TNO-rapport

TNO 2019 R11079

Een kwalitatieve analyse van cybersecurity onderzoek door TNO

Eindrapportage

Datum	9 oktober 2019
Auteur(s)	Frank Fransen, Martijn Neef, Annemarie Zielstra (TNO)
Exemplaarnummer	
Oplage	
Aantal pagina's	38 (incl. bijlagen)
Aantal bijlagen	
Opdrachtgever	
Projectnaam	
Projectnummer	060.40113

Inhoudsopgave

1 Inleiding ... 3
1.1 Aanleiding ... 3
1.2 Doel ... 4
1.3 Scope ... 4
1.4 Context van het onderzoek ... 5
1.5 Aanpak en bronnen ... 5
1.6 Kader ... 5
1.6.1 Missie en strategisch plan ... 6
1.6.2 Verantwoording bronnen ... 7

2 Zelfevaluatie: cybersecurity-onderzoek door TNO ... 8
2.1 Focus & massa ... 8
2.1.1 Organisatie van het cybersecurity portfolio ... 8
2.1.2 Units en Researchgroepen ... 9
2.1.3 Inhoudelijke speerpunten (PMC's) ... 11
2.1.4 Belangrijkste financieringsinstrumenten ... 13
2.1.5 Volume in omzet ... 15
2.1.6 Profielen expertisegroepen ... 15
2.1.7 Kennispositie waarderingen expertisegroepen ... 16
2.1.8 Patenten ... 17
2.1.9 Klanttevredenheid waarderingen expertisegroepen ... 17
2.2 Marktgericht en adaptief ... 18
2.2.1 Afstemmingsmechanismen ... 18
2.2.2 Ontwikkelingen in aard projecten portfolio ... 18
2.3 Continue ontwikkeling ... 19
2.4 Intensivering van de samenwerking ... 19
2.4.1 Positie TNO als TO2 instituut ... 19
2.4.2 Ministeries ... 19
2.4.3 Topsectoren ... 20
2.4.4 Cybersecurity bedrijven ... 21
2.4.5 Andere bedrijven (eindgebruikers) ... 21
2.5 Internationalisering ... 22
2.5.1 Aantal internationale onderzoeksprojecten ... 22
2.6 Onderzoeksfaciliteiten van wereldklasse ... 24
2.7 Huis voor talent ... 24
2.8 Technology transfer ... 25
2.8.1 Aantal spin-outs met TNO cybersecurity technologie ... 25
2.9 Impact ... 25
2.9.1 Ingebruikname TNO-technologie ... 27
2.9.2 Doorontwikkeling van kennisopbouw naar technologieontwikkeling ... 28

3 Wat gaat goed en wat kan beter? ... 29

4 Conclusies ... 30
4.1 Positie TNO ... 30
4.2 Sturen op het geïmplementeerd krijgen van innovaties en samenwerking ... 30
4.3 Tot slot ... 31
Bijlage(n)
Bijlage 1: Voorbeelden impact

1 Inleiding

De groeiende complexiteit van cyberaanvallen en grote impact op het bedrijfsleven en de maatschappij vragen om een gedegen aanpak om de cyberweerbaarheid te vergroten. TNO doet dit door samen te werken met het bedrijfsleven, de overheid en de wetenschap. Door onderzoek vanuit een breed perspectief uit te voeren waarbij technologie, organisatorische en menselijke factoren van cybersecurity worden meegenomen. Binnen TNO zijn ruim 110 experts actief op het terrein van cybersecurity-onderzoek.

Als onafhankelijke onderzoeksinstelling heeft TNO - zonder specifiek de belangen van een bepaalde doelgroep te vertegenwoordigen - een positie tussen wetenschappelijke instellingen, overheid en bedrijfsleven (zowel afnemers als aanbieders van cybersecurity-technologie/-oplossingen).

1.1 Aanleiding

De afgelopen twee jaar is er door de ministeries op het gebied van cybersecurity (Defensie, Justitie en Veiligheid, Onderwijs Cultuur en Wetenschap en Economische Zaken en Klimaat), NWO en TNO intensief samengewerkt rond de Maatschappelijke Uitdaging Veilige Samenleving (MUVS) en specifiek op het onderwerp Cybersecurity. Intussen zijn ook externe verkenners in opdracht van het ministerie van Economische zaken en Klimaat (EZK) aan de slag geweest om tot een gezamenlijke analyse van aandachtspunten te komen voor de verbetering van de publiek-private programmering van cybersecurity-onderzoek (fundamenteel en toegepast) én mogelijke bundeling van financiering op het terrein van cybersecurity.

Daarnaast is in het kader van de vernieuwing topsectorenbeleid gestart met de ontwikkeling van een missiegedreven aanpak, waarbij cybersecurity één van de onderwerpen is binnen de missie Veiligheid.

Een belangrijke doelstelling van deze aanpak is dat de innovatieketen op het terrein van cybersecurity versterkt gaat worden. Dit moet in 2019 leiden tot een gezamenlijke Kennis en Innovatieagenda (KIA) en daaruit voortvloeiend Kennis- en Innovatiecontract (KIC) op het terrein van Cybersecurity. Uitgangspunt is dat, gegeven de beperkte schaal van Nederland, er keuzes gemaakt moeten worden op welke onderwerpen Nederland onderzoek wil uitvoeren binnen het cybersecurity-domein.

Ter verdere onderbouwing van te maken keuzes heeft het ministerie van EZK, zowel NWO als TNO gevraagd een kwantitatieve en kwalitatieve analyse uit te voeren om tot een goed beeld te komen van de kennispositie op het gebied van cybersecurity en de wijze waarop er met cybersecurity-onderzoek wordt omgegaan.

De kwantitatieve analyse is uitgevoerd door het Centrum voor Wetenschaps- en Technologie Studies van de Universiteit Leiden (CWTS).
De kwalitatieve analyses van NWO en TNO alsook de kwantitatieve analyse van het CWTS en NWO leveren tezamen een overall analyse op van de kennispositie op Cybersecurity van Nederland.

1.2 Doel

De opdracht voor de gezamenlijke door NWO en TNO uit te voeren analyse is als volgt geformuleerd (in de context van een breder onderzoek naar de Nederlandse excellentie op het cybersecurity-onderzoeksveld):

> *"Evalueer de opbrengst van deze onderzoeksactiviteiten in kwalitatieve zin. (…) Geef een kwalitatief (…) beeld over bijvoorbeeld internationale waardering van onderzoeksresultaten, ingeschatte noodzaak tot versterking van de (inter)nationale positie van het vakgebied en relevantie van het onderzoek. Betrek in de analyse zowel, alpha, bèta als gamma georiënteerd onderzoek als wel het onderzoek in internationaal samenwerkingsverband."*

1.3 Scope

De onderhavige kwalitatieve analyse hierna te noemen zelfevaluatie richt zich op het toegepast wetenschappelijk onderzoek van TNO op cybersecuritygebied, waarbij zowel mens, technologie als organisatie en beleid in beeld zijn. Er wordt gekeken naar cybersecurity-onderzoek voor alle soorten opdrachtgevers (publiek-privaat, civiel-militair, nationaal-internationaal). De periode 2015 tot heden is in scope.

