Rijksdienst voor Ondernemend Nederland

Overview IA Netwerk

Nationale veiligheid: internationale kansen en ontwikkelingen

Inhoud

Voorwoord

Geachte lezer,

Voor u ligt een overzichtspublicatie van het Innovatie Attaché Netwerk (IA Netwerk) over het thema Veiligheid. Dit overzicht geeft u een bloemlezing over internationale trends en ontwikkelingen op dit thema uit de landen waar het Ministerie van Economische Zaken Innovatie Attachés heeft gestationeerd. De Innovatie Attachés hebben aan de hand van de prioriteiten in Nederland bondige overzichten per land geschreven. Ze besteden aandacht aan de wetenschappelijke en technologische ontwikkelingen, toonaangevende bedrijven, kennisinstellingen en het overheidsbeleid in hun land.

Dit boekje is geschreven naar aanleiding van een bijeenkomst georganiseerd door het IA Netwerk en The Hague Security Delta op 21 april 2015 in Den Haag. Tijdens deze dag komen Nederlandse bedrijven en kennisinstellingen in contact met de Innovatie Attachés om ervaringen uit te wisselen, ideeën op te doen en kansen op samenwerking met het buitenland te signaleren.

Het Innovatie Attaché Netwerk is er ook voor u: bedrijven, kennisinstellingen en overheden met ambities ten aanzien van internationaal innoveren en samenwerken. Wij zijn aanwezig in 16 landen. U kunt direct met één of meerdere Innovatie Attachés contact opnemen. U kunt ons inschakelen voor het leggen van contacten en voor dienstverlening op maat met betrekking tot internationaal innoveren. Innovatie Attachés zijn uw oren, ogen en – waar nodig – handen, zijn uw vraagbaak, gids en adviseur voor internationaal innoveren en samenwerken. Daarbij scouten zij naar nieuwe ontwikkelingen waarover zij u gevraagd en indien relevant ook ongevraagd rapporteren.

Mocht u naar aanleiding van de inhoud van dit overzicht vragen hebben of onze hulp willen inschakelen, dan staan wij u met veel plezier te woord. Het kan dan gaan over het thema Veiligheid, maar uiteraard ook over thema's uit de andere topsectoren. U vindt onze contactgegevens achterin dit overzicht.

Ik wens u veel leesplezier!

Namens het gehele Innovatie Attaché Netwerk,

Bart Sattler,
Coördinator Innovatie Attaché Netwerk

Website: www.ianetwerk.nl
Twitter: @ianetwerk
Linkedin: https://nl.linkedin.com/in/ianetwerk

EU

Kansen voor onderzoek en innovatie op het gebied van veiligheid onder Horizon 2020

Onderzoek en innovatie op het gebied van veiligheid heeft met het thema 'Secure Societies – Protecting freedom and security of Europe and its citizens' een prominente plek gekregen in het Europese onderzoeks- en innovatieprogramma Horizon 2020 (H2020). Binnen dit programma wordt niet alleen ingezet op technologische innovatie, maar ook op juridische en ethische kennisontwikkeling. Het doel is om de stakeholders op het gebied van veiligheid via verschillende financieringsinstrumenten bij elkaar te brengen en te ondersteuning in hun ambities betreffende onderzoek en innovatie. Deze veiligheidsstakeholders komen uit de industrie -met inbegrip van het MKB-, onderzoeksinstellingen, universiteiten, overheden, en publieke en private organisaties op het gebied van veiligheid.

Horizon 2020

De Europese Commissie (EC) wil door middel van de Europa 2020 Strategie economische groei stimuleren, de concurrentiepositie van de Europese Unie (EU) verbeteren, banen creëren en maatschappelijke problemen aanpakken, en hee hierin de politieke steun van de Europese leiders en de leden van het Europees Parlement (EP). Zij plaatsten met de oprichting van het H2020 programma onderzoek en innovatie in het hart van een Europese Unie gericht op slimme, duurzame en inclusieve groei en banen. H2020 is daardoor een belangrijk, zo niet het belangrijkste, onderdeel in de toekomststrategie van de EC, en hee als doelen:

- reageren op de economische crisis doormiddel van investeringen in groei en werkgelegenheid;
- reageren op de zorgen van mensen over hun levensonderhoud, veiligheid en milieu;
- het versterken van de positie van de EU op het gebied van onderzoek, innovatie en technologie.

De EC hee iets meer dan 70 miljard euro gereserveerd voor H2020 (2014-2020) en hee een uitgebreide programmastructuur ingericht. Deze valt uit te splitsen in de drie pijlers 'Excellent Science', 'Industrial Leadership' en 'Societal Challenges', en in de drie minder bekende zogenaamde *cross-cutting themes*: 'Science with and for Society', 'Fast Track To Innovation' en 'Spreading excellence and widening participation' (meer informatie: h p://ec.europa.eu/programmes/horizon2020/h2020-sections).

H2020 is in chronologische en thematische zin de opvolger van het Zevende Kaderprogramma (KP7) van de EU en verleent via verschillende financieringsinstrumenten en op basis van excellentie financiering aan internationale consortia, onderzoekers en instellingen.

Interessante conclusies uit de evaluatie van KP7 waren dat onderzoek en innovatie op het gebied van veiligheid en vooral cyber security zichtbaarder had mogen zijn, slechts ten dele inging op de zorgen van de EU-burgers en vooral ten dienste stond van de industrie en niet van de samenleving. H2020 beloo beterschap en hee onderzoek en innovatie op het gebied van veiligheid bij 'Societal Challenges' onder thema 7 'Secure Societies' een prominente plek gegeven.

Secure Societies'

Onze wereld verandert en nieuwe veiligheidsdreigingen ontstaan, denk bijvoorbeeld aan internationaal en grensoverschrijdend terrorisme, digitale oorlogsvoering en radicalisering. 'Secure Societies' hee als inzet het beschermen van burgers, de samenleving en de vitale infrastructuur. Elke veiligheidsdreiging of -verstoring, opze elijk of per ongeluk, kan hierop een schadelijk e ect hebben met hoge economische en/of maatschappelijke kosten. Veiligheid is een gebied waarin uitdagingen voor ons liggen die niet kunnen worden opgelost door zelfstandig en sectorspecifiek onderzoek, maar waar juist een ambitieuze, gecoördineerde en holistische benadering nodig is.

'Secure Societies' springt hier op in en richt zich op de ontwikkeling van nieuwe kennis en technologieën voor de bestrijding van misdaad en terrorisme, crisismanagement en de externe dimensie van Europese veiligheid. Het programma is civiel georienteerd en richt zich in tegenstelling tot veel andere onderdelen uit H2020 specifiek op de eindgebruikers. 'Secure Societies' hee de EC voor het jaar 2015 een budget vrijgemaakt van 216.7 miljoen euro welke wordt verdeeld over vier pijlers:

- 'Disaster-resilience' (82.3 miljoen) hee als doel om de veerkracht van onze samenleving tegen natuurlijke en door de mens veroorzaakte rampen te versterken;
- 'Fight against Crime and Terrorism' (42.2 miljoen) hee als doel het strijden tegen (internationale) criminaliteit en terrorisme (met inbegrip van cybercriminaliteit en –terrorisme);
- 'Border Security and External Security' (42.2 miljoen) hee als doel om de bescherming van de Europese grenzen en samenlevingen te verbeteren;
- 'Digital Security: Cybersecurity, Privacy and Trust' (50.2 miljoen) hee als doel om te voorzien in verbeterde digitale veiligheid in Europa.

Op deze thema's worden de relevante stakeholders via verschillende financieringsinstrumenten bij elkaar gebracht en ondersteund. Deze stakeholders komen uit de industrie -met inbegrip van het MKB-, onderzoeksinstellingen, overheden, en publieke en private organisaties op het gebied van veiligheid.

'Disaster-resilience'

Het beschermen van een samenleving tegen natuurlijke en door de mens veroorzaakte rampen is essentieel om deze goed te laten functioneren. Een groot deel van de financiering binnen 'Secure Societies' wordt dan ook gereserveerd voor onderzoek en innovatie om de weerbaarheid van de Europese samenleving tegen rampen te vergroten. Voorbeelden van onderzoek en innovatie die hierbij genoemd worden zijn de ontwikkeling van nieuwe instrumenten voor crisisbeheer, het vergroten van de Europese communicatie interoperabiliteit en het bedenken van nieuwe oplossingen voor de bescherming van onmisbare infrastructuren. Verder wordt er specifiek aandacht gevraagd voor de gevolgen van klimaatverandering voor de nationale en internationale veiligheid. Dit leidt onvermijdelijk tot kansen voor veiligheidsonderzoek en -innovatie in en crossover met klimaatacties, klimaatonderzoek en de verschillende klimaatuitdagingen zoals te vinden onder thema 5 'Climate' en andere delen van H2020.

'Fight against Crime and Terrorism'

Het bestrijden van criminaliteit en terrorisme in de eenentwintigste eeuw vereist nieuwe (forensische) instrumenten en technologieën. In deze pijler wordt er ingezet op de betere bestrijding en preventie van criminaliteit (met inbegrip van cybercriminaliteit), illegale handel en terrorisme (met inbegrip van cyber-terrorisme). Aandachtsgebieden zijn hierbij onder andere de bescherming tegen aanslagen en explosies, en het aanpakken en voorkomen van radicalisering, onderzoek naar de humanitaire aspecten en gevolgen van grenscontroles, en het veilig houden van de Europese luchtvaart.

'Border Security and External Security'

Deze pijler richt zich op onderwerpen variërend van de bescherming van maritieme en landsgrenzen, tot de ondersteuning van het externe veiligheidsbeleid van de EU (met inbegrip van conflictpreventie en vredesondersteuning). Zo wordt er om de Europese grenzen nu en in de toekomst goed te kunnen blijven bewaken ingezet op de ontwikkeling van nieuwe systemen, apparatuur, instrumenten, processen en methodes om te komen tot de snelle identificatie van mensen en goederen (onder andere in het kader van het Europese douanebeleid). Bovendien zullen oplossingen ontwikkeld worden om het externe veiligheidsbeleid van de EU te ondersteunen bij bijvoorbeeld humanitaire hulp, grensbeheer, vredeshandhaving, conflictpreventie, vredesopbouw en bemiddeling.

'Digital Security: Cybersecurity, Privacy and Trust'

Onder deze pijler wordt er ingezet op het vergroten van de veiligheid van de huidige digitale toepassingen, diensten en infrastructuur door de integratie van de nieuwste beveiligingsoplossingen en processen. Hierbij staan de uiteindelijke gebruikers en hun wensen centraal. Deze stakeholders zijn onder andere wetshandhavingsinstanties, politie, brandweer, exploitanten van vitale infrastructuren, ICT-dienstverleners, ICT-fabrikanten en burgers.

In het licht van de Amerikaanse spionageactiviteiten in Europa, evenals de problemen betre ende de diefstal van gegevens, is de uitdaging 'Digital Security' in het Werkprogramma 2014-2015 uitgebreid. Zo is er meer financiering beschikbaar voor projecten over veilige informatie-uitwisseling en betere toegang tot data monitoring. Binnen 'Digital Security' is er voor gekozen om zowel onderzoek naar traditionele beveiligingsbehoe en als onderzoek naar nieuwe digitale veiligheidsvraagstukken te financieren. Deze strategie is bedoeld om de eindgebruikers, de industrie en het bedrijfsleven te (kunnen) betrekken.

De digitale dimensie van veiligheid komt ook in andere delen van H2020 prominent terug. Onder andere bij het thema 'Future Emerging Technologies' en de pilaar 'Leadership in Enabling Industrial Technologies' en dan specifiek onder 'Information and Communication

Technologies (ICT)' waarin 733 miljoen euro voor 2015 beschikbaar is. De uitdagingen en speerpunten betre ende ICT binnen H2020 zijn: *security-by-design*, cryptografie, privacy, toegangscontrole en risicomanagement.

Hoe verder in 2016-2017?

Het Werkprogramma 2016-2017 voor H2020 is nog niet vastgesteld, maar het is goed alvast vooruit te kijken naar mogelijke kansen in 2016-2017. Zo is de Secure Societies Advisory Group is in het proces van het opstellen van aanbevelingen voor de het Werkprogramma 2016-2017 en is de EC druk met de consultatie van het veld en het opstellen van de eerste conceptwerkprogramma's.

Nederland is actief bezig om input te leveren voor het Werkprogramma 2016-2017 voor 'Secure Societies'. Daarbij wordt er ingezet op het verzamelen van de behoeften van publieke eindgebruikers, industrie, bedrijfsleven, overheden en wetenschap. Verder werkt Nederland intensief met verschillende andere lidstaten samen om de Nederlandse input zo goed mogelijk in het nieuwe Werkprogramma te krijgen zodat Nederlandse geïnterneerde partijen goede projectvoorstellen kunnen indienen onder het nieuwe Werkprogramma.

Als lezers bij bovenstaand proces betrokken willen worden kunnen zij zich via Paul Kruis, nationaal contactpunt H2020 en Veiligheid (paul.kruis@rvo.nl), aanmelden voor de klankbordgroep van de Rijksoverheid over 'Secure Societies'. Deze groep wordt regelmatig geraadpleegd om zo de behoe en uit het veld te horen en om reacties te verkrijgen op de conceptwerkprogramma's.

Kansen voor onderzoek en innovatie

'Secure Societies' en de thema's en onderzoeken die daar onder thuishoren zijn er specifiek op gericht om via internationale onderzoeks- en innovatieprojecten bij te dragen aan de veiligheidsuitdagingen (met inbegrip van cyber security)zoals binnen de EU en op nationaal veiligheidsbeleid worden herkend. In concrete zin valt dan te denken aan kansen voor onderzoeksprojecten over onder andere:

- Crisis management: extreme weersomstandigheden, CBRN-verontreinigingen, pandemiebescherming, de bescherming van essentiële infrastructuren, communicatietechnologieën.
- Criminaliteit en terrorisme: forensische infrastructuur en instrumenten, internet monitoring, identiteitsmanagement, veiligheid in steden.
- Grens- en externe veiligheid: kunst- en landgrensveiligheid, radarsystemen, biometrie, scanners, vracht inspectie, externe veiligheid.
- Cyber security: privacy, toegangscontrole, ICT in de bescherming van essentiële infrastructuren, veilige informatie-uitwisseling.

Met een succesvolle aanvraag tot financiering binnen bovenstaande kaders krijgt de aanvragende partij toegang tot onder andere:

- financiering van een innovatief project;
- het aantrekken of behouden van onderzoekers;
- de intellectuele eigendomsrechten;
- een groot internationaal netwerk van partners voor onderzoek en ontwikkeling;
- toegang tot nieuwe markten;
- nieuwe expertise, technologie en kennisoverdracht.

Indienen van een projectvoorstel

De deadline voor het indienen van projectvoorstellen binnen het thema van 'Secure Societies' is 27 augustus 2015. Elk project wordt ondersteund door een specifiek financieringsinstrument. Elk van deze financieringsinstrumenten kent zijn eigen criteria met betrekking tot de gewenste doelen, het gewenste aantal betrokken partners en de mogelijke maximale hoeveelheid financiering.

Partijen die een project voorstel willen indienen kunnen soms, a ankelijk van het financieringsinstrument, zelfstandig opereren. Dit is gezien de benodigde middelen vaak lastig. Om de juiste kennis en middelen bij elkaar te krijgen wordt er veelal ingezet op de vorming van internationale consortia tussen bedrijven, overheden en kennisinstellingen. Consortia moeten veelal bestaan uit drie of meer partners uit drie of meer EU lidstaten. Er zijn voldoende kansen voor individuele stakeholders om aan te haken bij consortia of gebruik te maken van de instrumenten die meer op het MKB gericht zijn. De Rijksdienst voor Ondernemend Nederland (RVO) is voor Nederland het aanspreekpunt voor mogelijke indieners en informeert en adviseert geïnteresseerden graag over de mogelijkheden.

Iedere organisatie die actief is in veiligheidsonderzoek kan een projectvoorstel indienen. In de projecten is de betrokkenheid van een eindgebruiker van veiligheidsoplossingen vaak een vereiste, de eindgebruiker is immers ook vaak de beoogde inkoper van een ontwikkelde oplossing. Hierbij valt te denken aan politie, brandweer, beheerders van vitale infrastructuur en overheidsorganisaties. Verder moet het project/onderzoek wetenschappelijk excellent zijn, een potentieel sterke socio-economische impact hebben, voortbouwen op bestaande of ontwikkelen van nieuw kennis, en een Europees veiligheidsprobleem oplossen.

Ondersteuning bij het indienen van een projectvoorstel

In Nederland is de Rijksdienst voor Ondernemend Nederland (RVO) het aanspreekpunt voor advies over projectvoorstellen onder H2020. Vanuit de RVO informeert en adviseert Paul Kruis (HYPERLINK "mailto:paul.kruis@rvo.nl" paul.kruis@rvo.nl), nationaal contactpunt H2020 en Veiligheid, geïnteresseerde partijen over de volgende punten:

- de procedures;
- de strategie van de aanvraag;
- het zoeken naar partners;
- het schrijven van een projectvoorstel;
- de contractuele kwesties.

Meer informatie

Horizon 2020 & Veiligheid & 'Secure Societies':

- h p://ec.europa.eu/programmes/horizon2020/en/area/security
- h p://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

Documenten Horizon 2020 Werkprogramma 2014-2015:

- h p://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html

Rijksdienst voor Ondernemend Nederland (RVO):

- h p://www.rvo.nl/horizon2020
- h p://www.rvo.nl/subsidies-regelingen/horizon-2020-onderzoek-en-innovatie
- h p://www.rvo.nl/subsidies-regelingen/veilige-samenleving-horizon-2020
- Of vul het contactformulier in op h p://www.rvo.nl/ of bel naar +31 880424242.

Handleiding over de criteria voor en het proces van indienen van projectvoorstellen:

- h p://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/pse/h2020-guide-pse_en.pdf

Meer informatie

Jeroen Arts en Dave Pieters
Email: brussel@ianetwerk.nl
IA EU

Frankrijk

Security in Frankrijk: cybersecurity, betrouwbaarheidslabel en drones boven Parijs

Who's who in de Franse veiligheid

Veiligheid, inclusief cybersecurity, valt in Frankrijk onder de verantwoordelijkheid van het *Secrétariat Général de la Défense et de la Sécurité Nationale* (SGDSN). Dit valt rechtstreeks onder de Premier Ministre.

Het SGDSN is belast met het geheel aan strategische vraagstukken die betrekking hebben op het de nationale veiligheid, waarbij het gaat om de militaire programmeringswe en, het afschrikbeleid ten opzichte van een nucleair conflict, het nationale interne veiligheidsprogramma, cybersecurity, de controle van wapenexporten, maar ook de economische en energieveiligheid, de strijd tegen terrorisme en proliferatie en het opstellen van crisisplannen.

Binnen het SGDSN is een aparte instantie specifiek belast met cybersecurity, het ANSSI, *Agence Nationale de la Sécurité des Systèmes d'Information*.

De basis van het nationale veiligheidsprogramma is vastgelegd in het Witboek, *Livre Blanc Défense et Sécurité Nationale*, dat Yves Le Drian, Minister van Defensie in april 2013 presenteerde.

Cyberdéfense Pact

Op 7 februari 2015 voegde Le Drian daaraan het zogenaamde Cyberdefense Pact toe. Het betre een document met daarin zowel maatregelen voor cybersecurity binnen de Franse defensie, als activiteiten bedoeld om cyberinitiatieven vanuit overheden en bedrijfsleven te ondersteunen. Voor de komende twee jaar is voor het programma bijna een miljard euro uitgetrokken.

Het 'pact' is opgebouwd uit zes hooflijnen en 50 maatregelen:

1. Het verhogen van het veiligheidsniveau van informatiesystemen binnen het Ministerie van Defensie, de verbetering van beschermings- en bestrijdingsmiddelen;
2. Uitbreiding van het onderzoek, zowel technologisch als operationeel en ondersteuning aan de Franse industrie;
3. Versterking van de personele middelen op het gebied van cybersecurity en het ontwikkelen van relevante specialistische loopbanen;
4. Het opze en van een Cyberdefence Center of Excellence in Bretagne, ten behoeve van het Ministerie van Defensie en tevens voor de nationale cybersecurity-gemeenschap;
5. Het creëren van een netwerk van buitenlandse partners, zowel binnen Europa als de NAVO, in het kader van strategische interessegebieden;
6. Het vergroten van de cybergemeenschap door de banden met nationale partners aan te halen en een groter beroep te doen op het reservistenbestand.

In lijn met het Livre Blanc voorzien de financiële plannen in een verdrievoudiging van de middelen, bestemd voor cybersecurity. Zo worden er binnen Defensie de komende 5 jaar 550 nieuwe cyber banen gecreëerd.

Critical security

Ruim 200 bedrijven van vitaal belang voor de economie

In Frankrijk wordt een groep bedrijven van overheidswege als vitaal voor de economie beschouwd. Deze zijn bij wet verplicht om te investeren in de beveiliging van hun interne informatie- en communicatiesystemen. In totaal gaat het om ruim 200 bedrijven. Welke dat precies zijn, daarover wordt niet gecommuniceerd.

