SLAGKRACHT IS NODIG OM NEDERLAND TE BESCHERMEN **EN ECONOMISCHE KANSEN** VOOR CYBERSECURITY TE **VERZILVEREN**

Digitale bedrijvigheid zorgde de afgelopen 25 jaar voor ruim een derde van alle economische groei.[1] Meer dan 5 procent van ons bnp verdienen we met ICT. Nederland heeft een toppositie in de wereld als het gaat om de digitale economie. Maar het is niet vanzelfsprekend dat we die behouden. Volgens *Harvard Business Review* behoort Nederland zelfs tot de categorie 'rapidly receding'.[2] We bevinden ons nog wel in de kopgroep, maar zakken snel af.

Nederland moet meer gaan investeren om het tij te keren. Een belangrijk onderdeel daarvan is een investering in kennis van cybersecurity. En wel om meerdere redenen. Een digitaal weerbaar Nederland is belangrijk om een goed vestigingsklimaat te bieden, maar zeker zo belangrijk is dat cybersecurity een groeiende markt is voor het Nederlandse bedrijfsleven. Door de sterke focus op bestaande kennis en buitenlandse technologie laten we veel economische kansen liggen.

Landen om ons heen investeren flink in een hoger cybersecurityniveau ter bescherming van maatschappelijke continuïteit, hun bedrijfsleven en economie. Nederland blijft achter. Ons land is zich bewust van digitale dreigingen en zet daarop in, maar anders dan bijvoorbeeld in het Verenigd Koninkrijk is de Nederlandse strategie te weinig gericht op de economische kant: ons vestigingsklimaat en kansen voor het bedrijfsleven.

TRENDS

We worden links en rechts ingehaald. Zonder doorontwikkeling van cybersecurity als dwarsdoorsnijdend vraagstuk komt de Nederlandse bedrijvigheid en daarmee onze digitale samenleving, economie en vestigingsklimaat onder druk te staan.[3] De volgende trends zijn zichtbaar:

- Cybersecurity is een kat-en-muisspel. Het kennisniveau van de hackers- en malware-community is hoog en stijgende. Hierdoor neemt de concrete dreiging naar overheden en bedrijven toe.
- Het Openbaar Ministerie verwacht dat de helft van zijn zaken over vijf jaar te maken heeft met digitale criminaliteit.[4]
- Investeringen in cybersecurity van overheden en bedrijven nemen toe, zowel in eigen personeel als inhuur van diensten en technologie om zichzelf beter te beschermen.
- Die technologie is vooral afkomstig van de grote buitenlandse leveranciers, waarbij zij wordt aangeboden als 'black box'.
- Het bedrijfsleven, zeker de 'high end'-gebruiker, heeft steeds meer behoefte aan inzicht in de werking van die 'black boxes'. Standaardoplossingen voldoen verder lang niet altijd voor 'high end'-omgevingen, maar het aanbod richt zich op de grote gemene deler.
- TNO en ook de andere kennisinstellingen en universiteiten hebben technologieën in huis die een weg naar de markt zouden moeten vinden, maar dat gebeurt te weinig. Het ontbreekt aan innovatiedrang in het bedrijfsleven, lijkt het. En waar meerdere eindgebruikers tot een kansrijke oplossing komen, ontbreekt in het Nederlandse cybersecurityecosysteem ook een neutrale partij die kan zorgen voor verdere productontwikkeling, verkoop en eerstelijns-support.
- Anders dan de drie grote banken in een gedeeld onderzoeksprogramma met TNO doen, werken individuele bedrijven en industrietakken nog onvoldoende samen om zich te beschermen tegen digitale aanvallen.

Deze ontwikkelingen stemmen tot nadenken, maar bieden geweldige economische kansen voor de gouden driehoek van overheid, bedrijfsleven en kenniswereld. Met elkaar kunnen we de potentie van de BV Nederland volledig benutten, een stevige impuls geven aan de digitale economie, een einde maken aan de neerwaartse spiraal en onze toppositie in de wereld terugveroveren.