Als werkdefinitie voor cybersecurity houden we de definitie aan die CBS voor de Cybersecuritymonitor hanteert. Deze definitie dekt de breedte van het onderwerp goed af, en omvat zowel de onderwerpen cyber operations, cyber crime als cyber resilience. Deze gaat uit van de ideale situatie omschreven door NCSC (NCSC, 2016):

> *"(h)et vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (NCSC, 2016)*[1]*" Uitgaan van deze ideale situatie, definieert CBS-cybersecurity als alle maatregelen die bijdragen aan het bereiken daarvan. CBS voegt daaraan het volgende toe: "cybersecurity – of eigenlijk het ontbreken ervan – omvat echter ook het tekortschieten van deze maatregelen of het ontbreken van maatregelen. Deze laatste twee situaties kunnen zich manifesteren in de vorm van incidenten."*[2]

[1] Nationaal Cyber Security Centrum, Cyber Security Beeld Nederland CSBN 2016. September 2016.
[2] idem

CBS Definitie – uitleg:

> *"Bij cybersecurity ligt de focus op de ICT-systemen zelf: het beschermen van de ICT-systemen en de daarin opgeslagen informatie tegen misbruik. In tegenstelling tot cybercrime gaat het hier vooral over de te treffen maatregelen om misbruik tegen te gaan en de kans op onbedoelde incidenten te verkleinen. Dit zijn deels ICT-**technische** maatregelen, zoals firewalls (...). Deels zijn dit ICT-**organisatorische** maatregelen, bijvoorbeeld de doorlooptijd van het repareren van kwetsbaarheden in de software. (...) Ten slotte zijn dit ook maatregelen die erop gericht zijn om burgers en werknemers van bedrijven en organisaties **alerter te maken op misbruik**, zoals het vergroten van de kennis en de bewustwording op het terrein van cybersecurity en het aanreiken van makkelijk te implementeren maatregelen of gedragingen."*[3]

1.4 Context van het onderzoek

Dit onderzoek c.q. zelfevaluatie vindt plaats in de context van het versterken van de innovatieketen op het gebied van cybersecurity in brede zin.

Onderdeel van dit onderzoek is een kwantitatieve analyse die separaat door CWTS wordt uitgevoerd, en een kwalitatieve en kwantitatieve analyse die door NWO wordt uitgevoerd.

Voor de kwalitatieve analyse van TNO wordt gekeken naar de beschikbare expertise binnen de researchgroepen die zich bezighouden met cybersecurity. De researchgroepen geven samen met de cybersecties uit de Units ICT en Defensie en Veiligheid van TNO het technologieportfolio van TNO op het gebied van cybersecurity vorm.

1.5 Aanpak en bronnen

Deze zelfevaluatie is tot stand gekomen door bestuderen van de Kennis- positie Audits (KPA's) uit 2017 van de diverse researchgroepen, de Mid-Term Reviews (MTR's) uit 2019 van de researchgroepen die zich met cybersecurity bezighouden, Klanttevredenheid Audits (KTA's) van relevante projecten, het Strategisch Plan 2018-2021 van TNO, cybersecurity gerelateerde documenten, de financiële boekhouding van TNO (SAP) en gesprekken met TNO-collega's uit Expertise, Units en staven.

1.6 Kader

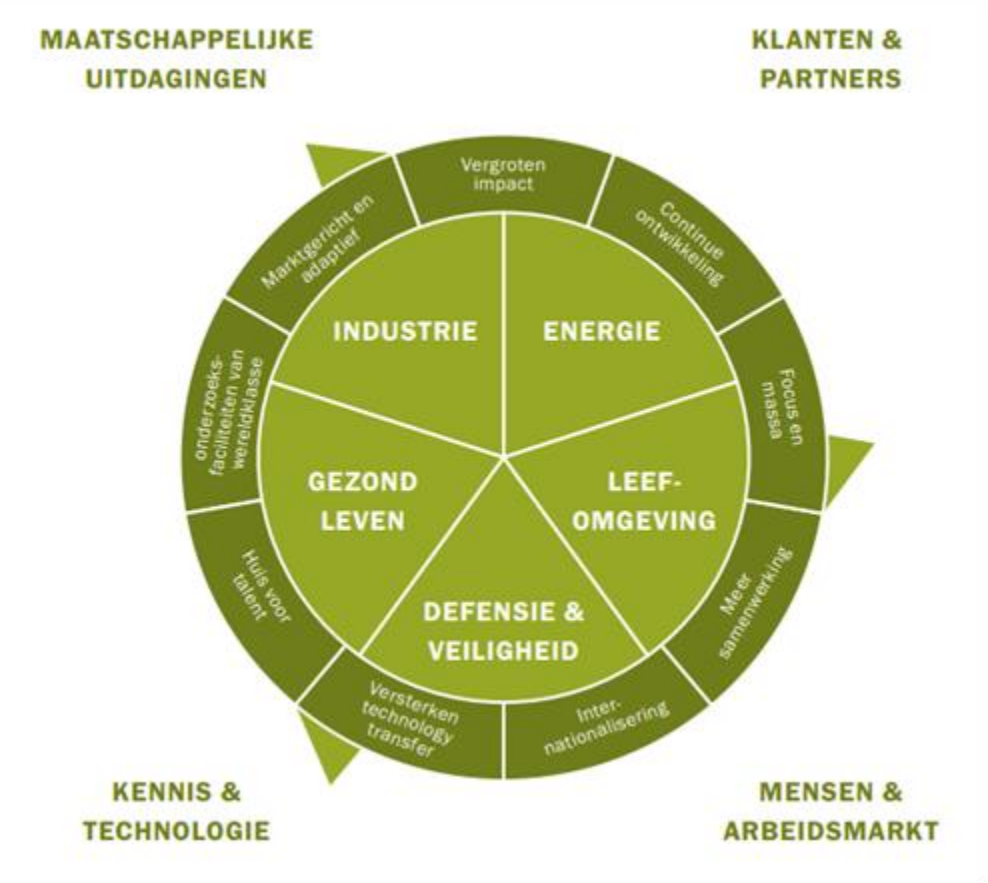
Voor de zelfevaluatie is een kader (9 ontwikkelgebieden) gebruikt dat gebaseerd is op de missie van TNO in combinatie met het TNO Strategisch Plan 2018-2021, 'Vliegwiel voor Innovatie'.

[3] https://www.cbs.nl/-/media/_pdf/2018/38/csm2018_web.pdf

1.6.1 Missie en strategisch plan

De Missietekst van TNO luidt als volgt:

> *"Innovation for Life. TNO verbindt mensen en kennis om innovaties te creëren die de concurrentiekracht van bedrijven en het welzijn van de samenleving duurzaam versterken."*



Figuur 1: Het 'vliegwiel voor innovatie' uit het Strategisch Plan 2018-2021, met in de buitencirkel de ontwikkelspeerpunten

Deze missie geeft aan wat TNO wil betekenen voor de maatschappij. Het strategisch plan geeft aan hoe TNO zichzelf over de volle breedte moet ontwikkelen om de missie te realiseren. In het strategisch plan wordt de missie vertaald naar 9 actielijnen:

1. Focus & massa
2. Marktgericht en adaptief
3. Continue ontwikkeling
4. Meer samenwerking
5. Internationalisering
6. Onderzoeksfaciliteiten van wereldklasse
7. Huis voor talent
8. Technology transfer
9. Vergroten impact

De missie en het strategisch plan vormen óók de meetlat voor het onderzoek dat TNO uitvoert op het gebied van cybersecurity. Dit kan afwijken van de meetlat die universiteiten en Hbo-instellingen zichzelf opleggen voor hun onderzoek.
Over het algemeen is het onderzoek van TNO toegepast onderzoek.