Als immers de netwerken van grote banken, telecomproviders, vliegvelden, de SNCF (spoorwegen) of EDF (elektriciteit) gehackt worden, zouden de gevolgen voor de Franse economie gigantisch kunnen zijn. Hele steden zonder licht, hulpdiensten

uitgeschakeld, vliegtuigen aan de grond … kortom de economie zou bijna plat komen te liggen.

Opérateurs d'Importance Vitale (OIV)

Daarom wil de Franse staat dat deze bedrijven, de zogenaamde '*opérateurs d'importance vitale*' (OIV), spelers van vitaal belang, aan bepaalde beveiligingseisen voldoen. "Jaarlijks vinden meerdere serieuze cyberaanvallen plaats. Soms slagen de hackers er in om in het meest gevoelige deel van een ICT-systeem terecht te komen met kostbare technische, strategische of commerciële informatie. Het doel is om hierop te anticiperen", aldus Guillaume Poupard, Algemeen Directeur van het Franse Nationale Agentschap voor de Veiligheid van Informatiesystemen ANSSI (Agence Nationale de la sécurité des systèmes d'information).

In de meerjarige militaire wet die in december 2013 werd aangenomen, staan voor OIV-geklasseerde bedrijven nieuwe verplichtingen met betrekking tot hun cybersecurity. Ook krijgt het ANSSI nieuwe bevoegdheden: in geval van een ernstige dreiging kan het nationale agentschap de totale controle over een ICT-netwerk overnemen en dit eventueel van de rest van het net a oppelen.

Wat is vitaal belang?

De investeringen die de betre ende bedrijven verplicht zijn te doen, zijn a ankelijk van de situatie. Dat kan met een factor vijf oplopen van het ene tot het andere bedrijf. "Maar de mate van 'vitaal belang' is lastig te definiëren. Als bijvoorbeeld het klantenbestand van een bedrijf wordt gehackt, dan betekent dat niet een onmiddellijk gevaar voor het land. Het bedrijf kan waarschijnlijk nog steeds dezelfde diensten leveren. De discussies tussen het ANSSI en de OIV-bedrijven gaan er soms fel aan toe. Wat is een vitale functie in welke sector? Bij telecombedrijven zijn telefoonverbindingen van vitaal belang, maar hoe zit het met internet, is dat even essentieel? Is bij de SNCF de reizigersinformatie van vitaal belang? In sommige gevallen waarschijnlijk wel.

Business voor Thales, Orange, Airbus Defense&Space, Atos

Leveranciers van cybersecurity-technologie, zoals Thales, Orange, Airbus Defense&Space, Atos en CS, hopen te profiteren van het nieuwe we elijk kader en de verplichte investeringen die de OIV-bedrijven moeten doen. In twee of drie jaar tijd is het aantal tenders verdubbeld, bekent een grote cybersecurityspeler.

Volgens de consultant Pierre Audoin Consultants (PAC) hee het bedrijfsleven in 2013 meer dan een miljard euro uitgegeven aan producten zoals antivirussen, firewalls, en andere cybersecuritydiensten. Dat is gemiddeld tien procent meer dan het jaar ervoor. Franse technologieproviders kunnen hier een grote rol spelen.

Vertrouwen in technologie

Want de wet beoogt om 'betrouwbare technologie' te stimuleren, dat wil zeggen, a omstig uit Frankrijk of uit Europa. De meeste producenten hebben hun aanbod al gelabeld met "Speciaal voor OIV's", een label waar ze de aandacht op vestigen tijdens beurzen en forums, zoals in januari jl. tijdens het CybersecurityForum in Lille.

Thales en Airbus Cybersecurity zijn heel sterk op de markt van de 'soevereine lijntjes', die automatisch iedere abnormale activiteit bij een OIV-bedrijf melden bij het ANSSI. "Wij beheersen alle aspecten van het product", aldus Cyril Autant, directeur IT- en Ruimtevaartveiligheid bij Thales.

Ook de kleinere spelers proberen een graantje mee te pikken. Zo hee mkb Amossys uit Rennes so ware ontwikkeld waarmee een OIV-bedrijf zijn hele systeem in kaart kan brengen en alle datastromen die er rond gaan kan identificeren. "Onze so ware hee geen enkele invloed op het netwerk of op andere apparaten", benadrukt één van de oprichters van Amossys, Christophe Dupas.

Orange concurreert met IBM en Capgemini op de dienstenmarkt en vindt het absurd om uitsluitend met Franse technologie te willen werken. "Soevereine producten bestaan niet, soevereine diensten wel", legt Michel Van den Berghe uit, directeur van Orange Cyberdefense.

Die visie wordt bevestigd als je kijkt naar de tien grootste verkopers van beveiligingsso ware in Frankrijk, daar zit geen enkel Frans bedrijf tussen: Symantec (VS), Checkpoint (Israël), Kaspersky (Rusland), HP (VS), Intel (VS), en Trend Micro (Japan) beze en de eerste plaatsen.

Toch hee Orange een oplossing gevonden om te voldoen aan de OIV-veiligheidseisen door een Amerikaans gevoelig product te kopen, maar dat geheel op het eigen Orangenet te installeren, en door Orangeteams te laten beheren. Zo is men er zeker van dat de data op geen enkele manier Frankrijk uit kunnen komen.

Label 'France cybersecurity' voor betrouwbare spelers

Cybersecurity is één van Frankrijk's 34 strategische sectoren voor de economie. Eén van de prioriteiten van de in 2015 opgestelde cybersecurityroadmap is het oormerken van nationale partijen, bedrijven, en publieke spelers, die betrouwbare producten of diensten aanbieden op het gebied van cybersecurity. Dat gebeurde in januari 2015 voor het eerst.

Tijdens het International Forum on Cybersecurity in Lille, reikte Axelle Lemaire, staatssecretaris voor de digitale economie, de eerste '*France CyberSecurity*'-labels uit aan zeventien bedrijven, uiteenlopend van kleine tot hele grote spelers, te weten: Amossys (expertise en consulting), Arkoon (netwerk- en databeveiliging, eigendom van Airbus Defense and Space), Netasq (netwerk- en databeveiliging, eigendom van Airbus Defense and Space) -Arkoon en Netasq zijn samen Stormshield geworden-, Atos, Bertin (technologische innovatie), CS Systèmes d'information (designer, integrator, operator of mission critical systems), DenyAll (cybersecurity), Ercom (bescherming van mobiele netwerken, onder andere de tablets van het Franse Ministerie van Buitenlandse Zaken), Ingenico (smart solutions for payments), In-Webo (beveiliging van authenticatie), Opentrust (elektronische handtekening), Orange Cyberdefense (bescherming

netwerken en telecom), Prim'x (corporate encryption systemen), Sogeti (Filiaal CapGemini, cybersecurity, zojuist contract getekend met Franse DG burgerluchtvaart), STMicroelectronics (slimme oplossingen, sensoren), Thales (critical information systems and cybersecurity), The Greenbow (o.a. e-mailbeveiliging) en Wallix (privileged user management).

Het label wordt toegekend door partijen uit de sector, te weten:

- de aanbieders: ACN, de recent opgeze e brancheorganisatie voor alle spelers actief op het gebied van security en Hexatrust, een groep Franse mkb's die complementaire diensten op het gebied van veiligheid aanbiedt,
- de gebruikers: CESIN, de club van experts op het gebied van ICT-beveiliging, Cigref, club van 130 grote bedrijven, en Gitsis, selecte groep van zeer grote bedrijven -waaronder Airbus, Safran, Orange, Thales voor veiligheidstechnologie van gevoelige informatiesystemen, en
- overheidsorganisaties: ANSSI, het nationaal agentschap voor de beveiliging van informatiesystemen, de DGA, vergelijkbaar met de Nederlandse DMO bij Defensie en de DGE, DG Ondernemen van het Franse ministerie van economie.

Roadmap Cybersecurity Frankrijk

In januari 2015 werd de roadmap van de 'Topsector Cybersecurity' gepresenteerd. Deze sector is in Frankrijk goed voor 40.000 banen in Frankrijk en een omzet van 13 miljard euro.

Voorzi er van het projec eam voor het opstellen van de roadmap was Guillaume POUPARD, algemeen directeur van het ANSSI. Het secretariaat had Bull namens de zogenaamde 'Alliance pour la Confiance Numérique' (ACN), een overkoepelende organisatie die bedrijven, federaties en clusters vertegenwoordigt rond het thema digitale veiligheid.

Vanuit de industrie waren zowel hele kleine bedrijven, mkb's, als grote bedrijven vertegenwoordigd:

- - Hele kleine bedrijven: The Greenbow (lid van 'HEXATRUST) en Prim'x.
- MKB: Dictao, Ercom, beide lid van de pôle de compétitivité Systematic en Wallix, lid van HEXATRUST.
- Op het gebied van kaarten en componenten: Gemalto en STMicroelectronics.
- Uitvoerend: THALES Communications & Security en AIRBUS Defense & Space
- Diensten: SOLUCOM (vertegenwoordiger van CLUSIF), SOGETI (lid van de club van vertrouwensproviders van beveiliging van informatiesystemen)
- Evaluerende organen: OPPIDA, AMOSSYS (lid van CLUSIF)
- Normalisatie : AIRBUS Defence & Space, Trusted Labs

Ook de gebruikers en de overheid waren vertegenwoordigd bij het opstellen van de roadmap.

Vier grote doelstellingen

Het plan hee vier grote doelstellingen gedefinieerd:

1. Groei van de vraag naar betrouwbare cybersecurity-oplossingen, producten en diensten;
2. Ontwikkeling van een betrouwbaar cybersecurityproducten- en dienstenaanbod afgestemd op de behoe en van Frankrijk;
3. Het veroveren van buitenlandse markten;
4. Versterking van de nationale cybersecuritybedrijven.

Er bestaat weliswaar een goed nationaal aanbod, maar dit is vaak onbekend en erg versnipperd, en het hee veel concurrentie te verduren van buitenlandse spelers die een actiever marketingbeleid voeren.

Het Franse bestaande, betrouwbare, aanbod zou uitgebreid moeten worden om tegemoet te kunnen komen aan nieuwe technologische ontwikkelingen. Dit kan door een betere governance, door meer valorisatie van R&D, in nauwe aansluiting bij Europese instrumenten. Het probleem is ook dat het om een zeer groot aantal industriële spelers gaat, zo'n 600, maar die te weinig samenhang vertonen. Consolidatie van deze sector moet een doelstelling van de nationale overheid zijn.

Voor de versterking van de nationale spelers is ook ontwikkeling van de export nodig die te amateuristisch blij ten opzichte van de kwaliteit van het aanbod en die te lijden hee onder het ontbreken van een nationale aanpak.

De G4 van de Franse cybersecurity : Orange, Thales, CS en Airbus

Vier bedrijven vormen samen de 'Cybersecurity G4' van Frankrijk, te weten Orange Cyberdefense, Thales, CS en Airbus Defense & Space. Hieronder feiten en cijfers over deze 'grote vier'.

Orange Cyberdefense, het voordeel van het net

Omzet van de groep: 40,9 miljard euro
Cybersecurityomzet: 60 miljoen euro
Aantal werknemers: 1000 experts in ICT-veiligheid

Het statuut van Orange als telecomprovider gee het bedrijf een bevoorrechte positie. Het bedrijf ziet wat er op het net gebeurt! Abnormale tra cstromen, internetconnecties op ongewone tijdstippen, het zijn allemaal tekenen van een mogelijke cyberaanval. Orange kan zijn klanten bijtijds inlichten. Bovendien hee het centra die op afstand het net in de gaten houden.

Thales, getallenkampioen

Omzet van de groep: 14,2 miljard euro
Cybersecurityomzet: 500 miljoen euro
Aantal werknemers: 1500 experts in ICT-veiligheid

Dankzij zijn cryptografie-expertise uit de militaire wereld hee Thales een belangrijke plaats weten in te nemen als speler voor de beveiliging van communicatie bij banken, overheden en het leger.

Het bedrijf is zich nu richting diensten aan het ontwikkelen. Onlangs nam het de cybersecurity- en communicatiebeveiligingsdiensten van Alcatel-Lucent over.

CS, een technologische monopolie

Omzet van de groep: 162 miljoen euro
Cybersecurityomzet: 16 à 18 miljoen euro
Aantal werknemers: ongeveer 110 personen

CS is het enige bedrijf in Frankrijk dat een sleuteltechnologie voor cybersecurity bezit, de SIEM (Security Information and Event Management) genaamd Prelude. Deze so ware is in staat om in realtime

een groot aantal ICT-incidenten te analyseren om eventuele dreigingen te detecteren. Dat maakt CS een onmisbare speler om de meest gevoelige bedrijven te beschermen, temeer daar het ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) 'Made in France'-technologie gaat vragen.

Airbus Defense & Space, sterk en machtig

Omzet van de groep : 59,3 miljard euro
Cybersecurityomzet : ongeveer 100 miljoen euro
Aantal werknemers : ongeveer 600 personen

Dit filiaal van Airbus hee reeds de Franse securitybedrijven Arkoon en Netasq opgekocht. Om nog verder uit te groeien zou het wel eens nog meer acquisities kunnen doen. Dit is relatief eenvoudig, aangezien Airbus zowel in Frankrijk, Duitsland, als in de VK gevestigd is. Zodoende kan het ook breed werven, dit is aantrekkelijk want het vinden van de juiste competenties in de cybersecuritysector is lastig.

Urban Security: Drones-invasie

Een zestigtal mysterieuze dronevluchten boven Parijs en omgeving hebben tussen oktober 2014 en maart 2015 voor onrust en verwarring gezorgd in Frankrijk. Zeker in het licht van de terroristische aanslagen in Parijs van begin januari.

Vooralsnog tast men in het duister voor wat betre de bestuurders van deze drones. De plekken waar de vliegende machines gezien zijn, lopen uiteen van de Ei eltoren, Palais de l'Elysée, de Amerikaanse Ambassade en andere plekken in en rond Parijs, tot een groot aantal kerncentrales en zelfs Ile Longue in Bretagne, thuishaven van de Franse nucleaire onderzeeërs.

Experts van het Algemeen Secretariaat voor Defensie en Nationale Veiligheid (SGDSN, *Secrétariat Général de la Défense et de la Sécurité Nationale*) onderzoeken daarom alle mogelijke methoden om dit fenomeen een halt toe te roepen. De SGDSN hee de nodige ervaring met detectie- en neutralisatie-activiteiten. Maar nog deze maand gaat men aan de slag met het testen van nieuwe detectiemiddelen, door middel van passieve of actieve radars, met name in te ze en boven gevoelige opstellingen zoals kerncentrales. Want vooralsnog zijn de nationale veiligheidsdiensten niet echt in staat om de zone tussen 50 en 100 meter hoogte af te dekken. Men gee toe dat daar nog een slag gemaakt moet worden.

Frankrijk drone-pionier

Niet alleen dient er een betere coördinatie van de aanpak van het dronevraagstuk te komen tussen de premier en de Ministeries van Binnenlandse zaken en van Defensie, ook gaan er stemmen op om de boetes flink te verhogen voor dronebestuurders voor verboden doeleinden.

Men waarschuwt echter bij de SGDSN dat het hier gaat om de ontwikkeling van een jonge, sterk groeiende economische sector waarin Frankrijk pionier is. Het is dus zaak om niet op voorhand te zware regelgeving erop los te laten.

De sector bestaat uit zo'n 1.200 professionals die samen goed zijn voor 3.000 directe banen in Frankrijk. De dronemarkt vertegenwoordigt nu al een omzet van boven de 100 miljoen euro per jaar.

Critical infrastructure: Veiligheid vraagt om steeds meer technologie

Veiligheid bij bedrijven vereist de inzet van steeds meer technologie. Dat kan gaan om cameratoezicht en klassieke alarmsystemen maar ook om meer high-tech middelen.

Foxstream : realtime beeldanalyse

Het Franse bedrijf Foxstream hee al een flinke staat van dienst op het gebied van realtime beeldanalyse. Hun so ware kan verdachte bewegingen herkennen, gezichtsherkenning doen, en aanwezigheid van personen detecteren op bijvoorbeeld een landings- en startbaan van een vliegveld. Klanten zijn bijvoorbeeld de vliegvelden van Barcelona, Lyon en Biarritz, de Airbus A380 assemblagesite en de Ei eltoren.

Deze technologie is sinds een jaar of tien in ontwikkeling, en komt nu in de fase van rijpheid.

Drones en ballonnen

Daarentegen staat de technologie, die gebruik maakt van drones en ballonnen, nog in de kinderschoenen. Maar veiligheidsmanagers van grote bedrijven zijn zeer geïnteresseerd. De SNCF hee drones getest voor de bewaking van het onderhoud van zijn netwerk, Vinci wil er zijn bouwplaatsen voor de aanleg van de TGV Tours-Bordeaux mee bewaken. Ook Veolia hee een test gelanceerd in Bordeaux. Drones kunnen grote afstanden afleggen maar hebben nog weinig autonomie, terwijl ballonnen het voordeel hebben dat, als er niet te veel wind is, ze een bepaalde zone permanent kunnen bewaken.

Robots van EOS Innovation

Ook de robotica begint zijn intrede te doen in de wereld van de veiligheid. De robot van de Franse start-up EOS Innovation, gemaakt voor de bewaking van entrepots, is sinds zes maanden in actie bij één van de Franse filialen van ID Logistics. Het product is nog in de commercialisatiefase en kost zo'n 30.000 à 45.000 euro. Terwijl een fulltime bewaker 's avonds en in het weekend zo'n 100.000 à 150.000 euro per jaar kost. Uit kostenoogpunt dus een aantrekkelijk alternatief.

Bronnen

- *Quatre acteurs incontournables*, L'Usine Nouvelle, 15 januari 2015
- Un label France cybersécurité, L'Usine Nouvelle, 29 januari 2015
- Cybersécurité : 200 entreprises sensibles à protéger, L'Usine Nouvelle, 21 januari 2015
- *Drones malveillants : de nouvelles parades expérimentées par l'État d'ici à fin mars*, Le Figaro, 4 maart 2015
- Witboek Défense et Sécurité Nationale, avril 2013
- *Une sécurité de plus en plus technologique*, L'Usine Nouvelle, 29 januari 2015
- *Un label France cybersécurité*, L'Usine Nouvelle, 29 januari 2015
- *Comment le plan Cyberdéfense boostera les technologies "made in France"*, L'Usine Nouvelle, 7 februari 2015

Meer informatie

Joannette Polo-Leemreis
Email: parijs@ianetwerk.nl
IA Frankrijk

Duitsland

Cybersecurity – a Challenge and an Opportunity for Germany

Security in a world that is more and more interconnected is a challenging topic, both for people privately and for the society. Germany, with one of the strongest and high-tech economies in Europe, is o en a target for hackers and industrial espionage. Hacking a acks pose a real threat to power grids, industrial facilities, computers and smartphones. In Germany, there is a great awareness of the issue of data protection because of Germany's historical background. There is a prevailing scepticism towards governmental surveillance. How is Germany facing those challenges?

In 2011, the German Ministry of Internal A airs initiated the Cyber Security Strategy. This strategy includes the national Cyber Defense Center and the national Cyber Security Council. This Council advises companies as well as the government on how to improve their IT security. Simultaneously, the strategy covers critical infrastructure, which will be explained later on. There is also an IT-Planning Council which aims at giving political guidance for a voluntary cooperation between federal and state authorities in this field.

Cyber-A acks

German companies are frequently targeted out of either political or commercial intent. For one thing, know-how is o en stolen. It can be di cult to distinguish between espionage and reverse engineering. Reverse Engineering is a practice for analyzing a (commercial) product in order to uncover its unknown features. Sometimes it is not clear whether construction data was stolen or the product was copied via Reverse Engineering. It takes on average 243 days to discover Advanced Persistent Threats. APT is the name for a continuous hacking process. Those occur o en, especially targeting companies in order to steal their knowledge. This is di cult for companies as they don't know immediately whether their system has been hacked. Yet it poses a major problem to companies because it is unclear how to protect their expertise. It is estimated by the Federal Criminal Police O ce that cyber espionage costs the German industry 42.5 million EUR every year.

The Federal O ce for Information Security plays a central role in organising security strategies. In cooperation with the BITKOM it supports e.g. also the Alliance of Cybersecurity. BITKOM is the association of the ICT industry. Also, companies and organisations from the critical infrastructures sector have to report a acks to the o ce for Information Security.

But not only companies are targeted by hackers. An estimated 40 per cent of computers in Germany are a ected by malicious so ware. The government and associations are trying to inform citizens on how they can protect their computers from being hacked by giving advice on internet pages such as h ps://www.buerger-cert.de/ and h ps://www.botfrei.de/.

The other important federal institution concerning security is the Federal Ministry of Research and Education (BMBF). The BMBF initiated several research programs. Firstly, "Autonomously and safely in the digital world", with 190 million EUR. Running from 2015 until 2020, it focuses upon new Hightech-Technologies for IT security, data protection and secure ICT-systems. This program is also part of the Hightech-Strategy for Germany from the federal government. Furthermore, the BMBF initiated three competence centers for cybersecurity, with an amount of 17.2 million EUR.