CIJFERS

Cybersecurity is zowel in Nederland als wereldwijd een groeimarkt. Cijfers bekrachten dit. [5, 6]

- Nederland importeert relatief veel ICT-hardware en -diensten (50 miljard euro, waarvan 88% hardware en 12% diensten) en exporteert relatief weinig. De ICT-markt in Nederland zelf bedraagt rond de 70 miljard euro.
- Nederland verdient zo'n 4,5% van het bnp (rond de 30 miljard euro) aan ICT. Dit is vergelijkbaar met de landen om ons heen. Voor landen waar hardware wordt geproduceerd, geldt echter een hoger percentage.
- De markt voor cybersecurity in Nederland bedraagt 'tussen de 0,9 en 1,8 miljard euro'.[7]
- De markt voor cybersecuritysoftware was in Nederland in 2015 411 miljoen euro.[8]
- In 2010 droegen cybersecuritybedrijven met ongeveer 0,4% bij aan het Nederlandse bnp. In 2014 steeg dit percentage tot ongeveer 0,6%.
- In de periode 2010–2014 namen de omzet en toegevoegde waarde van cybersecurity in de ICT-sector jaarlijks met 14,5% toe. Voor cybersecurity verwachten ICT-bedrijven een jaarlijkse omzetgroei van ongeveer 7%.

KANSRIJKE KENNISGEBIEDEN

De Nederlandse kennisbasis voor cybersecurity is op delen heel erg goed. Universiteiten en TNO spelen internationaal een vooraanstaande rol in onder meer de detectie van geavanceerde cyberaanvallen, anomalie detectie, crypto, 'secure multi party computation' en 'blockchain security'. Ons land heeft alles in zich om cybersecurityuitdagingen en daarmee samenhangende maatschappelijke en economische kansen te pakken.

Relevant voor Nederland is post-kwantumencryptie en op langere termijn toepassing van kwantumcomputing op encryptie

Inhoudelijk gezien heeft Nederland een goede uitgangspositie om economische kansen voor cybersecurity te verzilveren. Mede op basis van onderzoek van VKA/SEO zien we als sterke punten:

- Verregaande digitalisering zorgt voor relatief sterke bedrijven in de cybersecuritysector.
- Goede reputatie van Nederland.
- Politiek neutrale wet- en regelgeving en toezicht op ICT en internet.
- Goede publiek-private samenwerking. Organiseren, inrichten van processen en samenwerken zijn internationaal gezien kerncompetenties van ons land. Op vrijwel elk land lopen we voor.
- Goed informaticaonderzoek en -onderwijs bij universiteiten, kennisinstituten, hbo en opkomend mbo.
- Ligging, cultuur en ondernemersklimaat: 'Digital Gateway to Europe'.

Opkomende kennisgebieden zijn bijvoorbeeld:

- Technologie voor detectie van geavanceerde cyberaanvallen.
- 'Beyond awareness': toepasbaar maken van fundamentele inzichten uit psychologie en sociologie om mensen zich digitaal veiliger te laten gedragen.
- Technologie voor cybercapaciteiten van Politie en Defensie.

Verder leiden technologische en maatschappelijke ontwikkelingen tot interessante kennisgebieden voor cybersecurityinstrumenten:

- Qua samengestelde jaarlijkse groei is de cybersecuritymarkt voor internet of things de grootste met 33%.
- Ook smart cities, smart mobility en e-health kunnen niet veilig worden uitgerold zonder bijbehorende cybersecurityconcepten en -technologie.
- Dit geldt ook voor de introductie van nieuwe betaalmethoden, waaronder op 'blockchain' gebaseerde technologie.
- Relevant voor Nederland is post-kwantumencryptie en op langere termijn toepassing van kwantumcomputing op encryptie.
- Groot achterstallig onderhoud op de cybersecurity van legacy-systemen biedt ook kansen, zeker in specialistische industriële omgevingen.

4½
PROCENT van het bnp verdiend aan ICT

DRIETRAPSRAKET

Met onze stakeholders en partners willen we de valorisatieketen voor cybersecurity stevig verbeteren. Samen creëren we maatschappelijke waarde, en vergroten we tegelijk de economische waarde van fundamenteel en toegepast wetenschappelijk onderzoek. Als drietrapsraket geven we een positieve impuls aan de concurrentiepositie: borg fundamenteel onderzoek, schep een sterker cyberecosysteem en organiseer een 'technology transfer'.