1.6.2 Verantwoording bronnen

Er is geen aparte Kennis Positie Audit (KPA) specifiek voor cybersecurity-onderzoek binnen TNO. KPA's worden uitgevoerd op het niveau van een expertisegroep/afdeling. Aangezien zowel vorming als uitvoering van het cybersecurity onderzoek verspreid is over verschillende expertisegroepen is ten behoeve van dit onderzoek voor cybersecurity een beeld gevormd door uit verschillende afdelings KPA's en andere aanvullende bronnen data te combineren, in de meeste gevallen handmatig.

2 Zelfevaluatie: cybersecurity-onderzoek door TNO

TNO doet al meer dan 35 jaar onderzoek naar cybersecurity. Cybersecurity is een veranderlijk begrip, en relatief nieuw als overkoepelend begrip. TNO doet al vanaf de eerste manifestaties van digitale systemen onderzoek naar informatiebeveiliging, systeembeveiliging, cryptografie, kwetsbaarheids- en afhankelijkheidsanalyses. TNO heeft daarin een belangrijke rol gespeeld voor Defensie, op gebied van maatschappelijke veiligheid door het agenderen van Kwetsbaarheid Internet (KWINT), door het uitvoeren van maatschappelijk relevante security analyses van ICT-systemen (bijv. OV-chipkaart en Rijkspas), is medeoprichter van het privacy & identity lab (PI.lab[4]) en was de oorsprong van security bedrijf Brightsight (het sinds 1984 grootste onafhankelijke security evaluatie lab in de wereld[5]. In deze periode werd cybersecurity geschaard onder het begrip security management en had het onderzoek een meer beleidsmatig karakter. Sinds 2011 wordt onder topteam ICT ook veel steviger ingezet op de technologieontwikkeling en valorisatie t.b.v. meerdere sectoren en domeinen. Ook in de KIA Sleutel technologieën worden hier substantieel middelen aan toegekend. Vanaf 2015 heeft cybersecurity als begrip zich sterk ontwikkeld zowel binnen als buiten TNO.

Hoewel (mono-)disciplinair cybersecurity-onderzoek noodzakelijk blijft (bijv. op gebied van cryptografie), neemt de vraag en noodzaak om een multi- en interdisciplinaire aanpak van cybersecurity vraagstukken toe om de complexe ‘wicked problems’ en maatschappelijke uitdagingen van cybersecurity succesvol aan te pakken. Binnen TNO wordt onderzoek op het gebied van cybersecurity daarom doorgaans multidisciplinair opgepakt. De vraagstukken op cybersecurity komen steeds vaker te liggen op combinaties van Techniek, Organisatie, Processen, Governance en de Mens. Dientengevolge is een versterking van de samenwerking tussen verschillende researchgroepen binnen TNO zichtbaar die elk hun eigen expertise inbrengen in de multidisciplinaire projecten.

In dit hoofdstuk wordt de huidige stand van zaken beschreven langs de negen ontwikkelgebieden uit het Strategisch Plan 2018-2021.

2.1 Focus & massa

2.1.1 Organisatie van het cybersecurity portfolio

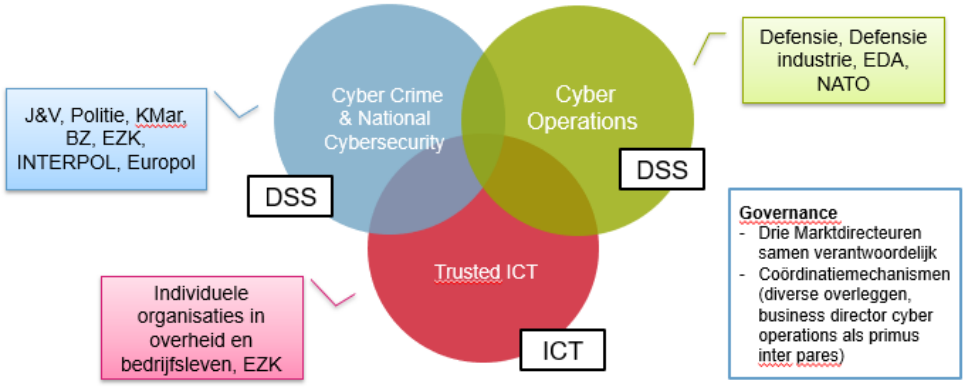
In de periode 2015 t/m 2017 werd TNO als matrix organisatie bestuurd en het cybersecurity-onderzoek vormgegeven vanuit een overkoepelende roadmap[6] ‘Cyber Security & Resilience’ aangestuurd.

Deze roadmap kende drie programmalijnen: Cyber Operations, Cyber Crime en Cyber Resilience. Vanuit deze roadmap werden onderzoeksprioriteiten vastgesteld en de verbinding gelegd met nationale- en industriële innovatie-agenda’s.

Vanaf 2018 is TNO overgestapt op een unit structuur en zijn deze drie programmalijnen verdeeld over twee units ten einde beter in staat te zijn de

[4] www.pilab.nl
[5] www.brightsight.com
[6] Roadmap: de LT innovaties die TNO in de markt wil realiseren worden in roadmaps beschreven binnen TNO

verschillende klantgroepen met verschillende wensen en uitdagingen te bedienen: *Cyber Operations* en *Cyber Crime & National Security* bij de Unit Defensie en Veiligheid; *Trusted ICT* bij de Unit ICT. De namen van de programmalijnen zijn tevens aangepast naar aanleiding van de introductie van de Product-Markt-Combinaties in 2018 (PMC's, zie ook 2.1.2).

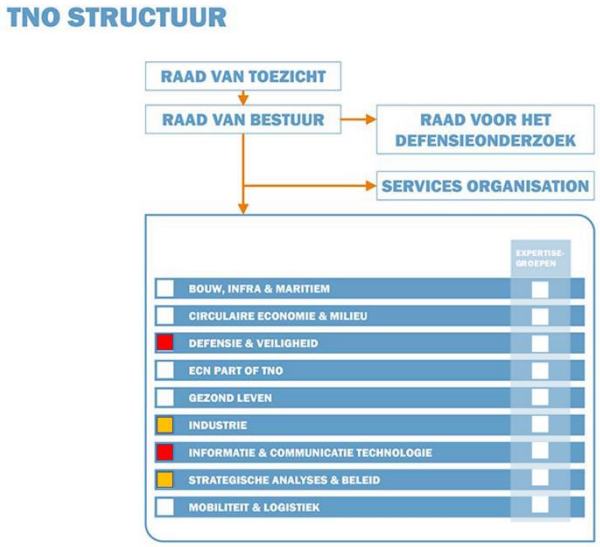


Figuur 2: actuele indeling en governance van het cybersecurity portfolio

Met ingang van de nieuwe strategieperiode (2018-2021) ligt de dagelijkse aansturing in cybersecurity-onderzoek zoals hierboven aangegeven bij drie programmalijnen in de twee genoemde Units. Binnen de programmalijnen zorgen product-markt combinaties voor structuur en verbinding in het portfolio.