Securing the world of interconnected Devices

More and more sensors are used in products and devices. This makes the production more connected and flexible and thus individualised because

companies have the possibility of reacting immediately. On the other hand, the "Internet of Things" represents a possible danger because they make a company or a private user vulnerable to cyber-a acks.

Data security and know-how protection is partly addressed in transnational panels.

- Fit4sec is a center for security and technology which is supported by the Federal Ministry of Education and Research is a part of the "German Applicants fit for Europe" program. It aims at pooling expertise in the German security sector to successfully form German-European research alliances together with end users and academic partners. The core team of fit4sec is composed of the IABG in O obrunn and Berlin, the Brandenburg Institute for Society and Security in Potsdam, Fraunhofer FOKUS in Berlin and the University of the Federal Armed Forces in Munich. h p://www.fit4sec.de/

Securing Clouds is important because more companies are using clouds to store their data online. By using external data centers you draw less from the company's own resources. Another advantage is that companies have world-wide access to their data. Since clouds are ge ing more and more essential for companies, there is also research done in that field. Three examples are:

- The Fraunhofer Institute for Secure IT, the SIT in Darmstadt, is developing OmniCloud. OmniCloud encrypts Data before they are being uploaded to a Cloud. h p://www.omnicloud.sit.fraunhofer.de/index_de.php
- Also, the SIT developed Hash Guard, a product providing protection from Advanced Persistent Threats. h ps://www.sit.fraunhofer.de/de/hashguard/
- One of the local clusters in Nord Rhine-Westphalia is the ICT Cluster NRW. It funds amongst others the CPS.HUB NRW with 2 Mio. EUR from 2012 until 2015. This Hub is doing research on security challenges in the connected world.

The Federal State Bavaria is also important to mention, since it is one of the strongest industrial areas in Europe. In addition, experts say that the conservative Bavarian State Government is investing traditionally more money in security.

There are many security clusters with different focuses located in Bavaria.

- Bavarian IT-Security cluster: h p://www.it-sicherheit-bayern.de/
- The Bavarian cluster for ICT: h p://www.bicc-net.de/
- Bavarian IT-Logistics Cluster: h p://www.it-logistik-bayern.de/it-logistik/
- The Bavarian association for Security in the industry: h p://www.bvsw.de/

Moreover, other trade associations such as the chambers of commerce (IHKs) and the association of Bavarian industry (h p://www.vbw-bayern.de/vbw/Home/) are also working on IT-Security-related topics.

Critical Infrastructures

Critical infrastructures, such as power grids and telecommunications, are becoming increasingly complex. They are interdependent and their reliable operation is essential for many aspects of our lives. Because of ICT they are ge ing smarter and more flexible, but also more complex and vulnerable.

One of the key instruments of the federal German government regarding critical infrastructures is the implementation plan Critical Infrastructures, launched by the federal o ce for information security and is a part of the Cyber Security Strategy. It brings together companies from the critical infrastructure sector with governmental institutions. The public-private cooperation is aiming at promoting information exchange, protecting vital processes of the ICT-components and se ing up a crisis management.

Most of the technology programs are supported by the Federal O ce for Information Security, or the Federal Ministry of Research and Education. The program "Research for civil security" is being government-sponsored with 400 million EUR; 100 million EUR are added by the industry. Two examples are:

- CamInSens, promoted by the Ministry of Research and Education within their program ''Research for civil security", is measuring data of movement by the use of cameras in order to detect potentially dangerous situations immediately and not only a er they happened. h p://www.caminsens.org/
- The Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS in Sankt Augustin in NRW is developing several tools which can be introduced for securing critical infrastructures: The physical infrastructure, such as the airport and stations for instance, as well as the "Cyber-infrastructure".

Drones

Privately used drones are strictly limited by law in Germany. They have to stay in sight of the person controlling the drone; they aren't allowed to fly near airports, preserved areas, a crowd of people, power plants and many more. However, the government is thinking of how to deal with illegally used drones. With the new satellite system Galileo it is possible to detect even drones that weigh less than two kilograms. The Galileo Satellites are using PRS, the European pendant to the military GPS, and is therefore be er protected against cyber-a acks. In Germany, the general public mainly disapproves of drones.

Research in this field, also on civil and not only military used drones is essentially done by the University of Federal Armed Forces in Munich. Their focus lays on human-machine-system integration and autonomous drones. Research is done on the ideal division of labour between the drone and the person in control: Drones aren't developed to fly entirely autonomously, only to a certain degree. The person controlling the drone mustn't be unchallenged whereas this can lead to boredom and thereby to negligence. The extent of technical support should be guided by not only the technical possibilities, but primarily by the human need for technical assistance.

Smart Grids

Climate change, the rapid surge in energy demand and scarce natural resources present Germany with challenges in the field of energy supply. The answer to the problem is the implementation of smart grids. The term smart grids describes power grids. Smart grids distribute energy intelligently and independently. A computer program checks where how much energy is produced and consumed.

Because of the energy transition (Energiewende) smart grids are a very important ma er for Germany. Many people produce energy on their own, with solar panels for example. Those are called prosumers. In 2013, 25.5 percent of the gross electricity consumption comes from producers of renewable energy. The delocalisation makes the distribution of energy in Germany more complicated. Transporting the energy produced with windmills from the north of Germany to the industrial centers in the south is a di cult task. Protecting smart grids is also one of the challenges. A study in the U.S. finds that power grids are a acked every four days, online or in person.

- The IAEW, a RWTH Aachen institute focusing on electrical systems, is doing for instance research on modern smart grids in Germany, supported by the Ministry of Research and Education. The objectives of the study are to quantify the required network expansion in German distribution networks as a result of the renewable energy systems and evaluating smart grid technologies. h p://www.iaew.rwth-aachen.de/
- Germany, Austria and Switzerland formed together DACH security. The transnational research cooperation focuses on ICT-based energy systems. That includes the development and testing of implementation strategies for smart grids. This cooperation is supported among others by the Federal Ministry for Economic A airs and Energy in their supporting program of E-Energy. h p://www.syssec.at/dachsecurity2014/

Secure Cities

Regarding the fact that securing cities is a great challenge for our society, it is worthwhile to take a look at these two examples:

- The Fraunhofer cluster ''Future Urban Security'' develops products protecting city residents from growing threats such as terrorism, climate change and crime. Fraunhofer EMI, the Ernst-Mach-Institut in Freiburg, is also participating. The EMI dedicates one entire department to research on critical infrastructures and secure cities. It is for example commissioned to carry projects by the German Federal O ce of Civil Protection and Disaster Assistance. h p://www.future-security.org/
- VITRUV is a tool by the Fraunhofer EMI for risk analysis in urban areas. The so ware integrates security measures directly into the urban planning process. h p://www.vitruv-tool.eu/

Predictive Policing

There is a so ware testing project called Precobs (Pre Crime Observation System) in Bavaria, led by the superintendent of Bavaria. The so ware is developed to support and direct police operations. Based on past data of housebreaking, it predicts which areas are vulnerable for burglaries in the future. More police o cers can be sent to those critical areas. The method itself is called Near Repeat Prognostic and is used in the U.S. and the U.K.

The project runs from October 2014 until March 2015 in Bavaria, more specifically in Munich and in Middle Franconia. Those two areas were chosen for their representativeness: Munich as a urban region and Middle Franconia as a rural region. If the project is successful, it will be rolled out in those areas. The results of the project will be presented to the Bavarian Ministry of Internal A airs soon. The figures are said to be similar to the ones in Zürich: in Zürich the number of burglaries dropped by 30 per cent.

Baden-Wuer emberg will soon use the so ware Precobs as well. Nord Rhine-Westphalia is also busy with starting a Predictive Policing project. However, they are approaching it with di erent so ware. The other federal states are a entively observing the pilot project in Bavaria before they implement it.

More information

Julia Klein en Joop Gilijamse
Email: berlijn@ianetwerk.nl
IA Duitsland

Turkije

Cybersecurity en Bescherming Kritieke Infrastructuur: ontwikkelingen in Turkije

Aanleiding

Ten behoeve van de The Hague Security Delta dag tijdens het IA voorjaarsbezoek worden in dit stuk de belangrijkste ontwikkelingen aangaande cybersecurity, bescherming vitale infrastructuur en stedelijke veiligheid beschreven. De onderwerpen bescherming vitale infrastructuur en stedelijke veiligheid worden bij elkaar genomen, omdat daar in Turkije beleidsmatig niet specifiek een onderscheid in wordt gemaakt.

Inleiding

De eerste stappen in Turkije om tot een moderne definitie en implementatie van bescherming van kritieke infrastructuur te komen, werden in 2009 genomen door de *e-Regulation Working Group* die werd voorgezeten door de premier. Deze werkgroep bereidde de *e-State and Information Society Law Proposal Draft* voor. Deze conceptwet definieerde weliswaar niet direct wat Turkije verstaat onder kritieke infrastructuur, maar gaat wel in op kritieke informatiesystemen. Op deze conceptwet volgde in 2013 het *National Cyber Security Strategy and 2013-2014 Action Plan* van het ministerie van Transport, Maritieme Zaken en Communicatie, welke op 25 maart 2013 in werking trad. Andere belangrijke actoren op het gebied van kritieke infrastructuur zijn de Turkse Nationale Wetenschapsraad (TUBITAK) en de *Prime Ministry Disaster and Emergency Management Presidency* (AFAD) [1]. De laatste bracht eind 2014 het 2014-2023 *Kritik Altyapilartin Korunmasi Yol Haritasi* document uit, dat vrij vertaald de 2014-2023 Roadmap voor de Bescherming van de Kritieke Infrastructuur betekent.

Cyber Security

Cyber security wordt in Turkije door verschillende partijen behandeld en daardoor is het niet eenvoudig een eenduidige een gecoördineerde strategie te ontdekken. Tot 2012 was de Turkse Wetenschaps- en Technologieraad verantwoordelijk voor cyber security. Vanaf oktober 2012 is deze verantwoordelijkheid verschoven naar het ministerie van Transport, Maritieme Zaken en Communicatie. Dit ministerie ontwikkelt beleid omtrent cybersecurity en dat beleid wordt vervolgens uitgevoerd door de Turkse *Information and Communication Technology Authority* (ICTA)[1]. Daarnaast is er ook een *Cyber Security Board*[2] ingesteld (deze valt onder de ICTA), waarin vertegenwoordigers zi en van onder andere verschillende ministeries, de Turkse AIVD, defensie, TUBITAK, de opsporingseenheid belast met financiële criminaliteit (MASAK), de telecommunicatie en communicatie commissie (TİB) en de telecomautoriteit [2]. Ook voert TUBITAK en het Turkse ministerie van defensie activiteiten uit op het gebied van cyber security en cyber defense. Zo hee TUBITAK een cyber security onderzoekscentrum[3] dat zich richt op de ontwikkeling van de volgende technologieën met betrekking tot cyber security:

- Het ontwikkelen van cyber space valkuilen en honeypot systemen.
- Systemen die het lekken van data tegengaan.
- Systemen ten behoeve van het analyseren van externe media.
- Controle en rapportage systemen met betrekking tot interne oegang.
- Simuleren van cyber aanvallen.

Hoewel de industrie via het Turkse ministerie van Defensie (vooral de bedrijven ASELSAN op het gebied van elektronica en HAVELSAN op het gebied van so ware) ook programma's ontwikkelt op het gebied van cyber security, bevindt 70% van alle cyber security programma's zich bij TUBITAK [3].

1. h p://www.btk.gov.tr/
2. h p://www.btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/siberguvkurulu.php
3. h p://sge.bilgem.tubitak.gov.tr/en

Turkije telt twee geaccrediteerde *Computer Emergency Response Teams* (CERT). USOM[4] wordt door de overheid beheert en hee een Memorandum of Understanding (MoU) met de NAVO getekend op het terrein van uitwisseling van personeelsleden, deelname in NAVO oefeningen, gezamenlijke reacties op incidenten, toegang tot de NAVO *Computer Incident Response Capability* (NIRC) kwetsbaarheden database en waarschuwingen en als laatste ondersteuning bij het analyseren van schadelijke code. De andere CERT valt onder TUBITAK (ULAK-CIRT)[5] en richt zich meer op onderzoek en training, bijvoorbeeld op het gebied van CEH, ISO IEC 27001 Lead Auditor, internet governance, IT recht en dergelijke. In de laatste drie jaar hee Turkije drie nationale oefeningen gehouden op het gebied van cyber security, waarbij deelnemers van zowel de publieke als de private sector cyberaanvallen simuleerden [3].

Het *Cyber Space Defense Center* (SOSAM) is een onderzoekscentrum in Ankara dat onder het *National Information Systems Security* programma valt. SOSAM beschikt over echte en honeypot systemen die data vergaren over internetverkeer en cyber aanvallen, waarbij de aandacht zich met name richt op aanvallen op publieke instellingen, profileren en rapporteren over cyberaanvallen, waarschuwen en voorzorgsmaatregelen nemen en het vernietigen van botnets [2].

Verschillende universiteiten, zoals Bahçeşehir Universiteit, Ankara Universiteit, Bilgi Universiteit, bieden opleidingen aan betre ende onder andere *information security engineering*, cyber security en IT recht [3]. Ook zijn er verschillende websites opgericht om onder het publiek meer bewustzijn te creëren op het gebied van cyber security[6].

Het ministerie van Transport, Maritieme Zaken en Communicatie hee in consultatie met stakeholders uit de private sector, de academische wereld en overheidsinstellingen een strategiedocument opgesteld. Deze Cyber Security strategie definieert 29 activiteiten en 95 sub activiteiten en wijst verantwoordelijkheden aan op het gebied van wetgeving, *capacity building* en de ontwikkeling van de technologische infrastructuur. Dit vormt op zijn beurt dan de *roadmap* voor cybersecurity in Turkije. De uitvoering van de cyber security strategie ligt bij de *Cyber Security Board* [2]. De activiteiten kunnen als volgt samengevat worden [3]:

1. De oprichting van een Nationale Cyber Security Raad (deze is inmiddels opgericht in de vorm van het Cyber Security Board).
2. Het uitvoeren van jaarlijkse risicoanalyses op het gebied van cybersecurity.
3. De oprichting van een *National Cyber Threat and Vulnerability Analysis Center Laboratory*.
4. De oprichting van een *Cyber Security Center of Excellence*.
5. De verplichting voor overheidsinstellingen en private partijen die met kritieke infrastructuur werken te voldoen aan TS ISO/IEC 27001 *Information Security Management System*.
6. Vergroten van het bewustzijn rondom cyber security.
7. Het ontwikkelen van een basis cyber security cursus in relevante universiteit curricula.

De volgende stap is om meer coördinatie aan te brengen via een nationaal raamwerk waarin alle cyber security en cyber defense initiatieven een plaats krijgen, dat de vorm moet krijgen van een *Cyber Security Operations Center* dat met behulp van nationale so - ware vorm moet krijgen [5].

Commentaar

Cyber security is relatief nieuw in Turkije en staat qua techniek, infrastructuur en we elijk raamwerk nog in de kinderschoenen. Er zijn veel partijen betrokken en deze partijen werken niet altijd even goed samen[7]. Ook zijn er de afgelopen paar jaar een aantal incidenten geweest, met name de afluisterschandalen rondom de premier, waaruit blijkt dat de bescherming van de kritieke informatie infrastructuur niet altijd goed op orde is[8 9]. Ook moet in ogenschouw worden genomen dat in Turkije de bescherming van de staat belangrijker wordt geacht dan de bescherming van individuele vrijheden. Dat betekent in de praktijk dat het uiten van een individuele mening via social media eenvoudig tot een gevangenisstraf kan leiden[10].

Kritieke Infrastructuur

Bescherming van de kritieke infrastructuur staat in Turkije ook nog in de kinderschoenen en is met de verse landelijke stroomstoring van 31 maart 2015 actueler dan ooit. Met name op het gebied van energie, waarvan Turkije een grote doorvoerder is, is bescherming van de infrastructuur van vitaal belang.

De *Prime Ministry Disaster & Emergency Management Authority* (AFAD)hee in oktober 2014 een rapport[11] uitgebracht dat een eerste aanzet is tot het formuleren van een strategie omtrent bescherming vitale infrastructuur en dat moet leiden tot een verbeterde governance structuur, communicatie en internationale integratie aangaande kritieke infrastructuur. Binnen dit rapport worden de volgende roadmaps gepresenteerd:

1. Roadmap technologiche calamiteiten.
2. Roadmap grote industriële ongelukken.
3. Roadmap mijnongelukken.

4. h ps://www.usom.gov.tr/index.html
5. h p://csirt.ulakbim.gov.tr/
6. Onder andere h p://www.bilgiguvenli.gov.tr, h p://www.bilgimikoruyorum.org.tr, h p://www.guvenliweb.org.tr.
7. h p://www.hurriyetdailynews.com/turkeys-cyber-security-a-long-way-to-go.aspx?pageID=238&nid=79076&NewsCatID=483
8. h p://www.todayszaman.com/national_no-qualified-experts-at-tubitak-to-examine-digital-documents_374726.html
9. h p://www.bloomberg.com/news/articles/2015-04-01/turkish-blackout-shows-world-power-grids-under-threat
10. h p://www.slate.com/blogs/the_slatest/2013/06/05/turkey_twi er_arrests_erdo_an_reportedly_detains_25_for_spreading_untrue.html
11. h ps://www.afad.gov.tr/TR/HaberDetay.aspx?IcerikID=3115&ID=5

4. Versterken en ontwikkelen van standaarden op het gebied van bescherming tegen straling.
5. Roadmap bescherming kritieke infrastructuur.
6. Roadmap ongelukken als gevolg van vervoer gevaarlijke sto en.
7. Roadmap ongelukken als gevolg van vervuilde zee.
8. Roadmap biosafety als gevolg van genetisch gemodificeerde organismen.
9. Roadmap calamiteiten als gevolg van klimaatverandering.

De roadmap bescherming kritieke infrastructuur zoekt nadrukkelijk de aansluiting met initiatieven van de Europese Unie zoals het *Critical Infrastructure Warning Information Network* (CIWIN), *European Programme for Critical Infrastructure Protection* (EPCIP), *The International Disaster Database* en het *European Referance Network for Critical Infrastructure Protection*. Verder identificeert de roadmap de volgende activiteiten:

1. Het opze en van een sectorale governance en communicatiestructuur, waarbinnen verantwoordelijkheden duidelijk zijn aangewezen en die moet leiden tot een gedefinieerde opsomming van kritieke infrastructuur per sector. De volgende sectoren worden daarbij als kritiek geïdentificeerd: energie, logistiek, water management en dammen, pers, banken en de financiële sector, landbouw en voedsel, cultuur en toerisme, kritieke dienstverlening richting private en publieke sector en de gezondheidszorg.
2. Het aansluiten bij EU initiatieven en het voldoen aan EU richtlijnen met betrekking tot bescherming kritieke infrastructuur.
3. Het opstellen van operationele veiligheidsplannen.
4. Binnen aangewezen kritieke sectoren en infrastructuren het aanwijzen van een Liaison richting de overheid.
5. Het ontwikkelen en uitvoeren van trainingsprogramma's
6. Het opstellen van nationale veiligheidsdoelstellingen en een daarop gebaseerd Nationaal Veiligheidsplan.
7. Het ontwikkelen van veilige procedures met het oog op het delen en integreren van *best practices*, imminente dreigingen en veiligheidsalarmen met CIWIN.

Commentaar

Omdat dit onderwerp nog in de planningsfase zit, is het nog niet mogelijk aan te geven hoe de gedefinieerde activiteiten zullen uitpakken. Wel is Turkije een land dat met verschillende dreigingen te maken hee , zowel natuurlijk (aardbevingen, overstromingen, ziektes en dergelijke) als door de mens veroorzaakt (onbedoeld dan wel opze elijk). Met het oog op een verdere integratie in de Europese systemen kan het geen kwaad met de Turkse autoriteiten in gesprek te treden om te kijken wat men aan kennis en kunde op het gebied van bescherming kritieke infrastructuur nodig hee .

Meer informatie

Rory Nuijens
Email: ankara@ianetwerk.nl
IA Turkije

Israel

Cyber security in Israel

National Cyber Bureau

De Israelische overheid erkende al in een vroeg stadium het belang van cyber security. Vanaf 1997 zijn er verschillende nationale overheidsprogramma's opgezet voor kennisontwikkeling, economische ontwikkeling en defensie. In 2011 leidde dit tot de oprichting van het Israel National Cyber Bureau (INCB) door premier Netanyahu. INCB maakt onderdeel uit van de Prima Ministers O ce (PMO). Onder leiding van de INCB is Israel uitgegroeid tot wereldleider op het gebied van cyber security.

The Bureau, zoals INCB in Israel wordt genoemd, hee als taak om de veiligheid te vergroten en om Israel tot koploper te maken of houden op het gebied van cyber space.