FUNDAMENTEEL ONDERZOEK EN EEN STEVIGE KENNISBASIS

Fundamenteel onderzoek en een stevige kennisbasis zijn randvoorwaarden voor een langdurige en sterke internationale concurrentiepositie. Alleen dan kunnen we antwoord geven op de cybersecurity- vraagstukken van de toekomst.
Ontwikkelingen in kwantumtechnologie, digitale transactiemethodes zoals 'blockchain', de exponentiële groei in het gebruik van sensoren en grote demografische veranderingen vereisen nieuwe inzichten en antwoorden op nog onbekende vragen.

Innovatieve concurrentiekracht vraagt ook om investering in voortgezet onderwijs: van een betere aansluiting tussen mbo, hbo en universiteiten tot een Cyber Security Academie, en van de bouw van testfaciliteiten tot investering in kansrijke kennisgebieden.

CYBERECOSYSTEEM

De Nederlandse cybersecurityindustrie is maar zeer beperkt gericht op innovatie: het ontwikkelen en vercommercialiseren van exporteerbare producten en diensten. In ons land ligt de nadruk sterk op dienstverlening. Daarbij worden veelal securityproducten en -diensten van buitenlandse leveranciers gebruikt. De afhankelijkheid van buitenlandse veiligheidsoplossingen én achterstand in concurrentiepositie ten opzichte van de internationale markt groeien.
Zonder sterk ecosysteem komt het koppelen van kennisvraag en kennisaanbod moeilijk tot stand. In landen met een succesvolle cybersecurityindustrie—denk aan de Verenigde Staten, het Verenigd Koninkrijk, Frankrijk en Israël—bundelen bedrijven, kennisinstellingen en overheid al jaren de krachten in langdurige onderzoeksprogramma's. Het bereiken van zo'n concurrerend ecosysteem vraagt een cultuuromslag bij het bedrijfsleven, maar ook kennisinstellingen én de overheid hebben een substantiële verantwoordelijkheid. Prof. Mariana Mazzucato weerlegde namelijk de mythe dat de overheid passief is en kan blijven in innovatie. Ze laat zien dat juist de overheid de belangrijkste stimulator is, óók ten opzichte van innovatief bekendstaande bedrijven zoals Apple en Google.
In Nederland is wel een cyberecosysteem aanwezig, maar de samenhang is niet goed geborgd. Zo is de aansluiting van universiteiten en TO2-instituten[9] op de Nederlandse cybersecurityindustrie minder ontwikkeld. Vaak bestaat wel een relatie met eindgebruikers zoals overheden, banken en telecom- en energiebedrijven, maar minder met de partijen die cybersecurityproducten en -diensten in de markt kunnen zetten.

'TECHNOLOGY TRANSFER FACILITY'

Het belangrijkste ingrediënt om de 'valley of death' tussen onderzoek en markt sneller en vaker te overbruggen, is een goed gestructureerd en georganiseerd proces van 'technology transfer'. We richten ons daarbij primair op de fase waarin toegepaste kennis—bijvoorbeeld in de vorm van 'demonstrators of prototypes'—de gang naar de markt moet maken, maar nu onvoldoende voedingsbodem vindt. Er is een incentive nodig, zodat cybersecuritybedrijven specialisten willen vrijmaken voor innovatie. AI is er op korte termijn ook omzet in de markt te behalen met bestaande kennis.

Een doelstelling die behaald moet worden, is het beter overbruggen van de fase waarin kennis uit fundamenteel onderzoek verder moet rijpen richting toepassing, maar waar nu potentieel veelbelovende resultaten verloren dreigen te gaan. Denk bijvoorbeeld aan DNS Ninja (anomalie detectie), CTI Capability Framework (welke 'capabilities' moet je ontwikkelen om goed met cyber threat intelligence om te gaan en daar maximaal rendement uit te halen) en 'targeted attack detection'.

Financieren van het 'durven te falen' is belangrijk om kennis die ook op lange termijn de concurrentiekracht versterkt, een weg naar de markt te laten vinden. Met een 'technology transfer facility' zorgen we ervoor dat kennisinstellingen en cybersecuritybedrijven de noodzakelijke ruimte krijgen om te experimenteren.