2.1.2 Units en Researchgroepen

TNO heeft diverse disciplines in huis en is daardoor uitstekend gepositioneerd om de vaak complexe cybersecurity-vraagstukken goed te kunnen beantwoorden. Relevante cybersecurity expertise ligt binnen TNO verdeeld over meerdere researchgroepen, en omvat het hele spectrum tussen mens, proces techniek, governance en beleid. Bij de ontwikkeling en toepassing van technische concepten wordt rekening gehouden met de context waarin deze worden toegepast, de wensen en mogelijkheden van de gebruikers, de aansluiting met de processen en cultuur van de organisatie en politiek-bestuurlijke agenda's.
TNO is georganiseerd in negen Units. Elke Unit is opgebouwd uit researchgroepen. De units Defensie en Veiligheid, Informatie & Communicatie Technologie, Industrie en Strategische Analyses & Beleid (zie figuur 4) houden zich bezig met cybersecurity- onderzoek binnen hun researchgroepen. TNO beschikt in totaal, over alle researchgroepen heen, over een pool van ruim 110 experts die zich bezighouden met cybersecurity-vraagstukken.



Hieronder worden de belangrijkste researchgroepen voor cybersecurity uitgelicht en aangegeven aan welke pijlers van de Nationale Cyber Security Research Agenda (NCSRA III[7]) ze een bijdrage leveren.

Figuur 3: De units Defensie en Veiligheid, Informatie & Communicatie Technologie, Industrie en Strategische Analyses & Beleid houden zich bezig met cybersecurity- onderzoek binnen hun researchgroepen.

Researchgroepen die een belangrijke bijdrage aan cybersecurity leveren zijn:

Cyber Security and Robustness (CSR, unit ICT) is een technische kerngroep in cybersecurity research voor TNO. De groep heeft diepgaande kennis van informatiebeveiligingsonderwerpen als risico assessment en management, cryptografie, netwerkbeveiliging, systeembeveiliging, identity en access management, digitale aanvalstechnieken, anomalie detectie, quantum, algoritmes en wiskundig modeleren van de robuustheid van netwerken en systemen. Onderzoeksonderwerpen waaraan CSR werkt zijn: Security Monitoring & Detection, Automated Security en Transaction Security (o.a. blockchain security, self-sovereign identity management, secure multiparty computation en post-quantum crypto). De expertise van CSR is veelal technisch van aard, en bevindt zich vooral in de *Design, Defence* en *Attack* pijlers van de NCSRA III.

Networked Organisations (NO, unit Defensie en Veiligheid) richt zich met name op onderzoek- en innovatietrajecten op het gebied van cybersecurity beleid- en strategie, informatie-uitwisseling, dreigingsanalyse en doet onderzoek naar cybercrime en Darkweb. NO zet haar kennis van vitale infrastructuren, ISACs, crisisbeheersing en ketenafhankelijkheden in om het veranderende cybersecurity landschap te duiden, en draagt bij aan de *Design* en *Governance* pijler van de NCSRA III.

Data Science (DS, unit ICT) brengt haar data analyse- en architectuurkennis in het cybersecurity domein door cybercrime (Darkweb) analyses, secure data sharing architecturen en privacy-beschermings-technieken. De kennisbasis van DS ligt met

[7] TNO is mede-auteur van de NCSRA III

name in Artificial Intelligence, machine learning, pattern recognition, Natural Language Processing, text mining, semantiek en interoperabiliteit. De recente focus van DS ligt op (A) Responsible Data Science (B) Interoperable Data Science, en (C) Explainable Data Science. De expertise van de groep Data Science bevindt zich met name op de *Design, Defence en Privacy* pijlers van de NCSRA III.

Electronic Defence (ED, unit Defensie en Veiligheid) werkt nauw samen met het Ministerie van Defensie op innovatie van het gebied van CEMA (Cyber and Electromagnetic Activities): elektronische signaal disruptie en beïnvloeding. De expertise van deze groep ligt in de *Attack* pijler van de NCSRA III.

Human & Organisational Innovations (HOI, unit Defensie en Veiligheid) heeft diepe kennis van menselijk en organisatie gedrag en past deze toe in het cyberdomein door onderzoek te doen naar menselijk handelen in het digitale domein, en het opbouwen aan tactieken die bijdragen cyber-veilig gedrag. De expertise van de groep HOI bevindt zich voornamelijk op de *Design* pijler van de NCSRA III.

Daarnaast leveren de volgende researchgroepen ook een inhoudelijk bijdrage aan cybersecurityvraagstukken:

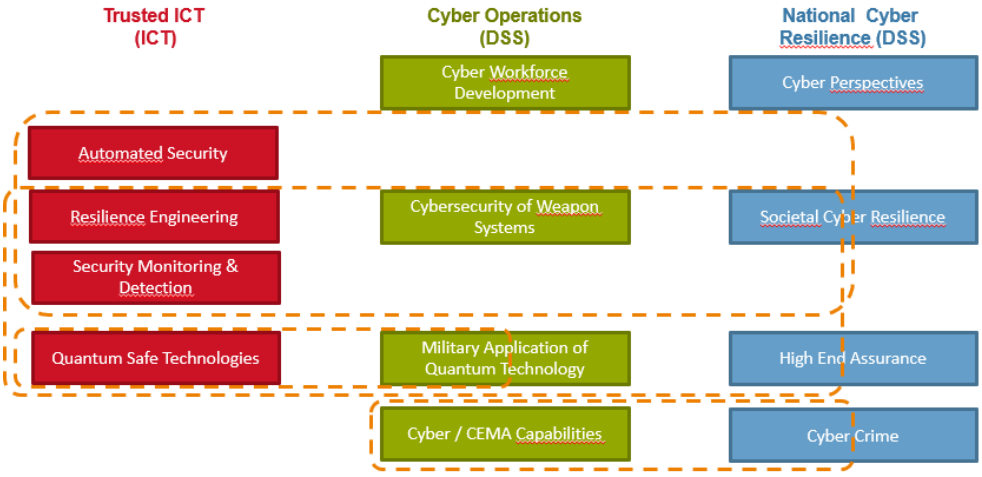
- Unit Defensie en Veiligheid: Military Operations (MO), Perceptual & Cognitive Systems (PCS), Modeling, Simulation & Gaming (MSG), Training & Performance Innovations (TPI)
- Unit Strategy & Policy: Strategy & Policy (S&P)
- Unit Industrie: Quantum Technology (QT)

2.1.3 Inhoudelijke speerpunten (PMC's)

TNO richt zich vanuit haar eigen rol en positie als toegepast wetenschappelijk kennisinstituut op die cybersecurity-technologieën die bijdragen aan een digitaal weerbare samenleving en aan de concurrentiekracht van de Nederlandse cybersecurity-industrie.

In 2018 heeft TNO besloten om 'portfolio management' te introduceren op basis van Product-Markt Combinaties (PMCs). De PMCs op het gebied van cybersecurity bepalen de belangrijkste speerpunten en roadmaps voor het cybersecurity-onderzoek binnen TNO. Ze zijn richtinggevend voor de besteding van middelen voor kennisopbouw en sturen de doorontwikkeling naar technologie. Bij grote voorkeur zijn de PMC's afgestemd op de behoeften van de belangrijkste

opdrachtgevers, hoewel dat niet in alle gevallen volledig mogelijk is (bijvoorbeeld in de sterk gedifferentieerde markt van de Unit ICT).