Activiteiten

- Ontwikkeling nationale cyber defensie strategie en coordinatie samenwerking tussen stakeholders
- Nationale cyber situation room
- Regulering bedrijfsleven
- Definitie van cyberberoepen
- Promotie cyber security binnen het publieke en private domein.
- Promotie Israelische cyber defense industrie.
- "Kidma" (Advancement of Cyber Defense R&D) programma in samenwerking met the Chief Scientist of the Ministry of Industry, Trade and Labor, budget $16 miljoen.
- Opze en "Masad" (Dual Cyber R&D) in samenwerking met Mafat (Directorate of Defense R&D in the Ministry of Defense), budget $2 miljoen.
- Aantrekken investeringen buitenlandse cyber bedrijven.
- Ontwikkeling human capital
- Opze en academisch research fonds voor cyber security in samenwerking met Ministry of Science and Technology ($ 6,5 million voor 2012-2014)
- Afgeven scholarships aan students in cyber, in samenwerking met Ministry of Science and Technology (budget $ 3,5 million for 2012-2014)
- Internationale samenwerking met buitenlandse overheden; delen informatie en gezamenlijke R&D

Israel Defence Force (IDF)

In Israel speelt het leger (een belangrijke rol in de cyber space. Grote investeringen worden gedaan in nieuwe technologie en kennis ontwikkeling ook op gebied van cyber security. Israeliers vervullen een driejarige dienstplicht. Voor de elite high-tech units van het leger zoals Unit 8200 worden de knapste koppen gerekruteerd die zich bezig houden met de nieuwste technologische ontwikkelingen. Veel mensen in tech startups, cybertech en defensie industrie hebben een achtergrond in deze units.

De ontwikkeling van veel producten producten en techniek wordt uitbesteed binnen de eigen Israelische defensie industrie:

- Elbit,
- IAI ELTA,
- Rafael,
- Lockheed Martin (sterke aanwezigheid in Israel)

Belangrijke ontwikkeling in cybertech waar IDF op inzet:

- dataverzameling via UAV (Unmanned Aerial Vehicles),
- dataverzameling en -analyse via internet en andere telecommunicatie systemen
- bescherming kritische infrastructuur
- cyber warfare in om vijandige doelen aan te vallen. (Stuxnet aanval Iraan atoomprogramma)

Naast de IDF zijn ook het ministerie van Jusitie, de binnenlandse (Sjin Bet) en buitenlandse veiligheidsdiensten (Mossad) in Israel verantwoordelijk voor cyber security en het beschermen van kriti-

sche infrastructuur. De geheime diensten gebruiken cybertech om te infiltreren in vijandige netwerken en verdachte informatie uit communicatie data te filteren.

De hackers die worden gerekruteerd door de veiligheidsdiensten of de Israelische defensie industrie hebben vaak een achtergrond in de high-tech units van IDF. Het rekruteren van hackers is in Israel daarom ook makkelijker dan in de meeste andere ontwikkelde landen.

High tech industrie

Israel hee vanaf het begin een belangrijke rol gespeeld in de opkomst van de IT sector; met name in de ontwikkeling van microprocessoren (Intel Lab in Haifa). Onderzoekers hebben een bepalende rol gespeeld bij ontwikkelingen energiezuinige microprocessoren voor mobiele toepassingen. Op dit moment hebben alle belangrijke spelers een researchcentrum in Israel: Cisco, Microso , Google, Apple, IBM, Oracle, SAP, Motorola, HP, Facebook, and eBay.
Veel van de onderzoeksactiviteiten richten zich nu op cyber security.

Check Point

Een belangrijke speler uit Israel is Check Point dat in de jaren 90 als eerste kwam met firewalls . Dit bedrijf is inmiddels uitgegroeid tot een wereldwijd toonaangevend cyber security bedrijf en staat genoteerd aan de Nasdaq. Het is in 20 jaar tijd uitgegroeid tot het grootste Israelische high-tech bedrijf (Revenue $1,5 B, 100.000 klanten wereldwijd).

Andere belangrijke cyber security bedrijven actief in Israel met centers of excellence en/of R&D Centers:

- Oracle
- Cisco
- EMC
- RSA
- Trend Micro
- Kaspersky lab
- IBM
- Deutsche Telecom

Startups

Israel wordt ook wel "The Startup Nation" genoemd omdat het de hoogste dichtheid aan startups per inwoner hee in de wereld. Een op elke 1.844 inwoner (2,5 keer de hoeveelheid in de VS). Er zijn meer Israelische bedrijven genoteerd aan de Nasdaq dan alle Europese bedrijven samen. Israel staat derde als het gaat om beschikbaarheid van Venture Capital en tweede in de wereld voor wat betre de beschikbaarheid van gekwalificeerder wetenschappers en technologen.

Ook op het gebied van startups in cyber security is Israel toonaangevend.
In 2013 en 2014 zijn acquisities gedaan door IBM, Cisco, en GE in Israelische cyber tech startups.

De meeste startups zijn actief in de regio Tel Aviv. Maar er vind nu ook een concentratie plaats van cyber security bedrijven in de woestijnstad Be'er Sheva.

Veel startups houden zich bezig met de analyse van big data en patroonherkenning. De technologie en algoritmen die creditcardmaatschappijen en banken gebruiken om verdachte transacties te herkennen zijn veelal a omstig van Israelische startups. Een mooi voorbeeld is het bedrijf Thetaray dat samenwerkt met Nederlandse banken bij data analyse en compliance.

Een belangrijke nieuwe ontwikkeling waar veel startups zich nu op richten is ontwikkeling en de security van the Internet of Thing (IOT).

Op 24 en 25 maart vond de Cybertech conferentie plaats in Tel Aviv. Dit is na de RSA Conferentie in Silicon Valley de belangrijkste conferentie voor cybersecurity bedrijven. Het gaat vooral over de toepassing van nieuwe technologie. Er waren ook tientallen startups aanwezig. Een lijst met de meeste Isralische cyber startups en hun producten is hier te vinden:
h ps://www.cybertechisrael.com/startups

Cyber campus Be'er Sheva

Op 3 september 2013 was een nieuwe mijlpaal in de ontwikkeling van de high-tech en cybersecurity sector in Israel. Premier Benjamin Netanyahu opende het Advanced Technology Park (ATP) op de campus van Ben Gurion University in Be'er Sheva.

In ATP komen drie belangrijke onderdelen van het Israelische innovatie ecosysteem samen: universiteiten, tech industrie en het leger (IDF).

De eerste private investeerders in ATP waren Deutsche Telekom, EMC, RSA, Lockheed Martin en Oracle

Begin 2015 is het incubator gebouw op ATP geopend waar de VCs met de startups zich vestigen. De investerende VCs zijn: Jerusalem Venture Partner's CyberLabs, Elbit Incubit, and BGN Technologies. BGN is de tech transfer o ce van de Ben Gurion University (BGU). BGN hee licenties afgegeven aan meer dan 150 verschillende bedrijven. 16% van de research budge en van de Ben Gurion University komt uit de licentie inkomsten van BGN.

Een belangrijke reden dat ATP in Be'er Sheva is gekomen is de aanwezigheid van de IDF technology campus; het R&D centrum van het Israelische leger. 5000 mensen van IDF's Center of Computing and Information Systems zijn werkzaam op deze campus. Deze units van IDF zullen zich bezighouden met een combinatie van traditionele cybersecurity en data analyse van het internet, communicatiesystemen, satellietsystemenen van de grensobservatie via drones.

Universiteiten

De Ben Gurion University hee een belangrijke rol gespeeld in de ontwikkeling van Be'er Sheva tot de cyber security hotspot van Israel. De universiteit is sterk in toegepast onderzoek en samenwerking met de industrie. ATP is verbonden met de campus van de BGU.

BGU doet veel onderzoek naar cyber crime en privacy issues op sociale media. Het begon met samenwerking met Deutsche Telecom. Die al in 2004 een center of excellence starte op de campus van BGU. Daarnaast zijn de onderzoekers van BGU betrokken bij Advanced Persistent Threats (APTs), honeytokens en intrusion detection systems.

Andere belangrijke universiteiten in Israel die een belangrijke rol spelen in het cyber domein zijn Technion, Hebrew University en Tel Aviv University. Deze hebben gerenomeerde wiskunde faculteiten met veel kennis over algoritmen en big data. Ook IOT is een belangrijk nieuw onderzoeksterrein voor de universiteiten.

Meer informatie

Marc Nellen
Email: israel@ianetwerk.nl
IA Israel

Rusland

Cyber security in Rusland

De ICT-sector in Rusland groeit, met so ware en digitale dienstverlening als essentiële pijlers. Deze ontwikkeling is niet verwonderlijk; na een jarenlange a ankelijkheid van buitenlandse hard- en so ware producten en diensten is de Russische overheid een weg ingeslagen naar de lokalisering van de eigen ICT-sector en de stimulering van technologieën van Russische origine.

Geholpen door de toetreding van Rusland tot de WTO en dankzij de harmonisering van industriële standaarden met internationale kaders, kunnen IT-bedrijven van Russische bodem daadwerkelijk steeds beter concurreren met buitenlandse bedrijven. In specifieke segmenten, zoals informatiebeveiliging, maken ze zelfs een aanzienlijk verschil: Kaspersky, Group-IB en Zecurion, alle van Russische origine, opereren wereldwijd.

Met het groeiende aanbod aan technologie, kennis en diensten, van zowel buitenlandse makelij als van eigen bodem, neemt ook de activiteit van gebruikers van 'Runet '(het Russische internet) toe. In 2014 maakte maar liefst 83 miljoen Russen gebruik van Internet (haast 60% van de Russische bevolking), een groei van 7% ten opzichte van 2013. Indien de lijn doorzet zijn er in 2018 ruim 96 miljoen Russen actief op Runet. Rusland is een van de grootste markten wereldwijd; alleen China, VS, India, Japan en Brazilië kennen een grotere internetpenetratie.

De afgelopen jaren is Rusland ook bekend geraakt met bij-e ecten van een onstuimige economische en sociaal-maatschappelijke ontwikkeling: cybercrime. In 2014 registreerde het Russische Ministerie van Binnenlandse Zaken 11.000 misdaden op internet en in cyberspace en voor 2015 verwacht het een forse toename. Deze vorm van criminaliteit kost de Russische economie in 2015 naar scha ing meer dan 1 miljard euro.

Sommige specifieke gebeurtenissen versterken het besef van kwetsbaarheid. Zo legde een veiligheidsoefening in de zomer van 2014 een aantal zwaktes van het internet en de vitale infrastructuur bloot. Wat volgde was een landelijke politieke dialoog over beveiligingsmaatregelen, waarbij extreme beschermingsmogelijkheden, zoals een 'kill-switch', niet werden uitgesloten. En uiteraard zijn er geopolitieke aanleidingen die aanleiding vormen de veiligheid van cyberspace en de landelijke vitale infrastructuur strakker te monitoren en analyseren.

Cyber-strategie

Begin dit jaar kondigde de Russische Veiligheidsraad, het Presidentiële adviesorgaan voor nationale veiligheid, dan ook de herziening aan van de nationale informatieveiligheid-strategie. De strategie borduurt voort op de cyber-doctrine die president Poetin in 2000 hee ingevoerd. Hoofddoel van de nieuwe strategie is het borgen van de veiligheid van personen, organisaties en de overheid, via een divers aantal maatregelen en stappen. Meer concreet: de Russische overheid wil gerichter kunnen optreden tegen cyber-crimes, specifiek identiteitsfraude en de productie en verspreiding van malware. En natuurlijk doelt de strategie ook op een e ectievere inzet in cyberoorlog, en tegen terrorisme en bedreigingen van de binnenlandse veiligheid.

De cyberstrategie omvat een breed en compleet spectrum van actielijnen: het introduceren van standaarden en audits; het opze en van technisch-wetenschappelijke programma's en aanwijzen van centra voor toegepast en fundamenteel onderzoek; het opze en van curricula voor cyber-security specialisten en het bijscholen van ambtenaren; nationale en internationale informatieuitwisseling en samenwerking; en, tot slot, voorlichting en publiekscampagnes.

De strategie is nog niet aangenomen. Vooruitlopend daarop is de komst van een nieuw Cyber Response Centre aangekondigd, dat 24/7 cyberspace zal afspeuren en analyseren. Deze organisatie wordt naar alle waarschijnlijkheid belast met de taak cyber-aanvallen af te wentelen en te weerstaan en in geval van bedreigingen nationale acties te coördineren.

Bescherming vs afscherming

Deze stap naar een nationale cyberstrategie gaat gepaard met de introductie van diverse we elijke maatregelen die het Russische internet reguleren. Zo verplicht de aangepaste Wet op Persoonsgegevens buitenlandse Internetbedrijven om data van en over Russische ingezetenen vanaf 1 september 2015 op Russische servers (lees: Russische bodem) te plaatsen. De herziene Wet op Informatieveiligheid maakt het mogelijk voor de overheid om zonder rechtsgang informatie te blokkeren, specifiek om drugscriminaliteit en extremistische cq terroristische acties tegen te gaan. Ook internet-piraterij wordt steviger bij wet aangepakt. Tot slot worden bloggers ingekaderd: met meer dan 3000 volgers moet men zich registreren bij toezichthouder Roskomnadzor.

De nieuwe we en stuiten op consumentenprotest én bezwaren vanuit de Russische IT-sector: op korte termijn werken ze kosten- en prijsopdrijvend voor IT-bedrijven en hun klanten. De kans is evenwel groot dat deze beschermende maatregelen op lange termijn het bedoelde katalyserende e ect hebben op de lokalisering van Russische IT-productie. En het andere vooruitzicht is er ook: buitenlandse bedrijven vrezen dat de versterkte regulering een negatief e ect hebben op het overall ondernemings- en investeringsklimaat in Rusland.

Concentratie

De groei en ontwikkeling in de informatietechnologie in Rusland concentreert zich in en rondom Sint-Petersburg en Moskou: 68% van de grootste Russische IT-bedrijven is gevestigd in Moskou, 7% rond Sint-Petersburg. De ITMO National Research University in Sint-Petersburg gee de toon aan op het gebied van IT-opleidingen, specifiek ook security. Skolkovo Innovation Center net even buiten Moskou is dé broedplaats voor technologische IT-start-ups vanuit heel Rusland.

Meer informatie

Pauline Döll
Email: moskou@ianetwerk.nl
IA Rusland

Innopolis

De republiek Tatarstan kan niet los gezien worden van de IT-sector en security-vraagstukken. Kazan (hoofdstad van Tatarstan, 800 km van Moskou) is door de Russische overheid aangewezen als IT-hub van Rusland. Dit megaproject, genaamd 'Innopolis', omvat een universiteit, diverse technoparks en Speciale Economische Zone. De overheid investeert fors in de diverse onderdelen van het project Innopolis. De stad zal in het najaar worden geopend en vanaf dan gaan fungeren als nationale bakermat én brug voor IT-kennis, technologie en industrie. De universiteit, Innopolis University, is de eerste volledig gespecialiseerde IT-universiteit in Rusland. De eerste bachelor en masters opleidingen zijn in 2013 van start gegaan. De richting Security is in wording en zal in 2016 van start gaan.

India

Cyber security in India

India is slowly starting to realise that security is an issue. Especially a er the Mumbai terrorist a acks (august 2008) security was stepped up and programs to develop strategies were started.
Especially in the fields of Cyber Security and forensic Science India is looking to the Netherlands for expertise, experiences and technologies. Also the Indian private sector is gaining speed in the security area. Companies like Tata and Reliance are building up expertise in cyber security and security of critical infrastructure.

Cyber security

National Cyber Security Policy is a Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India. The policy is still due to be passed by parliament, aimed at protecting the public and private infrastructure from cyber a acks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".

Under pressure, Government unveiled National Cyber Security Policy 2013 on 2 July 2013. Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country.
- To create an assurance framework for design of security policies
- To strengthen the Regulatory Framework
- To create workforce for 5,00,000 professionals skilled in next 5 years
- To provide fiscal benefit to businesses for adoption of standard security practices and processes.
- To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data the .

Stakeholders

1. GOVERNMENT AGENCIES: DEITY, CERT – IN (COMPUTER EMERGENCY RESPONSE TEAM)
2. APEX BODY DSCI – DATA SECURITY COUNCIL OF INDIA
3. INSTITUTIONS IIIT DELHI – Cyber security Education and Research Centre,

NWO has signed a MoU with the Department of IT to collaborate together in the field of Computer science. Last year they launched a joint call for proposals in the field of Big data, Internet of Things and Serious gaming. Indo-Dutch Scientist could submit proposal provided that at least 10% of the project costs were provided by industry. For India this is a novel way of involving industry in scientific research.

Urban security/Forensic Science

Recent rape cases has put Urban Security on top of the agenda of the Indian Government. The new Modi government has launched the police modernisation project. A large budget is available for training and upgrading of the policy force. The Central Bureau of Investigation (CBI), the premiere institute for high level investigations, has signed a MoU with NFI on collaborations in Forensic science. This is the only MoU which CBI has with a foreign entity. The focus is on DNA analysis, cyber forensics and quality/process control. Apart form training NFI will also assist with the design of the new forensic laboratory of CBI.

Security is a hot topic in India. Indian government, institutes and private sector are looking for technology and knowledge. There are good opportunities for doing business. But it is essential that western technology is adjusted to the Indian context. India is highly cost sensitive. Doing business requires an Indian partner who knows the system. The IA team is there to assist you!

More information

Jelle Nijdam
Email: delhi@ianetwerk.nl
IA India

Singapore

In Smart Nation Singapore hee veiligheid prioriteit

Het economische succes van de stadstaat Singapore is in hoge mate a ankelijk van 'security'. De economie is door gebrek aan thuismarkt in grote mate a ankelijk van internationale investeringen, services, handel en productie voor de export. Voor water, energie en voedsel is Singapore a ankelijk van de import.

Innoveren voor grensbewaking en binnenlandse veiligheid

In Singapore is smokkel (van personen en goederen), witwassen en cybercrime meest voorkomend. Het '*Ministry of Home Affairs*' (MHA), verantwoordelijk voor de binnenlandse veiligheid, is altijd op zoek naar nieuwe opsporingsmethodes. In het MHA neemt het '*Office of the Chief Science & Technology Officer*' (OCSTO) een prominente plek in. OCSTO ontwikkelt en implementeert nieuwe technologieën voor vroegtijdige opsporing. OCSTO hee zes thema's voor samenwerking geïdentificeerd: Maritiem & Grens; Infrastructuur; Transport; '*Emergency Preparedness & Response*'; '*Law Enforcement*'; en Humane Factoren. Ook de politie hee steeds meer toegang tot high tech tools om preventie en opsporing te verbeteren, zoals camera's en opnameapparatuur. De burgers worden aangemoedigd informatie te delen via online portals zoals '*CrimeStopper*' en '*E-Feedback on Road Users*' en ook elektronische aangi e van diefstal te doen.

Elektriciteit is a omstig van geïmporteerde LNG

Singapore's elektriciteitsnetwerk is zeer stabiel. De elektriciteit wordt voor 92% opgewekt met LNG, de rest via olie(derivaten), afvalverbranding en duurzame bronnen. Duurzame energiebronnen zijn voor Singapore zeer beperkt in verband met het geringe land- en dakoppervlak voor zonne-energie en afwezigheid van wind en getijden. De '*Energy Market Authority*', '*National Research Foundation*', '*Agency for Science, Technology and Research*' (A*STAR) en '*Nanyang Technological University*' werken in wisselende samenstelling samen met (inter)nationale private partijen en kennisinstellingen in onderzoek en innovatie gericht op cleantech, energie management, infrastructuur en duurzaamheid. Een voorbeeld is het '*Experimental Power Grid Centre*' (EPGC) is een onderzoeksinstituut onder A*STAR dat zich richt op onderzoek naar smart grids en micro grids. Het EPGC biedt onderdak aan een 1MW LV (400V) net dat volledig losgekoppeld kan worden van het vaste net. Door middel van emulators (netwerk, impedantie, wind en zon) en programmeerbare netwerkbelasting kunnen gewenste situaties nagebootst worden om onderzoek op te verrichten. Dit gee veel flexibiliteit ten opzichte van een smart/microgrid testbed opstelling. Het onderzoek binnen EPGC richt zich voornamelijk op integratie van decentrale duurzame energieopwekking. Een tweede focusgebied is integratie van opslag, hiervoor zijn ook verschillende types ba erijen en capaciteiten beschikbaar. Het laatste focusgebied is microgrids voor afgelegen gebieden in de regio en '*urban microgrids*' voor crisis management. Voor alles wat niet met het microgrid gesimuleerd kan worden is er ook een real-time simulator met '*hardware-in-the-loop*' mogelijkheden beschikbaar. Het EPGC is een geavanceerd onderzoekslab dat unieke mogelijkheden biedt om onderzoek te doen naar smart grids en microgrids in de tropen.

Voedselaanbod is gevoelig voor fluctuaties in kwaliteit en prijs

Singapore importeert meer dan negentig procent van haar voedsel en het voedselaanbod is daarmee gevoelig voor fluctuaties in kwaliteit, kwantiteit en prijs. Singapore hee niet genoeg land, water, energie en mankracht ter beschikking om zelfvoorzienend te zijn. Het voedselzekerheidsbeleid wordt uitgezet door het Ministry of National Development (MND) en uitgevoerd en gecontroleerd door de Agri-Food & Veterinary Authority of Singapore (AVA). AVA is de verantwoor-

delijke instantie voor voedselveiligheid en voedselzekerheid. In 2013 presenteerde AVA de eerste '*Food Security Roadmap*'. Het doel is om te zorgen dat iedereen in Singapore toegang hee tot veilig, voedzaam en betaalbare voedsel. Deze roadmap legt de nadruk op twee verschillende oplossingen, namelijk diversificatie van de import en optimalisatie van de lokale productie. Singapore is actief op zoek naar smart technologieën en vertical farming om de opbrengst van lokale productie van vis, bladgroente en eieren te verhogen.

