanjager van omzet in het ecosysteem van Nederlandse cybersecure IoT oplossingen en diensten.

COLOFON

Uitgave van

The Hague Security Delta

Wilhelmina van Pruisenweg 104

2595 AN Den Haag

T-31 (0)7- 2045180

info@thehaguesecuritydelta.com

www.thehaguesecuritydelta.com

@HSD_NL

Projectmanagement en auteurs

Drs. Max Remerie (HSD)

Ir. Guido te Brake (TNO)

Druk

The Communication Company

Met dank aan alle personen die betrokken zijn

bij de totstandkoming van deze verkenning.