Figuur 3: Overzicht van actuele PMC's. De oranje stippellijnen geven aan welke PMC's inhoudelijk samenhangen, over de Markten heen.

Hieronder wordt een korte toelichting op de cybersecurity PMC's gegeven:

Unit ICT – PMC cluster ICT: Trusted ICT

- Resilience Engineering: richt zich op ontwerpmethodieken en concepten voor het realiseren van veilige en weerbare systemen.
- Monitoring & Detection: richt zich op het ontwikkelen van tools en technieken voor monitoring en detectie van geavanceerde cybersecurity gerelateerde aanvallen en fraude.
- Automated Security: richt zich op het ontwikkelen van technologie en tools voor (semi) geautomatiseerd redeneren en reageren op cybersecurity dreigingen en aanvallen.
- Quantum Safe Technology: richt zich op kennis en toepassing van post-quantum cryptografie en Quantum Key Distribution (QKD).

Unit Defensie en Veiligheid, PMC cluster Information & Sensor Systems: Cyber Operations

- Cyber & CEMA Capabilities: richt zich op het ontwikkelen van technologie voor ondersteuning van Cyber/CEMA-capaciteiten van de krijgsmacht.
- Cyber Security of Weapon Systems: richt zich op het versterken van de digitale weerbaarheid van wapensystemen (o.a. risicomanagement en ontwerp/architectuur, monitoring & detectie, automated security).
- Cyber Workforce Development: richt zich op het bereiken van voldoende gekwalificeerd cyberpersoneel middels een integrale benadering, voor de taken die moeten worden verricht vanuit ambities en verplichtingen. O.a. cybercompetenties, veilig gedrag, cyber manning & automation, enz.
- Military Application of Quantum Technologie: richt zich op het verkennen van militaire toepassingen op het gebied van quantum computing en quantum communications technologie.

Unit Defense, Safety and Security – PMC cluster National Security: National Cyber Resilience

- Maatschappelijke Digitale Weerbaarheid: richt zich op het versterken van de maatschappelijke weerbaarheid tegen nieuwe dreigingen en persistente bestaande digitale dreigingen inclusief nieuwe technologie en samenwerkingsmogelijkheden.
- Bestrijden Cybercrime en Gedigitaliseerde Criminaliteit: richt zich op het ontwikkelen van tools en methoden om het actuele beeld van cybercrime fenomenen te kunnen volgen, de effectiviteit van interventies te meten en te ondersteunen en hiermee het handelingsperspectief te vergroten.
- Foresight & Horizon scanning: richt zich op het ontwikkelen van een Horizon scanning toolbox, met bron-scanners en analyse tools.
- High End Assurance: richt zich op het bevorderen van digitale soevereiniteit op cybersecuritytechnologie voor het hoog gerubriceerde domein (b.v. (quantum safe) crypto).

2.1.4 Belangrijkste financieringsinstrumenten

Binnen TNO wordt een veelheid aan verschillende financieringsinstrumenten ingezet voor verschillende vormen van onderzoek. Onderstaande tabel geeft een indruk van de verscheidenheid aan financieringsinstrumenten die in de verschillende markten gebruik wordt gemaakt.

Financieringsinstrumenten: kennisopbouw en- toepassing		
Defensie (DSS)	Nationale Veiligheid (DSS)	Private markt (ICT)
Risico Verkennend Onderzoek (RVO), Doelfinancierings-programma Defensie en additionele financiering (contractresearch), Defensie Technologie Projecten, nationaal en internationaal (NTP, ITP). EDA operational budget, Preparatory Action for Defense Research.	Early Research Programme, Vraaggestuurd Progamma Veilige Maatschappij/Cyber, Vraaggestuurd Programma HTSM Security, Aanvullende Rijksbijdrage, contractresearch, EU-projecten (o.a. H2020), EC-tenders	Early Research Programme, Vraaggestuurd Programma ICT, Vraaggestuurd Programma HTSM Security, Shared Research Programma (SRP) Cybersecurity met de banken, TKI, Aanvullende Rijksbijdrage, contractresearch, EU-projecten (o.a. H2020, ITEA), NWA-routes, NWO- calls, Technology Transfer, EC- tenders

De sturing van de kennisopbouw en valorisatie vindt doorgaans tenminste twee keer per jaar plaats via verschillende programma's. Deze programma's kunnen publiek gefinancierd zijn, publiek-privaat of geheel privaat. Afhankelijk van de aard van de financiering vindt bijsturing plaats met private partijen, via topteams (zoals HTSM), waarin het ministerie van economische zaken, industrie en kennisinstellingen afvaardiging hebben, ofwel direct via departementen afgestemd.

Binnen het cybersecurity onderzoek binnen TNO zijn onderstaande programma's de grootste:

VP Cyber (roadmap Security, HTSM): Het Vraaggestuurd Programma Cyber Risk Management & System Resilience draagt bij aan een weerbare samenleving met innovatieprojecten op vijf cruciale thema's:

- Security and Resilience Concepts
- Security Monitoring & Detection
- Automated Security
- Transaction Security
- Secure Behavior & Cyber Safe Culture

Binnen deze thema's wordt er gekeken naar zowel de technologische uitdagingen, als ook bijbehorende beleids-, gedrags- en cultuurvraagstukken, met het doel om bij te dragen aan de capaciteitsopbouw van de Nederlandse overheid en bedrijfsleven - op strategisch, tactisch en operationeel niveau - in de vorm van visies, advies, analyses en technische prototypes.

VP VM / Cybersecurity & Societal Resilience: Het VP VM/Cyber betreft een meerjarige samenwerking met het NCSC langs de onderzoekslijnen:

- Automated Security (NDN, CTI)
- Anomalie Detectie
- IoT
- ICS/SCADA
- Next Gen ISACs
- C-level Communication
- Incentives for cybersecurity

Programmering 'Kennisopbouw Politie': Kortgezegd KOP heeft als voornaamste doel om de politie proactief te laten inspelen op nieuwe technologieën en maatschappelijke ontwikkelingen. Activiteiten binnen het programma richten zich op: 'Inrichten van een gestructureerde kennisbasis ten behoeve van innovatie voor de politie', 'Starten van meerjarige kennisopbouw programma's met uitwerking op de korte, middellange en lange termijn', 'Inrichten van een innovatie-ecosysteem (samenwerkingsmodel) voor de politie, bestaande uit kennisinstituten, wetenschappelijke instellingen, bedrijven en overheid'.

In 2018 zijn binnen de programmering 'Kennisopbouw Politie' zes programma's gestart: Programma Kompas, Gestructureerde kennisbasis t.b.v. innovatie, Politiewerk in het cyberdomein, Operationele slagkracht (in specifieke zin versterken van het informatieproces), Politie in verbinding, en Ontwikkeling professional. Deze onderwerpen staan voor gebieden met hoge innovatiebehoefte, passend bij de kennisbasis van TNO. Resultaten op deze gebieden omvatten technologieverkenningen, horizon scans, concepten, methoden, technieken, werkwijzen, interventies, demonstraties, instrumenten en toolboxes.

Shared Research Programma Cybersecurity: Het Shared Research Programma (SRP) Cyber Security is een onderzoeks- en innovatieprogramma waarin TNO en haar partners vanaf 2015 samenwerken met als doel de cybersecurity te verbeteren door middel van innovatieve technologieën en processen. De huidige partners van het programma zijn TNO, ABN AMRO, Rabobank, ING, Achmea en de Volksbank.