Ontwikkelingen in kwantumtechnologie, digitale transactiemethodes zoals 'blockchain', de exponentiële groei in het gebruik van sensoren en grote demografische veranderingen vereisen nieuwe inzichten en antwoorden op nog onbekende vragen

FINANCIËLE IMPULS

De ICT-markt in Nederland bedraagt rond de 70 miljard euro. Cybersecurityuitgaven zou 10% van dat budget moeten bedragen.[10] Daarnaast zouden we de komende 5 jaar moeten inzetten op een betekenisvolle impuls van 140 miljoen euro per jaar om de achterstand in te lopen. Om die 140 miljoen goed in te zetten, zijn focus, massa en samenwerking nodig. De huidige beschikbare middelen schieten tekort om dit te bereiken.

De cybersecurityuitgaven moeten blijven groeien. Herna Verhagen, CEO PostNL, stelt terecht dat minimaal 10% van het ICT-budget van organisaties aan cybersecurity moet worden uitgeven. Maar er moet geld bij. Willen we de boot niet missen, dan is de extra impuls van 140 miljoen—de ordegrootte van de extra uitgaven in het Verenigd Koninkrijk, dat als open handelsland met een hoge mate van digitalisering veel met Nederland gemeen heeft—eerder noodzaak dan luxe.

Het is wel goed om te beseffen dat cybersecurity om meer dan ICT gaat. Denk aan opleiding en training, onderwijs, governance, processen, onderzoek en ontwikkeling. Bovendien is ICT steeds meer verweven met fysieke systemen zoals een auto of smart-tv.

De huidige beschikbare middelen schieten tekort om de gewenste impuls te geven:
- Topsector HTSM (circa 2 miljoen euro per jaar).
- Nationale Cybersecurity Strategie en de daaruit voortvloeiende Nationale Cyber Security Research Agenda (twee calls tot dusverre, totaal circa 11 miljoen).[11]
- Overige investeringen van de overheid in cybersecurityonderzoek (ordegrootte enkele miljoenen per jaar).
- De investeringen in eigen cybersecurity. Deze zouden naar de ondergrens van 10% van het ICT-budget moeten gaan.[12]

De extra impuls van 140 miljoen moet zich richten op de stimulering van economische kansen. Denk aan:
- Investeren in voortgezet onderwijs, verbeteren van de aansluiting mbo-hbo-universiteiten, Cyber Security Academie.
- Investeren in onderzoek in kansrijke kennisgebieden en bijbehorende testfaciliteiten.
- Specifieke, omvangrijke investeringsprogramma's uitvoeren om cybersecurity en cybercapaciteiten van de overheid en Defensie te vergroten.
- Vraag en aanbod koppelen, technologie scouten, een goede aansluiting organiseren van universiteiten en kennisinstellingen op de Nederlandse cybersecurityindustrie.
- Financieren van 'durven te falen', innovatie stimuleren bij bedrijfsleven, creëren van experimenteerruimte, transfer mogelijk maken van kennis en technologie naar producten en diensten.
- Participeren in internationaal fundamenteel en toegepast onderzoek op kansrijke niches (bijvoorbeeld via EU), faciliteren van kennisbruggen met landen met een vergelijkbare agenda zoals Singapore—dat niet alleen de veiligste, maar ook de beste van de wereld wil worden—en EDA en NAVO-lidstaten, 'cyber capacity building' (internationale samenwerking buiten de EU).

Met de financiële impuls kunnen we als Nederland de volgende economische kansen verzilveren:
- Sterke verbetering van de transfer van interessante cybersecuritykennis naar het bedrijfsleven en vertaling naar exporteerbare producten en diensten.
- Werkgelegenheid in de cybersecuritysector.
- Groei van het aantal gekwalificeerde cybersecuritymedewerkers.
- Scheppen van een interessant vestigingsklimaat voor hightechbedrijven.
- Versterking van onze digitale veiligheid en specifiek mogelijk maken van veilige adoptie van innovaties, zoals internet of things, smart cities, smart mobility en 'new payment methods'.
- Meer onafhankelijkheid voor en eigen kennis van cybersecuritycapaciteiten in het veiligheidsdomein, inclusief Defensie.