Waterzekerheid en -veiligheid is een constant aandachtspunt.

De motivatie om voortdurend te innoveren en ontwikkelen hee Singapore in de afgelopen decennia doen uitbloeien tot een innovatieve water- en milieu industrie. Singapore hee een lange weg afgelegd sinds haar waterrantsoenering en overstromingen in de jaren '60 en '70. Singapore kampt regelmatig met langdurige en intensieve regenval. In de meeste gevallen kan het drainagesysteem omgaan met deze regen, echter zeer zware regenval kan soms groter zijn dan de ontworpen rioolcapaciteit, vooral in laaggelegen gebieden. Dat is wanneer zogenaamde 'flash floods', kleine en plaatselijke overstromingen die relatief snel komen en gaan, kunnen optreden. Singapore kondigde in 2012 het '*Flood Resilience Plan*' aan, welke een compleet spectrum van drainage- en overstroming management bevat. Singapore hee zich ontwikkeld tot 'Global Hydrohub' en is koploper op het gebied van innovaties in watertechnologie. Op dit moment wordt 40% van het drinkwater geïmporteerd uit Maleisië, de overige 60% wordt verkregen uit lokaal opgevangen regenwater, gezuiverd afvalwater (NEWater) en ontzilt zeewater. Maar de ambitie is om geheel zelfvoorzienend te zijn en de hoeveelheid geïmporteerd drinkwater in 2060 terug te dringen tot 0%. Dit doet zij door flink te investeren in R&D en zich te profileren als 'Living Lab' waar buitenlands onderzoek, technologieën en bedrijven verwelkomd worden door de Singaporese overheid. Een voorbeeld van huidige innovatieve ontwikkelingen is het 'SMART Water Grid', welke door ICT en sterk analytische so ware de watersector zal versterken op het gebied van levering en kwaliteitswaarborging.

's Werelds Eerste Smart Nation

Singapore hee zichzelf in 2014 uitgeroepen tot 's werelds eerste smart nation. De komende jaren zal Singapore het netwerk van sensoren uitbreiden en verbinden, tools ontwikkelen voor verzamelen en analyseren van data. Het gebruik van slimme technologie zal de lee aarheid in het land verhogen en de burger en overheid een beter overzicht geven van wat er gaande is in de samenleving. Een verhoogde situational awareness verbindt burger, overheid en bedrijven en maakt uitwisseling van informatie meer interactief. Waar *smart solutions* en *cities* in Nederland gericht zijn op zorgen voor een duurzame toekomst, brengt Singapore de boodschap van lee aarheid en smart in verband met dagelijks gemak.

Cybersecurity is de voorwaarde voor succesvolle smart nation

De ontwikkeling van de cybersecurity sector in Singapore gaan snel. Dit hangt samen met de toenemende internetcriminaliteit enerzijds en de ontwikkeling van Singapore als een Smart Nation en (behoud van de) goede reputatie op het gebied van e-government anderzijds. Sinds 2005 stelt de Infocomm Development Authority een masterplan op voor 3-5 jaar. Het masterplan is de leidraad voor de nationale ontwikkelingen om de cyberdreiging voor overheid, kritieke infrastructuur, bedrijven en burgers te verminderen. De overheid hee drie strategieën voor sectorontwikkeling geïdentificeerd. Per april 2015 zal het nieuwe Cyber Security Agency (CSA) een coördinerende rol over deze drie strategieën op zich nemen.

1. Verbeteren van veiligheid en weerbaarheid van kritieke infrastructuur. Met 'security assessments' en '*national cyber security exercise programme*' wordt de weerbaarheid getest en verbeterd. De overheid neemt een proactieve rol door het 'upgraden' van '*Cyber Watch Centre*', voor monitoren van publieke sector, en '*Threat Analysis Centre*' voor analyseren van big data en advisering van publieke sector;
2. Stimuleren van veilig internet gebruik door bedrijven en burgers door informatie campagnes;
3. Vergroten van de talentpool aan professionals. Voor publiek-privaat onderzoek in '*National Cybersecurity R&D Programme*' is een budget van 130 miljoen SGD (95 miljoen EUR) voor 5 jaren vrijgemaakt. In het kader van leven lang leren is in samenwerking met 'CLT partners' een trainingprogramma ontwikkeld. Training met realistische simulaties van cyberaanvallen kan in het '*Digisafe Cyber Security Centre*'.

Alle bovenstaande strategieën staan open voor samenwerking met internationale bedrijven en kennisinstellingen. De vier universiteiten hebben onderzoeksgroepen in het cybersecurity domein. Een voorbeeld is iTrust, een multidisciplinair onderzoekscentrum in de '*Singapore University of Technology and Design*' (SUTD), in samenwerking met het '*Ministry of Defence*'. De focus ligt op onderzoek binnen de kritische infrastructuur (zoals elektriciteitsnetwerk, drinkwaterbedrijven en oliera naderijen) en op medische technologie zoals pacemakers, defibrillators en insulinepompen. Het Nederlandse consortium SEACRES onder leiding van TNO is sinds 2014 actief in Singapore en werkt onder andere samen met '*Interpol Global Complex for Innovation*' (IGCI). Dit hee onder meer geleid tot de zogenaamde Silk Road Training, een 5-daagse training waarbij de cursisten inzicht verscha en in de aard van internetcriminaliteit en methoden van opsporing van internetcriminaliteit op het anonieme Darkweb. De eerste training zal in juli worden gegeven aan medewerkers van Interpol. Daarnaast is een stevig fundament gelegd inde samen-

werking met lokale universiteiten zoals de '*Nanyang Technological University*' (NTU). In de komende maanden zullen enkele research programma's worden ingediend. Tenslo e is in april het zogenaamde '*Cyber Research and Capability Centre*' (CRCC) geopend. Het CRCC is een publiek-privaat centre of excellence waarbinnen Nederlandse en Singaporese cyber security expertise wordt gebundeld met state-of-the-art technologieën, om integrale oplossingen te bieden voor de strategische cyber cyber behoe en van morgen. De activiteiten in dit centrum zullen bijdragen aan de doelstelling om Singapore te positioneren als een betrouwbare en robuuste info-comm hub.

Bronnen

Dit overzicht bevat informatie uit onze eerdere artikelen:

- *Singapore versterkt haar voedselzekerheids-positie, 28 augustus 2014, Susan van Boxtel*
- *Smart City Singapore, maart 2015, Pam van de Klundert*
- *ICT voor Waterbeheer in Singapore, 12 april 2014, Briek Starink*
- *Singapore als Global Hydrohub, 10 april 2014, Susanne van Loon*
- *Flood Resilience Plan Needs to Evolve with New Challenges, last updated on 19 november 2014, http://www.pub.gov.sg/managingflashfloods/floodresilienceplan/Pages/floodplan.aspx*
- *National Cyber Security Masterplan 2018, Last updated on 08 October 2014, http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/National-Cyber-Security-Masterplan-2018*

Auteurs: *Susan van Boxtel, Bas Kil, Anne Marie Schrijver* en *TAN Chiew Seng Sean*

Meer informatie

Susan van Boxtel
Email: singapore@ianetwerk.nl
IA Singapore

Japan

The government forecasts Japan's first summer Olympics since 1964 will li the economy. But o cials worry it could also make Japan a target for computer hackers

Relevante ontwikkelingen

- Een serie opmerkelijke cyberaanvallen op overheid en bedrijfsleven (**Sony, Mitsubishi, Yahoo Japan**) hee er voor gezorgd dat cybersecurity hoog op de politieke agenda staat.
- In 2020 organiseert **Tokio** de **Olympische Spelen**. Bescherming van kritieke infrastructuur voor 40 miljoen inwoners plus deelnemers is topprioriteit (elektriciteit, communicatie, water en riolering).
- Japan is de derde economie van de wereld en hee toonaangevende industrie (o.a. **Softbank, NTT, NEC, Toshiba, Fujitsu**) en world-class technologisch vermogen.
- Om systemen voor kritieke infrastructuren te testen werkt onderzoeksinstituut CSSC in testbeds samen met industriele partijen.
- Bedrijven als het gigantische NTT Group ontwikkelen beveiligingsdiensten voor bedrijven, maar kijken daarbij ook naar kennis en kunde buiten de landsgrenzen. Overigens is NTT de eerste hoofdsponsor van de Olympische Spelen in Tokio 2020.
- Hoewel Japan traditioneel heel sterk is in hardware, is de kennis en kunde op gebied van so ware niet altijd op hetzelfde niveau. Verder hee Japan een groeiend tekort aan ICT-professionals. De taalbarriere bemoeilijkt soms de internationale uitwisseling van personeel.
- Het zoeken van nauwere internationale samenwerking is een expliciet beleidsdoel en wordt steeds actiever opgepakt door ministeries en research labs.
- Japan stuurt een stevige delegatie naar **GCSC-2015**, inclusief bedrijfsleven, een direct gevolg van de internationale agenda. NL-Japan contacten die op verschillende niveaus zijn gelegd tijdens het Staatsbezoek zullen tijdens de conferentie verder worden aangehaald.
- In 2014 is nieuwe wetgeving doorgevoerd om samenwerking te versterken tussen overheden en bedrijfsleven bij verhogen van cybersecurity.
- Japan is goed gequipeerd om de uitdagingen het hoofd te bieden, maar industrie en overheid tonen bereidheid om daarbij kennis en kunde van buiten aan te trekken.

Cybersecurity, Nederland en Japan

- Cybersecurity was een van de hoofdthema's van het Staatsbezoek van **ZKH Willem-Alexander** en **Koningin Maxima** aan Japan in oktober 2014.
- Een brede delegatie vanuit de Nederlandse cybersecurity gemeenschap nam deel aan de economische missie.
- Het Nederlandse European Network for Cyber Security (**ENCS**) hee sinds 2013 een lopende samenwerking met CSSC, sleutel-speler bij het beschermen van kritieke infrastructuur (gefinancierd vanuit Japanse **Ministerie van EZ**).
- Tussen **27 maart en 8 april 2015** organiseert RvO een **follow-up cybersecuritymissie naar Japan** plaats, met focus op kansen voor Nederlandse onderzoekers en entrepreneurs om bij te dragen aan bescherming van kritieke infrastructuren (o.a. bezoeken aan **Tokyo Electric Power Corporation, NTT Data, Toshiba, NEC, Univeristy of Tokyo**).
- Op gebied van forensische technologie bestaan er goede samenwerkingsverbanden tussen het **NFI** en diverse Japanse spelers, waaronder de Nationale Politie.
- ENCS en HSD kijken naar de optie om een **PIB**-convenant op te stellen.

- De Nederlandse **Cyber Security Raad** is in gesprek met het Japanse **JPCERT** (cyber emergency rescue team) over de mogelijkheden van bilaterale samenwerking, government-to-government.
- Het **IA-netwerk** Tokio is nauw betrokken bij bovenstaande vanuit de Nederlandse ambassade.

Kansen/ specifieke vraag naar buitenlandse kennis en expertise:

- bescherming van systemen voor kritieke infrastructuur; so ware oplossingen voor bescherming bedrijfsgegevens; veilige, intelligente chips; opleidingen; academische uitwisseling; The Hague, centre for global cybersecurity.

Voorwaarden om mogelijke samenwerking te realiseren:

- Een meerjarige aanpak is nodig in Japan. Om goede betrekkingen te smeden, om te bewijzen dat Nederlandse kennis en kunde echt toegevoegde waarde biedt, en om te bewijzen dat men serieuze intenties hee om langjarige (zakelijke) betrekkingen aan te gaan.
- De Olympische Spelen van Tokio 2020 bieden een logische stip aan de horizon. In anticipatie hierop is het Innovatie-team op de ambassade in Tokio al sinds 2012/13 aan de slag – in nauwe samenwerking met partijen uit de Nederlandse cybersecurity wereld zoals **ENCS, Security Matters, DNB en NFI** – om deuren te openen voor Nederlandse spelers en samenwerking met Japanse spelers te starten, versterken en uit te breiden.
- De meerjarige aanpak, vanuit een visie dat beide landen elkaar iets te bieden hebben bij het oplossen van dit grote maatschappelijke vraagstuk, hee gezorgd voor concrete matching van NL en Japan partijen. Er bestaan op dit moment goede contacten met verschillende sleutelspelers binnen overheid en bedrijfsleven, in het bijzonder voor wat betre bescherming van kritieke infrastructuur en forensische aangelegenheden.

Strategische acquisitie:

- Tijdens het staatsbezoek aan Japan in oktober 2014 was het Haagse veiligheids-cluster sterk vertegenwoordigd. O.a. de gemeente **Den Haag, HSD, KPN, de Cyber Security Raad en ENCS** waren op hoog niveau vertegenwoordigd.
- De mogelijkheden voor strategische acquisitie van kennis en activiteiten van Japan naar Nederland kunnen het beste in nauw overleg tussen Innovatie-team Tokio, HSD en specifieke spelers binnen het cybersecuritycluster in de regio Den Haag worden bezien. Op het gebied van academische uitwisseling bestaat reeds samenwerking binnen de MOU ENCS-CSSC.

Bronnen:

Timeline: Cybersecurity programme Netherlands-Japan (as facilitated by IA-network Japan)

June 2013

- First Netherlands cybersecurity and smart grid delegation to Japan
- Visit CSSC testbed facilities and both sides agreed to be in close contact.

November/December 2013

- CSSC delegation visited ENCS and signed a MoU (December 2, 2013)

April 2014

- DENSEK delegation to Japan
- DENSEK advisory board video conference in Tokyo
- (Filmed) interviews with o cials of METI and CSSC

October 2014

- State Visit of NL King and Queen/w second Netherlands cybersecurity delegation to Japan.
- Bilateral cybersecurity round table meeting joined by Minister Kamp and METI
- Discussions about cybersecurity activities on critical infrastructures and possible collaborations between the two countries
- A LoI sighed between ENCS and CSSC to extend further relations (October 29, 2014)

March/April 2015

- Third Netherlands cybersecurity delegation to Japan.
- Focused technology matchmaking mission to follow-up on state visit for selected partners
- Focus on utilities such as TEPCO and KEPCO and research institutes for possible collaborations on critical infrastructure protection.

November 2015 (TBC)

- Fourth cybersecurity delegation to Japan....

Meer informatie

Jan-Hein Chrisstoffels en Kikuo Hayakawa
Email: tokio@ianetwerk.nl
IA Japan

Taiwan

Cyber security in Taiwan

Introduction

Since the late 70's Taiwan is one of the leaders in the global IT industry and forms the heart of the global semiconductor and electronics industry. Over the past years the Taiwanese government tries to capitalize its industrial strengths and research capabilities and focusses strongly on the development of new economic boosters such as the Internet of Things (IoT), cloud computing, mobile communication, smart grids and the next generation communication technologies, such as 5G and near field communication technologies, but also on societal driven innovation such as smart cities and communities.

All these developments rely on sharing more and more information through cyberspace in terms of volume, density and frequency and in e ect cyber security becomes a vital element in future communication and IT technologies and infrastructures. However Taiwan faces serious threats on its cyber security and in 2014 alone Taiwan ranked on the 3rd place as target for cyber-a acks in Asia, only S-Korea a Hong Kong su er from more a acks, according to FireEye Inc, but globally it also ranks among the top targets for cyber-a acks. Taiwan's complex geo-political situation contributes significantly to the amount of cyber-a acks, not only on governmental organizations, critical infrastructure or military installations, but also on the industry and research infrastructure.

Therefore cyber security is a high priority area for the Taiwanese government to protect its national security and economy.

Cyber Security Infrastructure

Cyber-a acks have added a new dimension to the complex geo-political situation of Taiwan and therefore cyber security is taken very seriously in Taiwan and in e ect is an integral part of the homeland security policy over the past 15 years. From 2001 until 2013, the Taiwanese government executed several national programs to improve the information and communication security of Taiwan. In 2001 the National Information and Communication Security Taskforce (NICST) was setup, as an inter-governmental task force to enhance the cyber security of Taiwan and soon a er the Information and Communication Security Technology Center (ICST) was established in March of 2001. The ICST is a technical service center and project management o ce for cyber security projects.

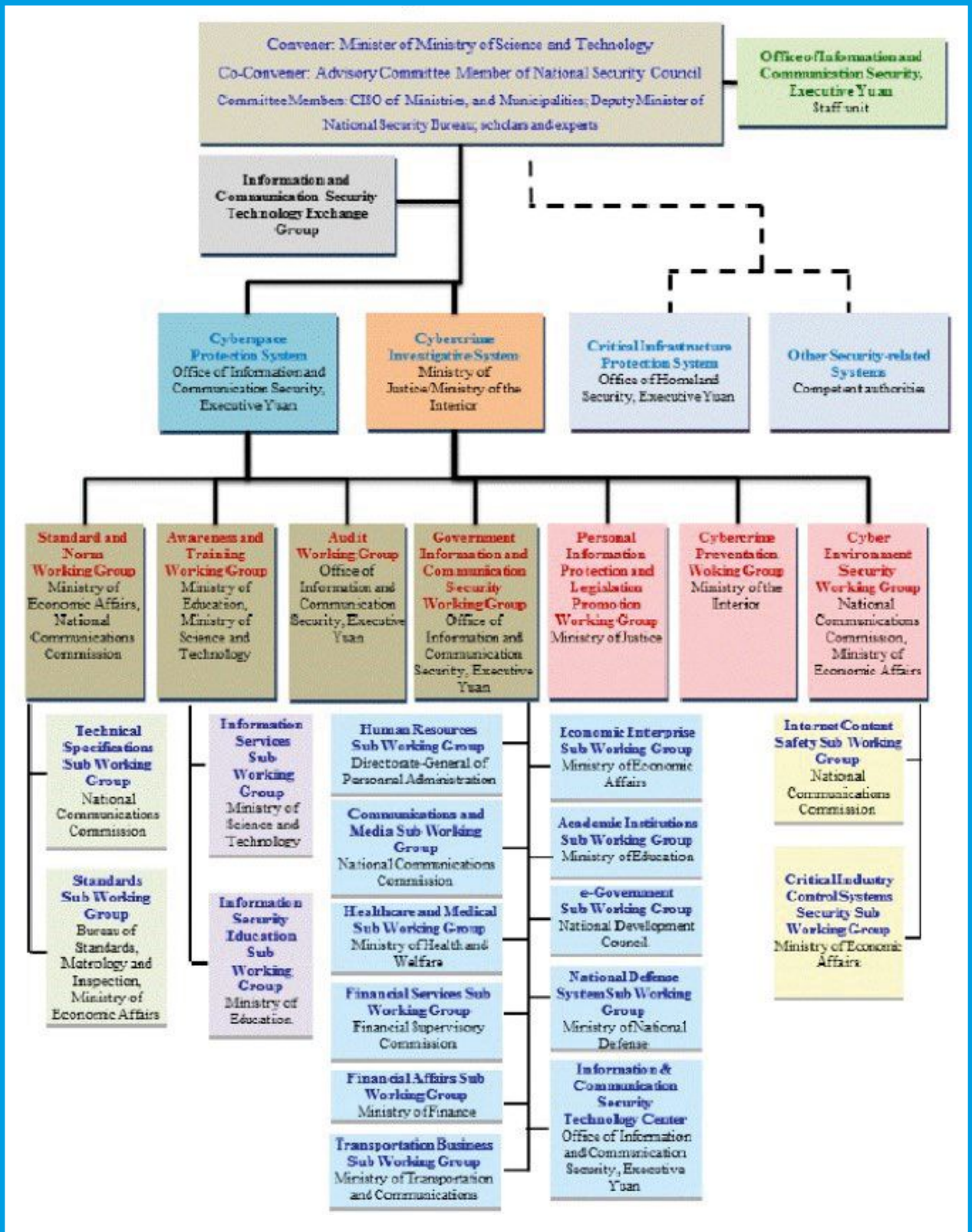

Figure 1 Governance Structure 'National Information and Communication Security Task Force' (NICTS).

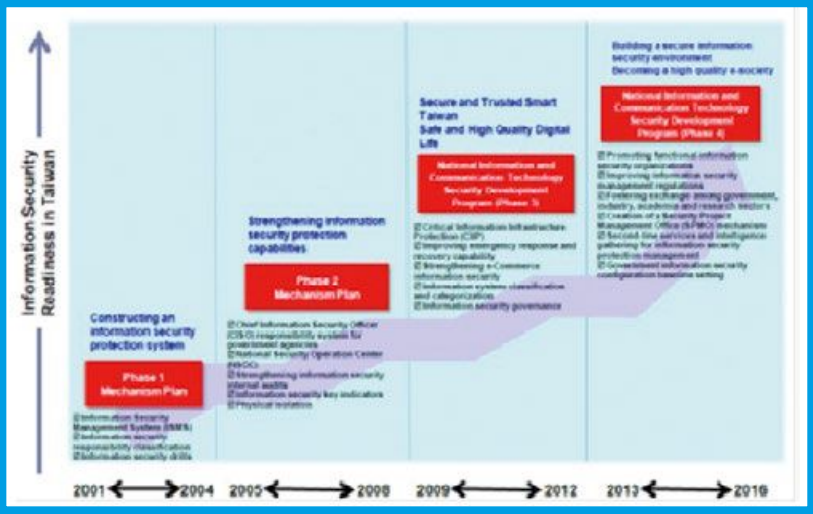

Figure 2 Policy Milestones

Figure 3 National Strategy Cybersecurity Development 2013 - 2016

In 2013 the latest program was initiated under the name: National Strategy Cybersecurity Development and will run until 2016. The program includes promoting information security configurations in information security infrastructures, enhancing second-line monitoring services and intelligence gathering for information security protection management, strengthening information security contingency functions.