Het SRP betreft een meerjarige verbintenis, langs onderzoekslijnen: Monitoring & Response, Digitale Weerbaarheid, Cyber Intelligence, Human Factors in Cyber.

V1622 Innovatieve Cyber Vermogens (2016-2020): dit programma richt zich op innovaties voor Defensie en inbedding van cyber operations in de processen van Defensie. Het programma bleek bij de Mid-Term Review in 2017 een kraamkamer voor verdere technologieontwikkeling en nieuwe doelfinancieringsprogramma's (zie V1907 en V2009 hierna). Grotendeels gerubriceerd.

V1907 Cyber & Electromagnetic Activities (CEMA) (2018-2022): richt zich op de combinatie van militaire cyber operations en electronic defense. Gerubriceerd onderzoek.

V2009 Automated Cyber Operations (2020-2023): kennisopbouw voor automated security en mogelijk automated attack support. Gerubriceerd.

Risicodragend Verkennend Onderzoek (RVO, 2017-heden): verkenning militaire toepassingen van quantum technologie (w.o. toepasbaarheid, quantum safe technologie, quantum algoritmes, quantum communicatie). Sluit aan op onderzoek in het kader van VP ICT en samenwerking met TU Delft in QuTech.

2.1.5 Volume in omzet

In deze rapportage zijn geen exacte cijfers opgenomen over omzet en verdeling over opdrachtgevers, vanwege het potentieel gevoelige karakter ervan. Voor de analyse van de positie van TNO volstaat de analyse dat het volume van het cybersecurity-onderzoek gemeten in omzet sinds 2015 sterk is toegenomen. Dit geldt zowel voor de gelden voor kennisopbouw als voor (hoger TRL) contractresearch.

In 2018 en 2019 is er sprake van een uitzonderlijke piek in SMO en Defensiedoelfinancieringsgeld, in verband met eenmalige intensiveringen op cybersecurity-onderzoek door het kabinet.

De groei in omzet is overigens niet tekenend voor de groei van het aantal cybersecurity experts binnen de verschillende TNO-expertisegroepen ondanks dat er om en nabij zo'n 20% nieuwe medewerkers instroomt per jaar. In het algemeen genomen is de bezettingsgraad van experts toegenomen. Daarnaast doet het aantrekken van nieuw personeel een stevig beroep op de zittende medewerkers, en kost het veel tijd om nieuwe medewerkers goed inzetbaar te maken.

De capabilities waar TNO een goede kennispositie op heeft zijn:
1. Monitoring & Detectie
2. Automated Security
3. Cyber and Electromagnetic Activities (CEMA)
4. Ketenweerbaarheid

2.1.6 Profielen expertisegroepen

Het totaal aantal cybersecurity-experts is groeiende en wordt geschat op ca. 110, Dit zijn ongeveer 2/3 deel technische cybersecurity-experts (bèta) en 1/3 deel experts op bijvoorbeeld menselijk gedrag, militaire operaties, electronic defense, organisatie, strategie en beleid en quantum technologie (gamma en beta).

De afdelingen Cyber Security & Robustness (CSR), Networked Organisations (NO) en Electronic Defence (ED) kunnen worden gezien als de 'hofleveranciers' van onderzoekscapaciteit, meer dan 90% van de experts zit in een van deze drie afdelingen.

Afdeling	Experts CS[8]	Expertise
CSR bèta	56	Security Monitoring & Detection, Automated Security en Transaction Security, risico management, anomalie detective, quantum, algoritmes, cryptografie, netwerkbeveiliging, systeembeveiliging
NO gamma	18	Cybersecurity beleid- en strategie, informatie-uitwisseling, dreigingsanalyse, cybercrime en Darkweb, ketenafhankelijkheden
DS bèta	10	Cybercrime (Darkweb) analyses, secure data sharing architecturen en privacy-beschermings-technieken
ED bèta	7	Cyber and Electromagnetic Activities): (bescherming tegen) elektronische signaal disruptie en beïnvloeding.
HOI gamma	9	Menselijk gedrag in het digitale domein, cybercrime gedrag
Overig bèta + gamma	10	Networks (op het gebied van netwerkbeveiliging), Military Operations (MO) op het gebied van automated security in het militaire domein, Strategy & Policy (S&P), Strategic Business Analysis (SBA) en Modelling Simulation & Gaming (MSG) op het gebied van systeembeveiliging.

2.1.7 Kennispositie waarderingen expertisegroepen

Binnen TNO wordt bij expertisegroepen iedere vier jaar een Kennispositie Audit (KPA) en deze beslaat de periode van de voorgaande jaren. Groepen voeren een uitvoerige self-assessment uit, waarbij alle facetten van toegepast wetenschappelijk onderzoek beoordeeld worden. Een externe commissie beoordeelt de self-assessments, en komt na verdere consultatie tot een eindoordeel dat uit drie indicatoren bestaat:

- Kwaliteit (Q), de technische wetenschappelijke kwaliteit van het kennisniveau binnen de expertisegroep
- Impact (I), de relevantie van de expertisegroep voor industrie en maatschappij
- Vitaliteit (V), de mate waarin TNO is toegerust en gepositioneerd voor de toekomst in het licht van de ontwikkelingen. De scores worden gegeven op een schaal van 1 tot 5

Voor alle scores geldt dat er gestreefd wordt naar een score 4 ('zeer goed'), wat betekent dat de groep internationaal erkend is, concurrerend is, goede focus heeft en potentie voor vernieuwing laat zien. Een score 3 ('goed') betekent een nationale toonaangevende positie.

[8] Hier worden de medewerkers geteld met cybersecurity expertise die ingezet kunnen worden op cybersecurity onderzoek

Analyse van de meest recente KPA scores van de betrokken researchgroepen levert de volgende inzichten op de drie KPA elementen:

Scores op impact zeer goed
TNO scoort vanuit alle betrokken expertisegroepen in het cybersecuritydomein hoog (4) op impact bij haar klanten. Opgebouwde kennis wordt toegepast bij haar klanten en ontsloten in het (internationale) cybersecurity-ecosysteem. Voorbeelden hiervan zijn weergegeven onder het kopje impact (2.8).

Scores op kwaliteit en vitaliteit goed tot zeer goed
TNO scoort vanuit veel van de expertisegroepen in het cybersecuritydomein hoog (4) op kwaliteit en vitaliteit. Op deze aspecten scoren de jongere expertisegroepen CSR en DS iets lager (3), hetgeen deels verklaard kan worden uit het feit dat zij pas sinds 2011 stevig inzetten op dit domein en ten tijde van de KPA nog in opbouw waren.

2.1.8 Patenten

TNO heeft vanaf 2017 zo'n 20 octrooien in het cybersecurity domein in portfolio. De aanwas van octrooiaanvragen is ca. 3 per jaar.

2.1.9 Klanttevredenheid waarderingen expertisegroepen

TNO houdt systematisch klantwaarderingen bij voor haar activiteiten, de zogeheten Klanttevredenheids Audits (KTAs). Er worden steekproeven uitgevoerd waarbij klanten door een extern evaluatiebureau worden gevraagd om het uitgevoerde werk van TNO te beoordelen. Deze beoordeling gaat over verschillende aspecten van het project, zoals de kwaliteit van het eindproduct, de presentatie, de samenwerking, de financiële en administratieve aspecten, de waarde van het product voor de klant, en of de kans op vervolgopdrachten. De resultaten van alle steekproeven worden samengebracht in een jaarlijks evaluatierapport.