Financieren van het 'durven te falen' is belangrijk om kennis die ook op lange termijn de concurrentiekracht versterkt, een weg naar de markt te laten vinden

KAMPIOEN **SAMENWERKEN**

Nederland is kampioen samenwerken. Dat doen we op allerlei manieren. Zo zijn er al een Nationale Cybersecurity Strategie, een Cyber Security Raad, een Nationaal Cyber Security Centrum, dcypher, The Hague Security Delta, Defence Innovation Greenhouse i.o. en een Nationale Cyber Security Research Agenda. We beginnen dus niet vanaf nul, maar maken een vliegende start als we de lopende initiatieven beter op elkaar aansluiten en intensiveren.

Digitale weerbaarheid en veiligheid zijn belangrijke voorwaarden om een koppositie als digitale economie te behouden. Met cybersecuritykennis die is ontwikkeld bij de technische universiteiten, technische hogescholen en TO2-instellingen kunnen nieuwe producten en diensten worden ontwikkeld, om daarmee de concurrentiepositie van bedrijven te versterken. Dit gebeurt niet zomaar. De overheid heeft hier ook een rol in.

Er moet een ministeriële stuurgroep, een functionaris of zelfs een minister worden benoemd die een meerjarig cybersecurityactieprogramma opstelt. In samenwerking met het bedrijfsleven en lagere overheden kan die stuurgroep of functionaris ambities, bevoegdheden en geld samenbrengen. Met als resultaat één kennis- en investeringsagenda die cybersecurity structureel verbetert, zowel voor wat betreft veiligheid als economie. Het is belangrijk na te denken op welke cybersleuteltechnologie we als Nederland willen inzetten. Alleen door de vele bestaande en soms versnipperde initiatieven te stroomlijnen en de krachten te bundelen, komen we als land weer vooruit.

Als het gaat om de veiligheidskant van cybersecurity heeft de Nederlandse overheid al veel bereikt op het gebied van coördinatie, ondanks verspreide bevoegdheden en competenties. Internationaal gezien doen we het zeker niet slecht, ook niet als het gaat om publiek-private samenwerking. De economische kant is tot nu toe echter onderbelicht gebleven in deze coördinatie, wat consequenties heeft voor onze veiligheid op langere termijn.

Cybersecurity is een wereldwijd issue, en Nederland uiteindelijk maar een kleine speler. Het is daarom belangrijk dat de Nederlandse overheid zeer actief haar economische beleidsprioriteiten voor cyber security agendeert bij de Europese Unie en andere internationale fora, om in groter verband te kunnen optreden. Meerdere ministeries spelen hierin een rol: Defensie, Economische Zaken, Buitenlandse Zaken en Veiligheid en Justitie. Dat vraagt om een scherpe, afgestemde agenda.

7
PROCENT
omzetgroei
in cybersecurity

Alleen door de vele bestaande en soms versnipperde initiatieven te stroomlijnen en de krachten te bundelen komen we als land weer vooruit

DE ROL VAN **TNO**

TNO werkt samen. Met klanten en partners, publiek en privaat, nationaal én internationaal. Samenwerking vraagt om ecosystemen die dit faciliteren en stimuleren. De organisatie verbindt en brengt de juiste mensen en partijen bij elkaar, waar ook ter wereld, en katalyseert innovaties. Door allianties te vormen, ontstaan de beste oplossingen voor morgen. Deze manier van werken, naast een integrale aanpak, vergroot de impact.

TNO zet Nederland op de internationale cyberkaart en zorgt dat Nederlandse cyberexperts en onze kennis de meeste gewilde ter wereld worden. De organisatie is vanuit haar bestaansrecht onafhankelijk. Diepgaande kennis van het speelveld en de behoefte om uit te blinken daagt de professionals uit om hun prestaties te verbeteren. Zij zien grote maatschappelijke problemen en cybervraagstukken nog voordat iemand anders ze ziet en anticiperen hierop. Ze agenderen nieuwe onderwerpen en komen met ambitieuze oplossingen die wérken.