The Information and Communication Security Technology Center (ICST) plays an important role in the execution of the National Strategy for Cyber security and its main functions are:

1. Enhancing national information security policies and establishing a secure information environment
2. Improving information security protection management and sharing diverse intelligence on information security
3. Building a firm foundation for information security technology capabilities and integrating practical technological applications
4. Expanding information security talent cultivation and increasing international information security exchanges

Next to the internal policy developments and instruments that have been put in place to enhance Taiwan's Cyber security, Taiwan also reaches out to seek international collaboration with countries that face similar cyber threats as Taiwan.

Research & Development

Taiwan's IT industry and a liated industries have a strong focus on cyber security, especially those involved in the IoT, smart grids, IT hardware and communication technologies, not only for the applications they target with their products or technology, but also to protect their own business against industrial espionage.

The goals set by to government to enhance the national cyber security are also reflected in the focus of the national funded research labs and institutes under the Ministry of Science & Technology and the Ministry of Economic A airs. The la er

ministries are tasked to ensure that the national labs and institutes develop technologies to ensure cyber security for the government, industry and the society. Taiwan's industrial research e orts are also supported by the national research institutes and labs, tasked to do scientific and academic research and to develop applied technologies for the Taiwanese Industry. The most important institutes that are active in the field of Cyber Security or work in fields related to cyber security are listed below:

Institute for Information Industry – III
www.iii.org.tw
- Taiwan's national IT R&D Institute
- Cyber Trust Technology Institute – CTTI (Part of III)
  - Cyber Security and IT Security
- Communication technologies
- Cloud computing
- Smart grids
- Smart living & smart cities
- Policy making

National Applied Research Lab – Narlabs
www.narlabs.org.tw
- Cloud Computing
- Network and Information Security
- High speed computing (Shared facility for super computers and big data)

Industrial Technology Research Institute – ITRI
www.itri.org.tw
- Cloud computing & big data
- Next gen communication technologies – e.g. 5G
- Smart living

Research Center for Information Technology Innovation – CITI
h p://www.citi.sinica.edu.tw/

Research facility under Academia Sinica
- Taiwan Information Security Center – TWISC (Part of CITI)
  - Cryptology
  - Network security
  - So ware security & Multimedia security
  - Information security management

Chinese Cryptology and Information Security Association
h p://www.ccisa.org.tw/
- Association for academic research in cryptology, top IT universities in Taiwan
- Information Security Theory and Technology
- Promotion of Academic research

References

1. Information and Communication Security Technology Center (ICST)
   h ps://www.icst.org.tw/Intro.aspx?lang=en
2. National Information and Communication Security Task Force (NICST)
   h p://www.nicst.ey.gov.tw/en/cp.aspx?n=24F1E75EE39BB346
3. Cyber Security Development Program 2013 - 2016
   h p://www.nicst.ey.gov.tw/en/News.aspx?n=833B775CE6C4F9F5&sms=0A29FF40DDCD03DD

More information

Kasper Nossent
Email: taiwan@ianetwerk.nl
IA Taiwan

China

Cyber security in China

Internet of Things, Smart, Intelligent. These concepts are widely used to indicate the increased integration of information technology in our daily lives. The benefits and potential in our professional and private lives may be obvious, as are the risks that arise when information falls into the wrong hands.

Various questions pop up when thinking about China in this perspective. How does the 'Great Firewall' work? What are the censorship rules from the Chinese cyber authority? Are we pointing in the right direction when talking about the 'Chinese hack at ASML'? How secure is the Netherlands with a Huawei 4G Network? How secure is China with NXP chips in 90% of the Chinese bankcards? How advanced is the hyper secure quantum connection between Shanghai and Beijing?

Currently, China has 642 million active Internet users (47% of the total population). Most of them do not use a virtual private network (VPN) account and are therefore blocked from various international websites. At the beginning of 2015 China cracked down on VPNs, but many are now functioning again. Internet censorship in China is conducted under more than sixty Internet regulations. The governmental authorities not only block websites, but also control the Internet access of geographical regions and individuals.

Besides preventing undesirable information from reaching the Chinese public, censorship and Internet control has two additional e ects. In the first place it is a considerable obstacle for researchers, both in private companies and public institutes, as they o en are barred from accessing information that is relevant for their work. This has led some multinational companies to reconsider the extent of their R&D activities in China. In the second place these policies in practice function as a proxy for a protectionist industrial policy, which heavily favors Chinese enterprises.

In 2014, the Chinese Cyber Authority approved a cyber security directive which requires foreign so - ware companies to disclose source codes before their products can be installed at Chinese financial institutions. In 2019, at least 75 per cent of the information technology infrastructure of any bank in China has to comply with these new regulations. The American and European Chambers of Commerce in China as well as 17 other U.S. business groups have expressed concerns towards the Chinese cyber security authorities, from which no o cial response has been documented yet.

Nonetheless, with a huge number of Internet users as well as a fast developing smart industry, many organizations are involved in designing, maintaining and securing essential infrastructures. These include organizations such as ASML, NXP, Philips, Irdeto, Gemalto, Nedcard. The University of Science and Technology (Advanced Institute for Advanced Technology) is the Chinese frontrunner in the field of hypersecure communication through quantum-base encryption networking.

Highlights Cyber Security China – the Netherlands

- March 1, 2015; ASML confirms that part of its IT system was hacked. Media point at Chinese government (really, government?) hackers. ASML later stated in a press release that the origin of the hackers' intrusion was unclear.
- Huawei has been active in the Netherlands for many years, where it makes a significant contribution to digitizing the Netherlands. For example by building 4G networks, providing intranets for local governments and installing WiFi.
- NXP dominates China's bankcard market as ca. 90% of China's 'smart' bankcards use NXP chips. The chips in Chinese passports are also provided by NXP. NXP is very much aware of the security issue and puts 'cyber security' as one of the four

focus areas. They work together with Chinese parties such as Union Pay, Alipay, Huawei and others, to make the application of their chips more secure.

Hyper secure quantum connections

- In 2014 China started with building a glass-fiber cable connection of 2,000 kilometers providing the opportunity to distribute quantum keys (in order to encrypt information) between Shanghai and Beijing. Ensuring hyper secure data tra c would boost the security of information technology, with applications in on-line payments and communicating sensitive information. The connection is expected to be ready by the end of next year, primarily with connections to financial institutes and (government and army) authorities in Beijing, Hefei, Jinan and Shanghai.
- China is building a satellite for distribute of photons between Asia and Europe in so-called entangled states. This way of teleportation can realize super fast and hyper secure information exchange. The plan is to launch the satellite in 2016.

Trends

End-users/ consumers

- There is a strong enthusiasm for (mobile) Internet use in China. There are around 330 million online shoppers in China. In general it seems that sharing information is trusted.
- More and more products are linked with mobile devices, as a customer service.
- The customer enjoys products/services, while companies collect and use their data.

Companies

- In order to increase the security of products/services, organizations are working more closely together with their clients in order to know what is expected in the field of cyber security.
- There is a strong focus on cyber security within the semiconductor industry. Reasons are the increase in mobile transactions, eGovernment, smart bankcards and user authentication. Also 'connected cars' is expected to play an important role in the field of Cyber Security.

Government

- Strong requirement of ID registration in China, even when traveling by train.
- 'Everyone' is still unaware about the arguments and future plans related to Internet censorship in China, with respect to foreign services (google) and domestic services as well. New regulations require all users of social media, websites, forums and other online entities to register with their government-verified ID. Unsure is when this will be completely integrated as it is di cult to define as well as to implement.
- A er Beijing and Shanghai, the plan is to extend the quantum connection to Guangzhou (North to South connection) and a er that, an East to West strategy is aspired. Existing chip technology will be combined with quantum encryption technology and create hyper secure chips, available for consumer use.

More information

Anouk van der Steen
Email: shanghai@ianetwerk.nl
IA China

Korea

Cyber security in Korea

Introduction

Local governments, broadcasting companies, financial institutions, nuclear power stations and game companies in Korea have one thing in common. They have all been targets of big hack-a acks in the last 12 months. Passwords, blue prints and social security numbers were stolen. Since the incidents, prevention, investigation and prosecution of cybercrime became more important in this country where online and mobile game, shopping, payment are booming and where everyone is connected to a fast mobile and fixed internet connection and where big data and IoT are supposed to be the new growth engines in all major Korea companies.

Structure

Korea's e orts go back a long way. Back in 1985, the Korea Information Technology Research Institute (KITRI) was established for the research and development of cyber-security technology and training of IT-security human resources under the Ministry of Trade, Industry and Energy (MOTIE). In 1997, the Korea National Police Agency (KNPA) established a department fully dedicated to solving cybercrimes.

Since then, the number of related organizations has significantly grown. Organizations are much more structured and segmented. The National Intelligence Service (NIS) is directly under the president of Korea taking charge of general national cyber security policy. It is in charge of investigating government and public facilities. Under the NIS, there are two organizations to protect national information network system: the National Cyber Security Strategy Commi ee and the National Cyber Security Center. National Cyber Security Strategy Commi ee acts as a deliberative body and National Cyber Security Center collects and analyzes information on cyber threats, making manuals, investigations and international cooperation when such a ack occurs.

The Korea Communication Commission (KCC) is in charge of internet monitoring, establishing prevention system, mobile security, corporation information protection and personal information protection. The Ministry of National Defense (MND) is responsible for cyber-terrorism countermeasures. The Personal Information Protection Commission (PIPC) deals with infringement of the personal information countermeasure. Korea National Police Agency (KNPA) operates Cyber Terror Response Center (CTRC) for cyber-crime investigation.

There are also some specialized organizations. The Korea Internet and Security Agency (KISA) works on Internet and information protection. The National Security Research Institute (NSRI) conducts research for public cyber security. The National Computing Information Agency (NCIA) is in charge of the management of the main information network system of governmental organizations.

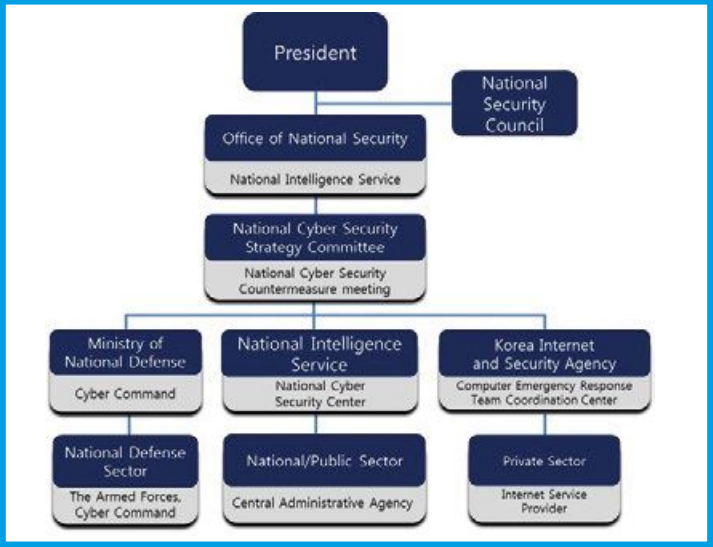

Figure 1 Organizational structure

Research

The renowned *Electronics and Telecommunication Research Institute* (ETRI) in the city Daejeon is supporting the e orts with research activities. ETRI has one department fully devoted to develop cyber technology. Its Cyber Security Research Division focuses on the following topics:

1. Cryptographic Technologies for Data-Privacy

This projects develops fundamental technics to encrypt data of stored information.

2. Smart Wallet 2.0 Technology

The goal of this project is to provide secure login, payment and electronic signature services for smart phones and wearable devices. It works on/o ine anti-phishing technology, NFC-technology, and risk analyzing technology.

3. Device Security Analysis and its Countermeasures

This project is developing technology which analyzes a acks on various layers in a device and designs various countermeasures for an array of possible intrusions. Among others analysis on fault a ack, di erential power a ack, and di erential electromagnetic a ack and intrusion detection in a next-generation wireless LAN access point are fields of interest of this project.

4. Cyber targeted a ack recognition and trace-back technology

The main goal of this research project is to develop an intelligent cyber security technology for the recognition and trace back of cyber targeted a acks on the critical IT system and infrastructure.

5. MTM-based Security Core Technology for Prevention of Information Leakage in Smart Devices

The main goal of this project is to prevent information outflow on lost or stolen mobile devices and block illegal and unauthorized access.

Figure 2 Convergence security at ETRI

6. Security incident detection of pipeline control system

Many pipes (water, oil and gas) are equipped with ICT measurement and control systems to monitor the conditions of the medium that is being transported. Research from this group is focusing on the protection of these systems.

7. Convergence Security

Other infrastructures (such as building, factories and airport) are more and more equipped with ICT-systems which are connected to the internet. This group focuses on the security of four sectors as depicted in the figure below.

Education

The most active university in cyber security is Graduate School of Information Security at Korea University. The purpose of the school is to nurture human resources against the national cyber warfare to protect from and remove local and global threats in the cyber environment. The school has two study tracks, Cyber warfare and Cyber national defense policies, and number of laboratories such as Digital Forensic Lab, Privacy Enhancing Technologies Lab, Multimedia Security Lab (MSL), Hacking and Countermeasure Research Lab, Signal Processing and Advanced Intelligence (SPAI) Lab, Security Analysis and Evaluation Lab, and Risk Management Lab.

National Information Defense Plan

The Ministry of National Defense (MND) in Korea is also heavily involved in the handling cyber threats and protecting its own ICT-systems and that of the country. In March of 2014, it released the “National Information Defense Plan” to address medium and long term plans to protect information based on the Information Protection Act of 2010. It contains three major points:

1. Appropriate timing introduction of IT-technology.

MND wants to search for ICT technology in the non-military sector and apply that in its own field. It is not only looking at communication technology, but also ways to visualize the ba lefield. It has created several test projects and pan-ministerial R&D cooperation projects.

2. Be er use of the ICT-based environments & information systems

Unite all communication networks (fixed and mobile) of all army divisions. This was finished by end of last year. Connect systems for resource management in the ba le field. Make them interoperable.

3. Strengthen the defense against cyber threats.

On all fronts, MND wants to strengthen networks and and protect existing and new ICT-means.

Cyber Security Spark

End of 2014 and beginning of 2015, Korea went through a tough time dealing with hacking incidents. December 2014, Korea Hydro & Nuclear Power was hacked and some critical information was leaked including reactor designs and electricity flow charts. Two months later, Internet Personal Identification Number (i-PIN, an online identification number similar to the o line social security number) system was hacked and 750,000 i-PINs were issued illegally. A er these incidents, Ministry of Science, ICT and Future Planning and Korea Internet & Security Agency (KISA) are planning on establishing the Cyber Security Spark to advance the cyber security technology level in Korea. Cyber Security Spark will be a cluster where cyber security focused research institutes, educational institutes and business support center are clustered to foster global cyber security companies. The ministry is going to carry out the feasibility test from March till May 2015 to materialize the plan for the cluster.

Sources and more information:

KITRI,
h p://www.kitri.re.kr/kitri/main/main.web?

Ministry of National Defense (**MND**),
h p://www.mnd.go.kr/mbshome/mbs/mnd_eng/

Electronics and Telecommunications Research Institute (**ETRI**),
h ps://www.etri.re.kr/eng/main/main.etri

National Cyber Security Center (**NCSC**),
h p://service1.nis.go.kr/

Korea Internet & Security Agency (**KISA**),
h p://www.kisa.or.kr/eng/main.jsp

Security World,
h p://www.securityworldmag.co.kr/

Boan News,
h p://www.boannews.com/

International Security Exhibition & Conference (**SECON**),
h p://www.seconexpo.com/2015/

e-Government Infrastructure Solution Exhibition & Conference,
h p://www.egisec.org/2015/

Graduate School of Information Security, Korea University,
h p://ime.korea.ac.kr/

Cyber Terror Research Center, CTRC,
h p://www.ctrc.go.kr/eng/index.do

More information

Yewon Cha en Peter Wijlhuizen
Email: seoel@ianetwerk.nl
IA Zuid Korea

USA & Canada

Overview of the Security Sector in the United States

Introduction

This document provides general information about industry trends and developments, hot-spots and key players as well as R&D related to the following topics in the United States:

- Cyber security
- Protection of critical infrastructures
- Urban security (specifically emergency response)
- Unmanned aerial vehicles / systems (drones)
- In the second part of this document similar information is provided for Canada related to cyber security only.

The information below may not be up-to-date in all aspects and is certainly not complete or exhaustive. However, it does give a brief overview of some of the key elements of the 'security' landscape in the Unites States which is considered a dominant global player from both a policy and industry perspective, and in which the dynamics are fast moving and gaining more and more public and political a ention.

Any questions related to this document, please contact NOST in Washington D.C.
Email: nost@nost.org.
Phone: +1 202 274 2727.

Cyber security

Industry and demand

Big U.S. companies have all fallen victim to cyber-a acks. As the a acks have go en more frequent, smarter, extended in scope the a acks have received more scrutiny from the public, investor and business communities. The demand for cyber security solutions is large and growing exponentially in the US in all sectors. For example, 2013 saw a record level of investment funding and deals with $1.71 billion invested in 240 deals to emerging cybersecurity companies. The (global) cyber security market is estimated to grow from $95.6 billion in 2014 to $155.7 billion by 2019, at a CAGR of 10.3% from 2014 to 2019. Some of the biggest trends in the cyber security industry are:

- A shi from prevention to response: organizations need (governance) plans and technologies that let them rapidly detect and react to threats that the vast IT landscape has made nearly impossible to stop.
- The trend of architecting cyber resiliency: as the cost of downtime in datacenters has risen, IT systems must be designed to work under failure and under a ack. Gaining faster response time through big data and mathematical analysis is the new frontier of cybersecurity.
- Mobile technologies and an expanding Internet of Things are making everyone and everything a network gatekeeper. The burden of protecting organizational infrastructure that was once le to experts now lies in the hands of everyone.
- The Internet of Things is expected to cause a huge expansion in the market of digital forensics: when all objects are smart we will generate and leave a visible trail at every place we visit, on everything we touch, and with everything we do.

There is a huge human capital and skills shortage in the cyber security industry. Companies, universities and government entities are all focused on finding ways to overcome this shortage: educational partnerships, hackathon competitions, internal corporate training programs etc.

Various sectors of industry such as banks, telecommunications and energy companies, which have all been targeted by a acks, as well as big technology companies like Google, Microso and Yahoo are pushing for be er sharing of threat and a ack details from government. They also want to be protected from privacy lawsuits if they share information on customers, and from negligence suits for failing to act on warnings.

Hotspots and key players

There are many di erent U.S. players specializing in cyber security. A selection:

- Large security so ware vendors: McAfee, Symantec, Cisco Systems, FireEye.
- Well-funded cybersecurity startups: Good Technology, Okta, OpenPeak, Lookout, AVAST So ware, Bit9, TeleSign, Bromium, CloudFlare and LogRhythm.
- Active investors in cybersecurity startups: Intel Capital, Accel Partners, Kleiner Perkins Claufield & Byers, Sequoia Capital, Andreessen Horowitz, Greylock Partners, Bessemer Venture Partners, Lightspeed Venture Partners, Norwest Venture Partners, Google Ventures, Khosla Ventures and Venrock.
- Top acquirers in Cybersecurity: Google, McAfee, Symantec, Cisco Systems, VMware, EMC, IBM and Trustwave.

U.S. hotspots with a high concentration of cyber security related activities include the following:

- The Washington DC Metropolitan Area (DC, Maryland, Northern Virginia) is home to the nation's top defense and intelligence agencies as well as a constellation of defense contractors such as Northrop Grumman and Lockheed Martin. Maryland is home to around 1,800 cybersecurity companies and Virginia to over 300. Northern Virginia houses the most data centers in the region. In the area you also find several NSA-DHS certified centers of excellence for cybersecurity education: Bowie State University, Capitol College, Johns Hopkins, Towson University, US Naval Academy, UMBC, UMCP, UMUC.
- St. Antonio, Texas, is home to more than 80 IT and cyber-related businesses in San Antonio. Many entrepreneurs are anticipating a flood of government contracts from the new Air Force Cyber Command headquarters in town.
- In San Diego, CA, the cybersecurity industry is closely tied to the federal government with a key component being the United States Navy Space and Naval Warfare Systems Command. The region is also home to large market leaders such as ESET and Sentek Global. Total estimated annual economic impact is $1.51 billion.

R&D

There is a large and diverse landscape of R&D cyber related activities and underlying roadmaps and programs in the U.S. Here are a few highlights.

DHS Science & Technology's Cyber Security Division focuses its R&D on cyber infrastructure, user protection & education, and development of an international-level cyber research infrastructure.