Het is niet mogelijk om specifiek voor 'cybersecurity-onderzoek' de scores te geven, maar we kunnen wel een aantal observaties delen:

Scores op klanttevredenheid zijn bovengemiddeld hoog
Het werk van units DSS en ICT (waar het gros van het cybersecurity werk plaatsvindt) wordt hoog gewaardeerd door klanten. De KTA-scores van unit DSS (4,45 uit 5) en unit ICT (4,44 uit 5) behoren tot de hoogste van TNO.

- Binnen deze scores worden met name de flexibiliteit, kundigheid en de kwaliteit van het eindproduct hoog gewaardeerd.
- Uit een aantal KTA's die uitgevoerd zijn op cybersecurity-onderzoek projecten, verschijnt een passend positief beeld. Een aantal quotes:
  - Cyber capacity building project voor een Ministerie: 'Nuttig, zoals beoogd. De inbreng van TNO wordt gebruikt in het kader van het ontwikkelen van de cyber capaciteit en het vergroten van de awareness op dit gebied bij defensie. We zijn nu bezig met de conceptontwikkeling, wat uiteindelijk moet leiden tot een product waar we in het kader van training en opleiding mee aan de slag kunnen.

- CSIRT maturity scan een Ministerie: ‘Kennis/deskundigheid, eindproduct en levertijd: De mensen hebben het onderzoek op een zeer professionele wijze en in korte tijd uitgevoerd.
- Agenda-zettend project voor een Ministerie: ‘Nuttig, zoals beoogd. We gebruiken dit verkennende onderzoek om een research-agenda op te zetten en om een researchnetwerk op te bouwen.
- Beoordelingsmethode voor securityproducten voor een Ministerie: ‘Ja, nuttig zoals beoogd. Met dit project proberen we andere ministeries te adviseren om beleidsmatig en operationeel goede keuzes te maken op beveiligingsgebied. (Inschatting risico's / aanschaf van producten).
- “Security measures should at least keep pace with ever evolving cybercrime threats. Traditional rule-based detection is no longer sufficient. Effective detection of threats calls for smart anomaly based detection. The Shared Research Program increasingly not only researches this topic but also develops implementation ready smart capabilities in the area of f.i. Phishing, prioritizing SIEM alerts, DNS Ninja. Participation in these projects makes us learn and gets us inspired and able to improve our capabilities by creating advanced models for early detection.” CISO ING

2.2 Marktgericht en adaptief

2.2.1 Afstemmingsmechanismen

Het belangrijkste afstemmingsmechanisme voor cybersecurity is een opdrachtgever of behoeftesteller die als programmabegeleider optreedt en zo de inhoudelijke prioriteitsstelling (en dus de maatschappelijke relevantie) van het cybersecurity-onderzoek stuurt. Dit zien we o.a. terug in de Vraaggestuurde Programma’s (NCSC als begeleider), het Shared Research Programma Cybersecurity (grootbanken, financiële instellingen als begeleider) en de Doelfinancieringsprogramma’s van Defensie (Defensie als begeleider).

Contractresearch geschiedt altijd op basis van een behoefte en met sturing van de opdrachtgever.

Zowel voor de Doelfinancieringsprogramma’s als voor contractresearch vraagt de opdrachtgever c.q. behoeftesteller steeds vaker om proof of concepts en demonstrators (TRL 4-5).

2.2.2 Ontwikkelingen in aard projecten portfolio

TNO heeft in de afgelopen jaren ingezet op het acquireren en vormgeven van grotere langdurige samenwerkingen/programma’s i.p.v. uitvoering van een groot aantal kleine opdrachten. Dit heeft geleid tot het ontstaan van een aantal van grote(re) ‘opdrachten’/meerjarige samenwerkingen met een specifiek doel: bijvoorbeeld het programma met BuZa, NCSC, Politie en INTERPOL ter versterking van het GFCE en het SRP Cybersecurity met de banken ABN AMRO, ING, Rabobank, Achmea, Volksbank) en strategische meerjarige samenwerkingen met de overheid (Def, JenV, EZK, BuZa).

2.3 Continue ontwikkeling

Het cybersecurity domein verandert snel van aard door nieuwe technologieën, nieuwe dreigingen, nieuwe organisatorische uitdagingen en nieuwe vraagstukken. Het cybersecurity domein verbreedt zich, verdiept zich, en raakt steeds meer vervlochten met andere domeinen. Deze dynamiek stelt hoge eisen aan TNO om actueel te blijven. Door de organisatie en manier van werken is TNO in staat om snel in te springen op nieuwe vragen en ontwikkelingen.

Hieronder volgt een niet-uitputtende lijst van (technologische) ontwikkelingen waarop TNO in de periode 2015-heden nieuwe onderzoeksactiviteiten heeft ontplooid:

- Cybersecurity van wapensystemen
- Cyber Electromagnetic Activities
- Quantum safe technologie (crypto en breder)
- Wet Computer Criminaliteit III
- Hybride statelijke dreigingen (inmiddels afgesplitst van cybersecurity door middel van het Hybrid Strategies Lab van TNO)
- Cyber Threat Intelligence
- Anomalie detectie
- Multi-party computation
- Veilig gedrag (‘beyond awareness’)
- IoT security en veilige hardware en software
- Information Sharing
- Incentives voor cybersecurity
- Horizon Scanning
- Impact ontwikkeling AI op cybersecurity vraagstukken

2.4 Intensivering van de samenwerking

2.4.1 Positie TNO als TO2 instituut

TNO voert een breed scala van toegepast onderzoek uit in het cybersecurity domein. Tot nu wordt er weinig samengewerkt met andere TO2 instituten op gebied van cybersecurity (Deltares, ECN, Marin, NLR, TNO en Wageningen-Research).

2.4.2 Ministeries

TNO is een strategische partner op cybersecurity voor het ministerie van Defensie, het ministerie van Justitie en Veiligheid, waaronder de Nationale Politie, NCTV en NCSC.

Sinds 2012 is Defensie een structurele opdrachtgever van Doelfinancierings-onderzoek en additioneel onderzoek en ontwikkeling. Met de groei en verspreiding van cybersecurity binnen Defensie, neemt ook het aantal individuele opdrachtgevers binnen Defensie de afgelopen jaren toe. Belangrijke opdrachtgevers zijn het Defensie Cyber Expertise Centrum (DCEC) en de afdeling Kennis, Innovatie Experimenten en Simulatie (KIXS, onderdeel van het Joint Informatievoorzienings Commando, JIVC).

In 2018 is voor de Kabinetsperiode 2019 – 2021 vanuit het interdepartementaal overleg (IO) met Buitenlandse Zaken, JenV/NCSC (Politie en INTERPOL) en EZK

een samenwerking opgestart op het onderwerp Cybercapacity Building, ter versterking van het GFCE. Het betreft hier de onderwerpen: Darkweb, IoT en CIIP/CSIRT.

TNO voert onderzoek uit voor het ministerie van Economische Zaken en Klimaat naar het verbeteren van de innovatieketen op het terrein van Cybersecurity.