Binnen The Hague Security Delta werkt TNO samen met partners in het Cyber Threat Intel Lab, het Nationaal Cyber Testbed waar gewerkt wordt aan de digitale veiligheid van toepassingen voor Internet of Things en het IoT Forensics Lab. In het Shared Research Program (SRP) Cybersecurity richt TNO zich samen met de banken onder andere op anomalie detectie. Ook heeft TNO in het SRP Cybersecurity een CTI Capability framework ontwikkeld om organisaties te helpen zich klaar te maken voor effectief gebruik van cyber threat intel om cyberweerbaar te worden.

Internationaal heeft TNO een strategisch partnerschap met Interpol IGCI afgesloten in Singapore waar onder andere wordt samen gewerkt rond training op het gebied van Darkweb. TNO is tevens betrokken in twee Europese H2020 trajecten waarin methoden en technieken worden ontwikkeld om politie- en opsporingsdiensten meer hulpmiddelen te bieden om verdergaand onderzoek op Darkweb te kunnen doen, bijvoorbeeld het ontsluiten en analyseren van gesloten fora en de-anonimiseren van criminelen. Ook ontwikkelt TNO kennis over de economie van criminaliteit op het Darkweb en de mogelijkheden om deze te verstoren.

TNO richt zich daarnaast in verschillende onderzoeksprogramma's op unieke technologieën en cybervraagstukken als publiek-private samenwerking op het gebied van informatie-uitwisseling t.b.v. nationale cybersecurity, post-quantum crypto en andere vernieuwing op crypto, blockchain security, ketenweerbaarheid, human factor in cyber, cybersecurity van wapensystemen, capacity building, innovatieve fraude bij nieuwe betaalmethoden en veilige hard- en software.

TNO Cyber Security & Resilience ziet de economische en maatschappelijke kansen van digitalisering, en heeft tegelijkertijd het risico en de dreigingen scherp in het vizier. De professionals maken het mogelijk de kansen die cyber biedt, te verzilveren – nu en in de toekomst. Ze agenderen de juiste vraagstukken, gaan voor diepgaand, integraal onderzoek en bieden innovatieve oplossingen voor het cyberrisico.

TNO maakt onze samenleving en economie weerbaarder, veiliger en succesvoller onder het motto 'We make cyber work for you'.

70

MILJARD euro ICT-markt in NL

AUTEUR

Annemarie Zielstra
Directeur Cyber Security & Resilience
annemarie.zielstra@tno.nl

REFERENTIES

1. Cybersecurityraad, De economische en maatschappelijke noodzaak van meer cybersecurity, Nederland digitaal droge voeten, 2016 ('Rapport Verhagen')
2. Tuft University, Digital Evolution Index, 2014, zie: https://hbr.org/2016/03/how-benchmarking-can-help-countries-become-more-digital, en de achterliggende bron: http://etcher.tufts.edu/eBiz/
3. Zie ook de Beleidsreactie Cyber Security Beeld Nederland 2016, Kamerstukken II 2015/16, 34 388, nr. 2
4. Rapport Verhagen
5. VKA/SEO, Economische kansen Nederlandse Cybersecurity-sector, 2016, https://www.vka.nl/actueel/nieuws/rapport-vka-economische-kansen-nederlandse-cybersecurity-sector
6. The Hague Security Delta (HSD), TNO, Metropoolregio Rotterdam Den Haag, Verkenning van Nut, Noodzaak en Haalbaarheid van een Nationaal Cybertestbed, 2017
7. HSD, 2017
8. www.ictmarktmonitor.nl/ict-marktmonitor-2015/software/#2
9. Kennisinstellingen voor toegepast wetenschappelijk onderzoek: TNO, NLR, Deltares, ECN, Marin en WUR/DLO; in het geval van cybersecurity zijn dat met name TNO en NLR
10. Rapport Verhagen
11. Ministerie van Veiligheid en Justitie, Beleidsreactie Cyber Security Beeld Nederland 2015, 14 oktober 2015
12. http://agconnect.nl/artikel/wat-kost-it-de-overheid-eigenlijk

TNO innovation for life

TNO.NL