The Department of Energy designed the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused R&D e ort.

The NIST does research and creates standards on a whole range of issues: Cybersecurity Framework, Cloud Computing, Smart Grid, Cyber-Physical Systems. Related to this has been the establishment of the National Cybersecurity Center of Excellence (NCCoE) that is hosted at NIST with a multiyear multibillion dollar investment form the U.S. government. The center provides businesses with real-world cybersecurity solutions—based on commercially available technologies. The center brings together experts from industry, government and academia to demonstrate integrated cybersecurity that is cost-e ective, repeatable and scalable.

Several cyber roadmaps have been published: NIST Roadmap for Improving Critical Infrastructure Cybersecurity; Cross-Sector Roadmap for Cybersecurity of Control Systems; Roadmap to Achieve Energy Delivery Systems Cybersecurity; Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise.

A er the release of the NIST framework, DHS has launched the C³ Voluntary Program, A Public-Private Partnership to Strengthen Critical Infrastructure Cybersecurity. The primary goals of the C³ Voluntary Program are to support industry in increasing cyber resilience, to increase awareness and use of the Cybersecurity Framework, and encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

A couple of public private partnerships are worth mentioning as well. A new PPP was announced between MITRE and the University System of Maryland to operate a new Cybersecurity R&D center for the National Institute of Standards and Technology (NIST), will be located in Montgomery County, MD. In San Diego CyberHive, another PPP, was established with a mission to help startup cybersecurity, big data, and predictive analytics companies be successful and grow in San Diego.

The Internet Security Alliance (ISA) was founded in 2000 in collaboration with Carnegie Mellon University. It is multi-sector trade association but also functions as think tank and has operational security programs. ISA membership is open to public and privately held entities and currently has substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries.

Policy

In both the House and Senate cybersecurity bills have been introduced most notably: Cybersecurity Information Sharing Act introduced by Senate Intelligence Commi ee Chairman Feinstein (D-Calif.) and Vice Chairman Chambliss (R-Ga.) which expands information shared about cybersecurity threats and defensive mechanisms between the government and companies and within the private sector in order to combat the rapid increase in a acks on computer systems

On the House-side, the Cyber Information Sharing Act (CISA) was passed earlier this year, which establishes equal cybersecurity partnerships between private industry and DHS. Both bills have been criticized by privacy advocates.

National Cybersecurity and Critical Infrastructure Protection Act was passed by the House, which strengthens e orts to combat cyber-a acks on critical infrastructure through the distribution of cyber threat information, the development and procurement of new technologies and support for DHS's cybersecurity workforce.

However, none of these bills has passed both Houses. In March 2015 an updated version of CISA has passed the Senate Intelligence Commi ee and will be introduced in April. Meanwhile, President Obama has issued the following Executive Orders on cyber security:

- Improving the Security of Consumer Financial Transactions (BuySecure Initiative) which calls for implementing enhanced security measures including securing credit, debit, with microchips in lieu of basic magnetic strips.
- Improving Critical Infrastructure Cybersecurity, which directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The first version NIST framework was published in February.
- Allowing the Treasury Department to impose financially punitive sanctions against cyber hackers who impose a significant threat to national security. This Order authorizes the government to impose sanctions on individuals or entities that engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Also, agencies have been established such as the National Cybersecurity and Communications Integration Center (NCCIC) that focuses on information sharing between the private sector, civilian, law enforcement, intelligence, and defense communities. Or a more recent agency, the Cyber Threat Intelligence Integration Center (CTIIC), which is focused on information sharing within the intelligence communities in the U.S.

Protection of critical infrastructures

Industry and demand

The global critical infrastructure protection market is expected to grow from $63.7 billion in 2013 to $105.9 billion in 2018 with North America expected to be the biggest market in terms of revenue contribution. In the US critical infrastructure is largely owned and operated by the private sector. However, Federal and SLTT governments also own and operate critical infrastructure, as do foreign entities and companies. The market for SCADA/ICS systems is expected to grow at an estimated CAGR of 7.24% from 2014 to 2020, reaching $11.16 billion by 2020.

The cost of improving infrastructure in the United States is significant and rising. The National Academy of Sciences reported that the Nation's earlier heavy investment in the design, construction, and operation of critical infrastructure systems—water, wastewater, energy, transportation, and telecommunications—has not been matched with the funds necessary to keep these systems in good condition or to upgrade them to meet the demands of a growing and shi ing population. The American Society for Civil Engineers estimated that the US needs to invest $2.2 trillion to meet future infrastructure needs, of which $1.1 trillion is unfunded.

The electricity infrastructure is highly automated and controlled by utilities and regional grid operators, using sophisticated energy management systems, such as SCADA, to keep the system in balance. The main threats and hazards according to DHS are cyber security, physical a acks and natural disasters. The North American Electric Reliability Corporation (NERC) has been stepping up its enforcement of enhancing the grid's cyber security. Its 2015 budget proposal includes a major new cybersecurity initiative, the Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a PPP whose aim is to facilitate timely information sharing of cyber threat information and to develop situation awareness tools that enhance the electricity sector's ability to protect its critical infrastructure.

DHS identifies natural hazards, malicious actors, and ageing infrastructure as the major threats to the dams sector. The overall number of high-hazard dams estimated at 14,000 in 2012 and the number of deficient dams is currently more than 4,000. The cost to repair these would be an estimated $21 billion. Cyber security proves also a major challenge in this sector. In 2013, U.S. intelligence agencies traced a data breach by China of a system containing U.S. Army Corps of Engineers' National Inventory of Dams (NID), which has critical information on the vulnerabilities of the roughly 8,100 major dams in the United States.

The chemical sector is an integral component of the U.S. economy, employing nearly 1 million people, and earning annual revenues between $600 and $700 billion. The three main threats of significant concern identified for this sector by DHS in 2014 are cyber-threats, insider threats and natural disasters and accidents.

Hotspots and key players

There are many di erent U.S. players specializing in the protection of critical infrastructure. A selection:

- Government: DHS, DoE, DoD, DoC, Department of the Treasury, Department of Agriculture, Department of Health and Human Services, Department of Transportation, Cross-Sector Cybersecurity Working Group, Environmental Protection Agency, NIST, FEMA, State, Local, Tribal, and Territorial Governments.
- Research facilities: Ba elle, SANDIA National Laboratories, Idaho National Laboratory, Pacific Northwest National Laboratory.
- Universities: University of Southern California Information Sciences Institute; George Mason University (VA) Center for Infrastructure Protection & Homeland Security; University of Illinois; Dartmouth; UC Davis; Washington State University.
- Advisory councils: Critical Infrastructure Partnership Advisory Council (public & private partners from all critical infrastructure sectors); Homeland

Security Advisory Council; National Infrastructure Advisory Council; National Security Telecommunications Advisory Commi ee.
- Critical Infrastructure Owners and Operators
- There are several companies that o er Critical Infrastructure Protection services such as Ericsson, Burns & McDonnell, ViaSat, SANS ICS.
- The largest US-based SCADA/DCS suppliers: Rockwell Automation, GE Intelligent Platforms, Emerson Process Management and Honeywell.

There are no clear hotspots or clusters as the infrastructure sector is vast and spread out all over the country. Naturally some of the main federal agencies are located in Washington D.C. Other key players reside in various parts of the country: Washington State, Southern California, Albuquerque (New Mexico), Idaho.

The most vulnerable regions vary with the type of threat. Coastal areas for floods and hurricanes; the Great Plains, the Midwest, the Mississippi Valley and the southern United States for Tornadoes; the chemical sector has the strongest presence in the North-East of the US; the US electric transmission grid is most concentrated in the eastern part of the country also; the main financial centers are New York, Chicago, San Francisco and Boston; and the top agricultural producing states are California, Iowa, Nebraska, Texas, Minnesota, Illinois, Kansas, Wisconsin, Indiana, and North Carolina.

R&D

There is a large and diverse landscape of R&D activities related to critical infrastructure protection and underlying roadmaps and programs in the U.S. Not to mention the work being done in light of the discussions around resiliency of critical infrastructures. Here are a few highlights that involve the Department of Homeland Security which is one of the major R&D funding agencies.

The National Infrastructure Simulation and Analysis Center (NISAC) is a modeling, simulation, and analysis program within the Department of Homeland Security (DHS). It provides strategic, multidisciplinary analyses of interdependencies and the consequences of infrastructure disruptions across all 16 critical infrastructure sectors at national, regional, and local levels.

In the DECIDE project the DHS Science & Technology Directorate, with support from the Financial Sector, is creating a tool that will enable private sector entities located within critical infrastructures to conduct collaborative, realistic, fully immersive, scenario-based exercises with response decisions made by subject ma er experts.

The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program is an ongoing collaboration of oil and natural gas companies and the DHS Science and Technology Directorate (S&T). The program undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector.

DHS S&T and the DoE jointly funded the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) e ort to address the challenge of protecting the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, reliable, and safe. University researchers and more than 35 power industry entities are participating to develop and evaluate technologies needed for realizing secure Smart Grid applications.

The DETER-Enabled Federated Testbeds (DEFT) consortium is a unique collaborative e ort by Pacific Northwest National Laboratory, University of Illinois at Urbana–Champaign, and Information Sciences Institute (ISI) to build a shared, distributed capability for experimental research on cyber-physical systems. This research capability will integrate a subset of the cyber and physical resources at the member sites with the tools necessary to explore and analyze cyber-physical systems.

Policy

They key policy document is the National Infrastructure Protection Plan (NIPP) of which the last version was published in 2013 as directed PPD-21 Critical Infrastructure Security and Resilience. The NIPP highlights that a voluntary public-private partnership approach continues to be the primary means to protect the nation's critical infrastructures.

Improving Critical Infrastructure Cybersecurity, which directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The first version NIST framework was published in February.

Urban security

Industry and demand

This section highlights some specific issues (and possible solutions) that relate to security in the U.S. urban environment, specifically those with regards to emergency response and disaster management:
- Risk-based Planning and Resourcing: As jurisdictions continue to have to figure out how to do more with less, risk-based planning and resourcing will become even more important.
- Social Media Use: Boston and New York City learned the value of a concentrated e ort to leverage social media use among citizens to inform and calm the populous during a disaster. Not everyone in emergency management is taking advantage of the opportunities social media o ers, but it's become a viable, even necessary way to communicate with the public during and a er a disaster.
- Evolving Terrorist Threats: Cybera acks are a real threat to 911 centers, emergency response centers and other resources, including law enforcement resources, not to mention, a major a ack on the power grid, water plant or similar infrastructure. Emergency managers and public safety o cials will have to increasingly discuss those possibilities and mitigating actions. So ware solutions for emergency situations have also been on the rise.
- Education: More and more, the emergency management and public safety fields will be asking for individuals

with more education. There is an ongoing debate about education versus experience but both are important in an increasingly complicated world. As emergency management grows as a profession, the knowledge of emergency managers will have to be deeper.

Hotspots and key players

There are many di erent U.S. players specializing in solutions for urban security. A selection:

- Government: DHS, FEMA, Department of Health and Human Services, Environmental Protection Agency, State and major urban area fusion centers (fusion centers) and emergency operations centers; United States Centers for Disease Control and Prevention; State, Local, Tribal, and Territorial Governments.
- Industry associations: NEMA, IAEM, DRCA, SDMI, NHMA, BCI.
- So ware/emergency notification technology: Coop Systems, xMa ers, MIR3, NogginOCA, Continuity Logic, ClearView, Everbridge, Risk Management Solutions
- Consultancy: KPMG, IBM Business Continuity and Resiliency Services, Ridge Global, RSA Archer Business Continuity Management and Operations, Co on Global Disasters Solutions, Avalution, Ripcord, Crisis Management International, Disaster Resilience Leadership Academy, Eagle Rock, Disaster Recover Institute, The Texas A&M Engineering Extension Service.
- University: Center for Hazards Assessment, Response & Technology Univ. of New Orleans; Center for Rebuilding Sustainable Communities a er Disasters (CRSCAD) U. Massachuse s Boston; Center for Resilience Design New Jersey Institute of Technology; Coastal Hazards and Adaptation Coastal Program State of New Hampshire; Disaster Research Center, University of Delaware; The George Washington University Institute for Crisis, Disaster and Risk Management; National Disaster Preparedness Training Center University of Hawaii; Natural Hazards Center Univ. Colorado at Boulder.

There are no clear hotspots or clusters in the U.S. Companies are spread throughout the country.

R&D

There is a large and diverse landscape of R&D activities related to urban security and underlying roadmaps and programs in the U.S. Here are a few highlights.

National Response Framework: is a guide to how the Nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the Nation. The last updated version was published in 2013 by DHS.

The Chemical, Biological, Radiological and Nuclear/Strategic Science and Technology Advanced Research and Development (CBRN/SST AR&D) Section awards contracts and enters into other business relationships with industry that promote the advanced research and development of medical countermeasures to prepare the Nation to respond to public health emergencies caused by the release of CBRN agents, as well as pandemic influenza and other emerging infectious diseases.

The All Hazards Consortium (AHC) is a 501c3 non-profit focused on homeland security and emergency management issues, and guided by the regional states of North Carolina, District of Columbia, Maryland, Virginia, West Virginia, Delaware, Pennsylvania, New Jersey and New York along with the urban areas (UASIs) of New York City-NY, Newark-NJ, Philadelphia-PA and the National Capital Region (Washington D.C.). The AHC has evolved into a network of thousands of stakeholders and resources to facilitate regional integration of systems and planning e orts between government and the private sector infrastructure owner/operators.
National Domestic Preparedness Consortium is charged with training the nation's first responders. The consortium is comprised of seven members, each of whom brings a di erent area of expertise in the field of emergency preparedness training. NDPC training comes at no cost to local agencies and includes courses that address the most urgent emergency preparedness needs.

The core purpose of the U.S. Dept. Health and Human Services Disaster Information Management Research Center (DIMRC) is to develop and provide access to health information resources and technology for disaster preparedness, response, and recovery. Our intent is to connect people to quality disaster health information and foster a culture of community resiliency.

Policy

Presidential Policy Directive / PPD-8: National Preparedness. This directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-a acks, pandemics, and catastrophic natural disasters. Through the development of a National Preparedness Goal; National Preparedness System; and a Strategic National Risk Assessment (SNRA).

Unmanned aerial vehicles / systems

Industry and demand

Currently, military applications dominate the UAV market with General Atomics currently holding 20.4% of the drone market, followed by Northrop Grumman's 18.9%. The budget cuts imposed on the DoD by the Bipartisan Budget Control Act of 2013 are making government contracts harder to come by. DoD procurement expenditures for UAVs have decreased from $3.9 billion in 2013 to a requested $2.4 billion for 2015.

However, commercial applications are expected to quickly ramp up over the next 10 years, particularly a er 2020. Interest in drones for commercial purposes comes from a wide range of groups including movie makers, real-estate agents, criminal-

defense lawyers and farmers. According to analysts, there is not just a bright future not just for the developers and manufacturers of unmanned aerial vehicles, however, but especially for companies developing what will be riding in those drone payloads.

The Association for Unmanned Vehicle Systems International —an Arlington, Virginia-based trade group— forecasts the industry will create 100,000 new jobs and $82 billion in economic impact in the decade a er the FAA allows drones to fly among traditional aircra .

The Small Business Association is also working to accommodate the potential for small businesses to control parts of the market by the awarding a regional innovation cluster contract to Southeastern New Mexico. This cluster will inaugurate an 85,000 square-foot innovation hub that will include 3D manufacturing and prototyping tools and co-working space/incubation for autonomous system startups.

Hotspots and key players

There are many di erent U.S. players specializing in solutions for urban security. A selection:

- Government: DoD, FAA; Unmanned Systems Caucus ("the Drone Caucus).
- Industry: Boeing (St. Louis, Missouri); General Atomics (San Diego, CA); Lockheed Martin (Bethesda, MD); Northrop Grumman (CA en VA); AeroVironment (CA); Textron Inc. (MD); General Dynamics Corporation (VA); SAIC (Washington/Viriginia).

Most of the big defense contractors who dominate the UAV market are located in the DC area and California. The recently appointed drone testing sites, however, are expected to be on the rise in the field. Most prominently: the State of Nevada (the Governor's O ce of Economic Development is o ering tax and business incentives); North Dakota; and New York State. For small business and start-ups the newly established UAV cluster in New Mexico is also a place to look out for.

R&D

In December 2014 the Federal Aviation Administration named six teams across the nation that will host the development and testing of drones to fly safely in the same skies as commercial airliners: The University of Alaska, the state of Nevada, New York's Gri ss International Airport near Utica; North Dakota Department of Commerce; Texas A&M University in Corpus Christi; and Virginia Polytechnic Institute and State University.

Policy

In 2005 the FAA issued a policy statement providing that "no person may operate a UAS in the National Airspace without specific authority." Obtaining a certificate requires a rigorous showing of how the drone system is designed and constructed, including so ware development, control, and quality-assurance procedures. For years, the FAA has issued cease-and-desist le ers to people and entities using drones domestically. Those le ers reflect the FAA's position that drones cannot be used for commercial purposes.

The FAA recently proposed new rules for drones for commercial use. The proposal would allow drones weighing up to 55 pounds to fly within sight of their remote pilots during daylight hours. The aircra must stay below 500 feet in the air and fly less than 100 mph. People flying drones would need to be at least 17 years old, pass an aeronautics test and be ve ed by the Transportation Security Administration, but a certificate wouldn't require the flight hours or medical rating of a private pilot's license.

Furthermore, in 2012, Congress enacted the FAA Modernization and Reform Act ("FMRA"). The Act requires the FAA to devise a "comprehensive plan to safely accelerate the integration of civil unmanned aircra systems into the national airspace" by September 2015.

Privacy concerns have, unsurprisingly, captured the eye of elected federal o cials. Several drone-related bills are pending in Congress. For example, the Preserving American Privacy Act would prohibit private drone operators from capturing data in "highly o ensive" ways that would violate a reasonable expectation of privacy. Similarly, the Drone Aircra Privacy and Transparency Act would require operators to submit a "data collection statement" to the FAA, delineating, among other things, what data will be collected, how the data will be used and retained, and whether the data would be sold to third parties.

Canada: cyber security

Industry and demand

Canada's companies are ill-prepared to meet modern cybersecurity challenges, according to a survey by the Ponemon Institute. Only one in four believe that they are winning the cybersecurity war, said the survey of 623 IT and security practitioners commissioned by IT services firm Scalar Decisions. Almost half of all respondents experienced an a ack in the last year that exposed sensitive information, and a third believed that a loss of intellectual property had caused a lack of competitive advantage.

The biggest barrier to cybersecurity was a lack of in-house expertise, the survey found. Security was also seen as siloed, meaning that it didn't collaborate e ectively with other parts of the business. When companies were breached, the average spent on each incident was $208,432. The biggest impact was to reputational damage and marketplace image, the research showed.

Organizations in Canada felt that cybercrimes were becoming more frequent (52 percent), and more sophisticated (73 percent). Almost one in every eight respondents felt that a acks were becoming more severe. Companies pledged to spend money on Big Data analytics for cybersecurity to help them gain broader visibility of the threat landscape, the report added. This was the area of most interest, with 47 percent of companies allocating funds to it. Network tra c surveillance and security information and event management (SIEM) were the next biggest areas of investment over the coming 12 months.

Key industry players

Company	Cybersecurity Sector	Corporate HQ
Perspecsys	Cloud Applications Security	Mississauga, Canada
CloudLink	Cloud Security & Data Encryption	Ottawa, Canada
Cyber Security Canada	Cybersecurity Services for SMBs	Toronto, Canada
WinMagic	Full-Disk Encryption Software	Mississauga, Canada
Privacy Analytics	Healthcare Data Privacy	Ottowa, Canada
Herjavec Group	Information Security Services	Toronto, Canada
Above Security	Managed Security Services Provider	Montreal, Canada
Messageware	Microsoft Exchange Security	Mississauga, Canada
NuData Security	Online Fraud Detection	Vancouver, Canada
Defence Intelligence	Real-Time Malware Protection	Ottawa, Canada
Security Compass	Software Development Security	Toronto, Canada
eSentire	Threat Detection & Prevention	Cambridge, Canada
Interset	Threat Detection & Prevention	Ottawa, Canada

Policy

Canada's Cyber Security Strategy is the Government's plan for protecting our country from these threats. The main objectives of the Strategy are to secure government systems, work with others to secure systems outside of government, and help Canadians to be safer online. Public Safety Canada is responsible for coordinating the implementation of the Strategy.

The Action Plan 2010-2015 for Canada's Cyber Security Strategy, outlines the Government of Canada's plan to implement Canada's Cyber Security Strategy.

Public Safety Canada works with provinces, territories, and the private sector to secure Canada's vital systems. The Department also works with international partners to reduce the risk to computer systems across the globe.

The Cyber Security Cooperation Program (CSCP) was developed as a means to improve the security of Canada's vital cyber systems. The program will provide $1.5M in grants and contributions over five years in support of projects that increase the resilience of Canada's vital cyber systems through strengthened partnerships with the private sector.

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public

Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital systems outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity.

CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

More information

Martijn Nuijten
Email: washington@ianetwerk.nl
IA Verenigde Staten

Brazilië

Cyber security in Brazilië

Inleiding

De security markt in Brazilië behoort tot de top 10 wereldwijd. Het bedrag van deze markt wordt geschat op meer dan € 1 miljard en is een van de sterkst groeiende markten, op jaarbasis. Naar verwachting zal deze markt de € 3 miljard overstijgen in 2020. Deze markt speelt zich af tegen een achtergrond van toenemende sociale onrust, verder aangewakkerd door de bezuinigingen op sociale programma's en kostenstijgingen in de eerste maanden van Dilma Roussef's tweede termijn als president van Brazilië. Veiligheid is een *hot topic* in Brazilië. Zo rapporteerde *Agência Brasil* in november 2014 dat geweld een kostenpost genereerde van R$ 258 miljard in 2013, wat overkomt met 5,4% van het BNP.Het merendeel van dit bedrag is toe te rekenen aan de sociale kosten van geweld en gezondheid gerelateerde onkosten – R$ 192 miljard in 2013. De totale berekening omvat ook onkosten in verband met gevangenissen en socio-educatieve factoren s (R$ 4,9 miljard) en publieke veiligheid (R$ 61,1 miljard). Al met al betekent dit een stijging van 8,65% ten opzichte van 2012. (De koers van de euro ligt rond de R$ 3,40).

Goederen en diensten in de Braziliaanse security market

De belangrijkste onderwerpen – niet uitpu end – zijn de volgende:

- elektronische beveiligings equipment (gescha e markt van €500 miljoen, kan verdrievoudigen tot 2020):
  - alarmsystemen tegen diefstal en inbraak
  - brand detectie
  - video monitoring systemen
  - systemen voor toegangscontrole
  - anti diefstal systemen
- luchthaven screening equipment
- certificering
- R&D samenwerking op het gebied van defensie en veiligheid

The Hague Security Delta

Belangrijke onderwerpen:

- Cybersecurity
- Critical infra
- Urban security
- Forensics

The Hague Security Delta, Brazilië en overige security thema's

Bovengenoemde 4 focusgebieden zijn ook belangrijke thema's in de Braziliaanse maatschappij. Daarnaast zijn er aanvullende security issues die een rol spelen in Brazilië. Onderstaand worden deze kort behandeld.

1. Cybersecurity

De noodzaak voor versterkte cyber security werd in Brazilië nog duidelijker nadat in 2013 een hacking incident had plaatsgevonden waarbij persoonlijke gegevens van verschillende politici zijn gestolen. In de Nationale Defensie Strategie hee dit onderwerp dan ook bijzondere aandacht gekregen. Zo star e het leger recent zijn *Cyber Defence Center*. Daarnaast overweegt de Federale overheid het opze en van een *National Agency for Cyber Security*, gericht op cybersecurity als geheel. Eind 2014 is bovendien een security-manifest ondertekend door vertegenwoordigers van zowel de publieke als de private sector. In november 2014 is hier een eerste conferentie over gehouden in São Paulo: h p://www.cyber-manifesto.org/wp-content/uploads/2014/06/cyber_manifesto_english.pdf

Naast bescherming tegen hackers en kwaadaardig gebruik van de cyberspace zijn belangrijke subthema's bescherming van persoonsinformatie, zorgen voor een open en veilig online bankingsysteem en een toegankelijk net.

2. Critical Infra

Mede gelet op de sociale onrust zoals hierboven aangehaald, is er toenemend bewustzijn bij de overheid dat er geïnvesteerd moet worden in de (fysieke) bescherming van kritische infrastructuur. Naar verwachting zal het budget hiertoe de komende jaren drastisch toenemen. Voorbeeld: de zusterorganisatie van TNO in Brazilië, IPT, hee TNO gevraagd samen te werken in een project gericht op het verbeteren van gevels van financiële instellingen. Daarnaast hee het leger een programma ontwikkeld - Proteger, gericht op de bescherming van strategische infrastructuur.

Van belang zijn tevens de volgende thema's:

Veiligheid van havens: is in ontwikkeling. Vermeldenswaard is een discussie platform, begeleid door een "*Port Facility Security Officer*". In het noorden van Brazilië zijn er kansen voor instellingen van toegepaste kennis & technologie, als mede voor bedrijven voor de aanleg van havens en de verbetering van de infrastructuur.

Veiligheid van luchthavens: drie agentschappen zijn verantwoordelijk voor het regelen van luchtverkeer. ANAC (National Civil Aviation Agency) monitort regelgeving voor veiligheid 'in de lucht' en controleert kwaliteit van de verleende diensten. Het legt rekenschap af aan het Ministerie van Defensie (Comando da Aeronáutica). Infraero is de publieke luchtvaart operator en hee een belangrijke coördinerende functie. Het Secretariat of Civil Aviation (SAC) is verantwoordelijk voor het beleid.

In 2016 worden opnieuw openbare aanbestedingen gedaan voor de privatisering van nationale luchthavens. Het betre de luchthavens van Florianópolis, Curitiba en Fortaleza. Ook is het de bedoeling de komende jaren 270 lokale luchthavens te moderniseren. Dit levert kansen voor de electronica bedrijven en producenten van systemen om vogels te verjagen, etc.

3. Urban security

In Brazilië kan hierbij gedacht worden aan beveiliging van grote evenementen, zoals congressen, festivals, toernooien (WK voetbal en Olympische Spelen). Het Ministerie van Justitie hee een "Special Secretariat for the Security of Large Events", SESGE opgezet. Het was verantwoordelijk voor de veiligheid van de *Confederations Cup* in 2013 en de Wereldkampioenschappen voetbal in 2014. Ook zal het verantwoordelijk zijn voor de veiligheid rond de Olympische Spelen die in 2016 in Rio de Janeiro worden gehouden. Het event Rio+20 en het bezoek van de Paus waren andere mega-activiteiten. Het initiële budget van SESGE bereikte 0,5 miljard euro. De openbare veiligheid valt onder verantwoordelijkheid van de Burgerpolitie, maar die kan worden bijgestaan door de militaire politie.

Grote veiligheidsrisico's zijn er op parkeerplaatsen in woonwijken. Vooral voor snelle kidnapping van mensen die in de auto mensen opwachten. Er wordt steevast aangeraden niet in de auto te blijven. Beveiliging tegen ontvreemding van auto's een aanhoudend probleem is ook van belang.

Camerabewaking van strategische gebouwen en plaatsen waar geregeld demonstraties plaatsvinden, naast de genoemde parkeerplaatsen en voetbalstadia kan kansen bieden voor Nederlandse fabrikanten/ toeleveranciers. Het gebruik van drones komt ook steeds meer in de aandacht.

Monitoring en in goede banen leiden van verkeersstromen wordt ook steeds belangrijker ter voorkoming van ongevallen en economische verliezen in het stedelijk verkeer.

4. Forensics

In Brazilië ligt de verantwoordelijkheid voor de forensische DNA analyse bij het Instituto Nacional de Criminalística. Dit instituut vormt onderdeel van de Diretoria Técnico-Cientifica (DITEC) van het Departamento de Polícia Federal. Dit Departement valt onder het Ministerie van Justitie.

Brazilië hee 26 staten en het Federaal District. Daarvan beschikken er 18 over een Afdeling van het Instituut op staatsniveau. Het Federale instituut in Brasília is verantwoordelijk voor de misdaden die nationale impact hebben. Moordzaken en andere zaken worden op staatsniveau behandeld. Iedere staat hee een eigen databank met DNA gegevens, die onderling kunnen worden uitgewisseld. Het is belangrijk hierbij alert te zijn om te voorkomen dat misdadigers over de grens kunnen ontsnappen. Een goede communicatie is daarvoor fundamenteel.

De instituten beschikken over 80 – 100 gekwalificeerde deskundigen. Zij beschikken over goed geoutilleerde laboratoria, met de meest moderne apparatuur en werken samen met de FBI. De opdrachten voor DNA onderzoek komen voort uit interne onderzoeken, van het instituut zelf en van het Instituto de Medicina Legal (IML), dat onderzoek doet naar doodsoorzaken en identificatie van slachto ers. De DNA databanken zijn opgezet volgens het Combined DNA Index System (CODIS) van de FBI. Op het gebied van bilaterale samenwerking zijn er met het NFI bijvoorbeeld zeker kansen. Men is in Brazilië geïnteresseerd in training en opleiding, uitwisseling van data, gezamenlijk onderzoek op forensisch gebied.

Aanvullende security issues in Brazilië:

5. Controle aan de grenzen:

- Bestrijding van drugstra c vanuit de buurlanden;
- Bestrijding van mensenhandel en kinderprostitutie;
- Tegengaan van illegale houtkap, dat vaak gebeurt via illegale grensoverschrijdingen vanuit Peru en Colombia – veelal wordt de houtkap georganiseerd door drugsbendes ook via invasie van tribale gebieden en resulterende conflicten;
- Controle op handel in beschermde diersoorten;
- Smokkel en witwasactiviteiten veelal vanuit de drievoudige grens met Argentinië en Paraguay.

Twee omvangrijke projecten zijn op dit gebied ontwikkeld door het Ministerie van Defensie. SISFRON: *land border monitoring system*. Geschat initieel totaal budget € 6 miljard. SISGAAZ: *maritime border monitoring system*. Implementatie wordt verwacht in 2017. Geschat initieel totaal budget is € 3 miljard.

6. Aanscherpen van het **early warning systeem**, voornamelijk ten aanzien van overstromingen, landverschuivingen en andere natuurlijke calamiteiten en verbetering van de hulpverlening. De Braziliaanse regering hee daartoe in 2011 het Centro Nacional de Monitoramento e Alertas de Desastres Naturais (CEMADEN) opgericht. Het investeert in waarnemingssystemen om vroegtijdig uitzonderlijke natuurlijke verschijnselen op te sporen. Er is al een samenwerkingsverband met Deltares bijvoorbeeld.

7. Verbeteren van de **verkeerssituatie**. Het aantal verkeersdoden in Brazilië ligt rond de 40.000 per jaar en vormt nog altijd een punt van grote zorg. Urban mobility en communicatie systemen kunnen hierbij een grote rol spelen.

8. Laag percentage van opgeloste misdaden en geringe pakkans. Bij de jaarlijks 50.000 gepleegde moorden wordt in slechts 5 - 8% een dader gevonden. De Burgerpolitie (Polícia Civil) is in eerste instantie verantwoordelijk voor het onderzoek van misdaden. Zij wordt daarin bijgestaan door een technisch instituut voor deskundig onderzoek (Politec), de Militaire Politie, het Medisch Legaal Instituut (IML), Instituto Nacional de Criminalística, en overige instituten op Federaal en Staatsniveau. Samenwerking en communicatie zijn vatbaar voor verbetering.

Bronnen (niet uitpu end)

- SESGE (Special Secretary for Security at Big Events – Ministry of Justice) h p://sesge.mj.gov.br/
- ABESE (Brazilian Association of Suppliers of Electronic Security Systems) h p://www.abese.org.br/
- Ministry of Justice h p://www.justica.gov.br/
- Ministry of Defence h p://www.defesa.gov.br/
- Harbour Security h p://www.segurancaportuariaemfoco.com.br/
- Cyber Manifest h p://www.cyber-manifesto.org/wp-content/uploads/2014/06/cyber_manifesto_english.pdf
- Artikel uit opinieweekblad Veja over Veiligheidsproblemen in Brazilë;
- Bezoek aan Policia Federal door IA Brasília: Braziliaans Forensisch Instituut (Instituto Nacional Criminalística).

Met dank aan TNO voor de bijdrage aan dit document.

Meer informatie

Hans Dorresteijn
Email: brasilia@ianetwerk.nl
IA Brazilië

1. Deze gegevens zijn a omstig van de achtste editie van de Anuário Brasileiro de Segurança Pública, opgesteld door de niet-gouvernementele organisatie Fórum Brasileiro de Segurança Pública (FBSP).

Colofon

Dit is een publicatie van:
RVO.nl

Bezoekadres
Prinses Beatrixlaan 2
2595 AL Den Haag
T (088) 602 15 04
E ianetwerk@rvo.nl
www.ianetwerk.nl
Postadres
Postbus 93144
2509 AC Den Haag

ISSN: 1572-6045

RVO.nl is een agentschap van het Ministerie van Economische Zaken. RVO.nl voert beleid uit voor diverse overheden als het gaat om duurzaamheid, innovatie en internationaal. RVO.nl is hét aanspreekpunt voor bedrijven, kennisinstellingen en overheden. Voor meer informatie en advies, financiering, netwerken en wet- en regelgeving.

IA Netwerk

Berichten over internationale R&D en technologische ontwikkelingen worden samengesteld door de Innovatie Attachés (IA's), verbonden aan de Nederlandse ambassades in de Verenigde Staten (incl. Canada), Japan, Korea, Taiwan, India, Singapore (incl. Maleisië), China, Duitsland (incl Zwitserland), EU (Brussel), Frankrijk, Turkije, Israël, Rusland en Brazilië. IA publicatie is een uitgave van RVO.nl. Ook kunt u Innovatie Attaché Netwerk vinden op Twitter: @ianetwerk of via Linkedin: https://nl.linkedin.com/in/ianetwerk

Overname van artikelen

Overname van (delen van) artikelen is toegestaan met bronvermelding. Stuur of mail u afdruk van de overname aan IA-thuisbasis.

Illustraties, tabellen en weblinks

De kwaliteit van illustraties, tabellen en weblinks kan bij het publiceren in themapublicaties niet altijd voldoende gewaarborgd worden. Daarom treft u in plaats daarvan een verwijzing naar onze website, www.ianetwerk.nl. Verwijzingen naar weblinks kunt u terugvinden onder het artikel of nieuws item van de betreffende post.

Meer informatie

Heeft u vragen, stel uw vraag aan de IA post in uw regio. Verderop vindt u de adressen. Stel uw vraag per mail, bij voorkeur via de website:www.ianetwerk.nl. Geef ook aan in welk kader en met welk doel u zoekt. U kunt uw vraag ook richten aan de IA-thuisbasis in Den Haag. Deze stuurt de vraag door naar de betreffende IA-post(en).

Eindredactie

Kris Kras Design

Ontwerp

Tigges, strategie, concept, ontwerp, Rijswijk

Drukwerk en verzending

Xerox/OBT, OBT is partner van Xerox voor de Rijksoverheid

NOST Central o ce - Netherlands
Headoffice of the Netherlands Office for Science & Technology
P.O. Box 93144 | 2509 AC The Hague
Bart Sa ier, Hans Bosch, Roy Paulissen, Lies Timorason, Wiwik Khohonggiem
P +31 (0)88 602 5021
E ianetwerk@rvo.nl
www.ianetwerk.nl (Dutch only)

NOST China
NOST Beijing 7 hrs later
Embassy of the Kingdom of the Netherlands
4, Liangmahe Nanlu, Beijing 100600, China
Taake Manning, Qing Ma, Maurits van Dijk
P +86-10-853 20259
E peking@ianetwerk.nl

NOST Shanghai
Consulaat-generaal Sjanghai
10/F East Tower, Dawning Center, 500 Hongbaoshi Road, Shanghai 201103, China
Sam Linsen, Anouk van der Steen
P +86-21 2208-7223
E shanghai@nost.org.cn
E shanghai@ianetwerk.nl

NOST Guangzhou
Consulaat-generaal Guangzhou
Teem Tower, 34 floor, 208 Tianhe Road, Guangzhou 510620, China
Jingmin Kan
P +86-20-3813-2228
E guangzhou@nost.org.cn
E guangzhou@ianetwerk.nl

NOST Germany
Botschaft des Königreichs der Niederlande
Büro für Wissenschaft und Technologie
Klosterstrasse 50, D-10179 Berlin
Eelco van der Eijk, Joop Gilijamse, Kristin Freyer
P +49 30 20956219
E berlijn@ianetwerk.nl

NOST EU
First Embassy Secretary
Research and Atomic Questions Division
Permanent Representation of the Netherlands to the EU Kortenberglaan 4-10, 1040 Brussels
Dave Pieters
P +32-2-679 1665
E brussel@ianetwerk.nl

NOST France
Ambassade du Royaume des Pays-Bas
Service pour la Science et la Technologie
7 Rue Eblé
F-75007, Paris, France
Eric van Kooij, Joanne e Polo-Leemreis, Pieternel van Oers
P +33 1 40 62 33 33
E parijs@ianetwerk.nl

NOST Turkey
Embassy of the Kingdom of the Netherlands
Turan Güneş Bulvarı | Hollanda Caddesi No. 5
06550 Yıldız, Ankara , Turkey
Rory Nuijens
P +90 312 409 1819
M +90 530 844 2810
E ankara@ianetwerk.nl

NOST India 3.30 hrs later
NOST New-Delhi
Embassy of the Kingdom of the Netherlands
Department for Science & Technology
6/50-F, Shantipath, Chnakyapuri,
New Delhi- 110 021, India
Jelle Nijdam, Vikas Kohli, Akanksha Sharma
P +91 11 24197625
E delhi@ianetwerk.nl

NOST Mumbai
Netherlands Office for Science and Technology
Consulate General of the Kingdom of The Netherlands
Forbes Building, 1st fl., Charanjit Rai Marg, Fort
Mumbai - 400 001.
Freek Jan Frerichs
P +91 22 221 942 10
E fjf@nost-india.org
E mumbai@ianetwerk.nl

NOST Japan 7 hrs later
Embassy of the Kingdom of the Netherlands
Office for Science and Technology
3-6-3 Shibakoen
Minato-ku, Tokio 105-0011
JanHein Chrissto els, Rob Stroeks, Kikuo Hayakawa, Mihoko Ishii
P +81 3 5776 5510
E tokio@ianetwerk.nl

NOST Singapore 6 hrs later
Embassy of the Kingdom of the Netherlands
Office for Science and Technology
541 Orchard Road, 13-01
Liat Towers Singapore 238881
Susan van Boxtel, Sean Tan, Anne Marie Schrijver
P +65 67 39 11 11
E singapore@ianetwerk.nl

NOST USA
NOST Washington 6 hrs earlier
Embassy of the Kingdom of the Netherlands
Office for Science & Technology
4200 Linnean Avenue N.W.
Washington DC 20008-3896, USA
Roger Kleinenberg, Martijn Nuijten Jantienne van der Meij-Kranendonk, Gerda Camara
P +1 202 274 27 27
E washington@ianetwerk.nl

NOST Boston 6 hrs earlier
Consulate of the Kingdom of the Netherlands
20 Park Plaza | Suite 524 | Boston MA 02116, USA
Walter de Wit
P +1 617 426 9224
M +1 202 615 7168
E walter@nost-boston.org

NOST San Francisco 9 hrs earlier
Netherlands Office for Science and Technology
1 Montgomery Street, Suite 3100
San Francisco, CA 94104, USA
Robert Thijssen, John van den Heuvel, Natasha Chatlein
P +1 415 2912080
E sanfrancisco@ianetwerk.nl

NOST South Korea 7 hrs later
Embassy of the Kingdom of the Netherlands
Netherlands Office of Science and Technology
10F Jeongdong Building
15-5 Jeong-dong, Jung-gu
Seoul, 100-784, South-Korea
Peter Wijlhuizen Yewon Cha
P +82 2 311 8600
E seoul@ianetwerk.nl

NOST Israel 1 hr later
Embassy of the Kingdom of the Netherlands
Office for Science and Technology
Beit Oz, 13e verdieping
14 Abba Hillel Street / Ramat Gan 52506
P.O. Box 1967 / Ramat Gan 52118, Tel Aviv
Marc Nellen
P +972 (3) 75 40 744
P +972 (0)3 7540 777 (direct)
E israel@ianetwerk.nl

NOST Russia 2 hrs later
Embassy of the Kingdom of the Netherlands
Netherlands Office for Science and Technology
Kalashny pereulok 6 | 115127 | Moscow | Russian Federation, Russia
Pauline Döll
P +7 495 797 29 69
M +7 915 348 08 99
E moskou@ianetwerk.nl

NOST Taiwan 6 hrs later
Netherlands Trade & Investment Office
Netherlands Office for Science & Technology
13F-2, 1 Songgao Road
Xinyi District
Taipei-11073 (Farglory Financial Center)
Kasper Nossent, Cha-Hsuan Liu
P +886 2 875 87200
E Taiwan@ianetwerk.nl
E kaspernossent@ntio.org.tw

NOST Brazil 5 hrs earlier
NOST São Paulo
Consulate General of the Kingdom of the Netherlands
Netherlands Office for Science & Technology
Avenida Brigadeiro Faria Lima, 1779 - 3. Floor
Jardin Paulistano
01452-001 São Paulo SP
Nico Schie eka e, Lucienne Vaartjes
P +55 (0) 11 - 3811 3307
E saopaulo@ianetwerk.nl

NOST Brasilia
Embassy of the Kingdom of the Netherlands
Netherlands Office for Science, Technology
SES - Quadra 801, Lote 05
70405-900 Brasília – DF
Brazil
Hans Dorresteijn
P +55 61 3961 3236
E brasilia@ianetwerk.nl


Singapore
Canada
Nederland
Frankrijk
Duitsland
Taiwan
Canada
Zuid-Korea
Israel
India
Frankrijk
Singapore
Frankrijk
Europese
Unie
Verenigde
Duitsland
Taiwan
India
China
Japan