2.4.3 Topsectoren

In juli 2018 heeft het kabinet een missiegedreven innovatiebeleid voor het nieuwe topsectorenbeleid vastgesteld. Veiligheid is een van de vier maatschappelijke thema's die daarin centraal staan, naast inzet op sleuteltechnologieën en sleutelmethodologieën.

Binnen het thema Veiligheid zijn onder leiding van het Ministerie van Defensie en het Ministerie van Justitie en Veiligheid acht missies gedefinieerd, die vragen om (toegepaste)innovaties. De missies voor Veiligheid zijn in 2019 uitgewerkt naar de Kennis- en Innovatieagenda (KIA) Veiligheid. Op het gebied van cybersecurity-onderzoek en innovatie verbindt de Nationale Cyber Security Research Agenda (NCSRA) verschillende disciplines met elkaar via vijf pijlers. Deze vormen voor de hieronder geprioriteerde onderzoeks- en innovatiegebieden een leidraad: ontwikkelen van kennis over cybercrime en betrokken daders; versterken van het gerechtvaardigd vertrouwen in digitalisering; bevorderen van veiliger digitaal gedrag; verminderen van de schaarste aan cybersecuritycapaciteit; versterken van offensieve en defensieve cybercapaciteiten; voorkomen van uitval van fysieke kritieke systemen ten gevolge van een cyberaanval in een keten.
Voor de KIA Veiligheid zijn vijf *deelprogramma's* voor Cyberveiligheid geïdentificeerd:

1. Bestrijden cybercrime
2. Bevorderen ontwikkeling cybercompetenties
3. Defensieve cybertechnologie
4. Offensieve cybertechnologie
5. Ketenweerbaarheid en governance

In de KIA sleuteltechnologieën komt cybersecurity ook expliciet aan bod. Binnen de sleuteltechnologieën wordt met name gewerkt aan technologieën die in meerdere missies relevantie hebben. Deze KIA sleuteltechnologieën is in opdracht van het ministerie van EZK door het topteam (HTSM) opgesteld. Cybersecurity technologie wordt vanuit meerdere sleuteltechnologieën gevoed: met name vanuit digital technologies en quantum technologies.

De genoemde deelprogramma's van de KIA veiligheid en de sleuteltechnologieën sluiten aan op de door TNO geprioriteerde onderwerpen.

2.4.4. Universiteiten

TNO onderhoudt banden met verschillende universiteiten in het veld van cybersecurity. TNO werkt samen met meerdere Nederlandse universiteiten in Europees en nationaal project-verband. Daarnaast nemen TNO-experts deel in vele expertgroeperingen, is TNO deelgenoot van dcypher, en zijn er meerdere TNO'ers gelieerd aan universiteiten via PhD trajecten of hoogleraarschappen. Een aantal actuele voorbeelden:

- Thijs Veugen (CSR) heeft een deeltijdaanstelling als onderzoeker bij het Centrum Wiskunde & Informatica (CWI) te Amsterdam.
- Thomas Attema (CSR) heeft een deeltijdaanstelling bij het Centrum Wiskunde & Informatica (CWI) te Amsterdam in het kader van zijn promotie.
- Maarten Everts (CSR) heeft een deeltijdaanstelling als onderzoeker aan de University of Twente in de Services, Cybersecurity and Safety (SCS) researchgroep.
- Rolf van Wegberg (NO) heeft een deeltijdaanstelling bij Technische Universiteit Delft, faculteit Technologie, Bestuur en Management in de onderzoeksgroep 'Economics of Cybersecurity' in het kader van zijn promotie.
- Rick van der Kleij (HOI) is op 1 januari 2018 gestart als senior onderzoeker aan het lectoraat 'Cybersecurity in het MKB' aan de Haagse Hogeschool. Zijn opdracht is om de digitale weerbaarheid van het MKB te vergroten.

Het ontbreekt aan een hoogleraar cybersecurity die verbonden is aan TNO. Er zijn binnen TNO diverse acties in gang gezet om een hoogleraar te verbinden aan TNO.

Ook wordt met de TU Delft intensief samengewerkt in het Blockchain Security lab, in partnership met de Singapore University of Technology and Design (SUTD).

2.4.4 Cybersecurity bedrijven

Het cybersecuritydomein in Nederland wordt met name gevormd door MKB en startups, de zogeheten 'pure players' die zich volledig met cybersecurity bezighouden.

Er zijn slechts twee bedrijven die hier meer dan 300 cybersecuritymedewerkers hebben, namelijk Fox-IT en KPN Security Services. De rest is klein tot veel kleiner. De meerderheid is gericht op dienstverlening in de vorm van consultancy (b.v. cyberrisicomanagement) ontwikkelen en/of implementeren van bestaande (buitenlandse) technologie. Dit betekent voor TNO dat de pool van partijen die bereid zijn structureel en langdurig te investeren in R&D beperkt is.

TNO werkt in projecten wel veel samen cybersecurity technologiebedrijven. Met bedrijven zoals Technolution, Netdialog, Bitdefender (RedSocks), DataExpert, TreadStone, Thales, KPN en Applied Risk.

In de praktijk blijkt het tot op heden voor TNO lastig met cybersecurity technologieleveranciers een langdurige en structurele samenwerking aan te gaan. De samenwerking met technologiebedrijven is nog vaak project gedreven en in een gelegenheids-consortium. Een nadere analyse hieromtrent zal blijken uit het EZK-onderzoek 'Verbeteren van de innovatieketen op het terrein van cybersecurity'.

2.4.5 Andere bedrijven (eindgebruikers)

Met eindgebruikers slaagt TNO er wel in langdurige samenwerkingen in programma's te gieten. Twee voorbeelden daarvan zijn het Shared Research Programma Cybersecurity met de banken en de meerjarige samenwerking met de Europese telecombedrijven via het ETIS platform9.

[9] www.etis.org

2.5 Internationalisering

2.5.1 Aantal internationale onderzoeksprojecten

TNO heeft van oudsher een sterke participatie in Europese projecten, en gebruikt deze om nationaal onderzoek te versterken en te complementeren, de zogeheten ‘multipliers’. Dit geldt ook voor Europese projecten in het cybersecurity domein. TNO voert deze projecten zoveel mogelijk uit in nauwe samenwerking met Nederlandse partners, waaronder betrokken ministeries, industriepartners en operationele netwerken.

De tabel hieronder geeft de belangrijkste lopende Europese projecten (H2020) weer waarin TNO participeert.

De toename van toegekende calls zijn een afspiegeling van de kennisbasis waarin TNO de afgelopen jaren op cybersecurity heeft geïnvesteerd. De Europese projecten leiden tot verdere kennisopbouw en -toepassing.

De keerzijde van het succes is dat daarmee de overheidsfinanciën (SMO) nagenoeg volledig voor matching worden ingezet.

Naam		Thema	Coördinator en NL Partners	NCSRA
PROMETHEUS (2018-2021)	PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS	Privacy-preserving cryptographic protocols voor gebruik in toepassingen zoals electronic payments, e-voting en cyberthreat intelligence.	Ecole Normale Superieure De Lyon (Fr) Centrum Voor Wiskunde En Informatica, Stichting Nederlandse Wetenschappelijk Onderzoek Instituten	DESIGN, PRIVACY
ASGARD (2016-2020)	Analysis System for Gathered Raw Data	Data analytics voor cybercrime bestrijding en opvolging.	Fundacion Centro De Tecnologias De Interaccion Visual Y Comunicaciones Vicomtech (Es) Netherlands Forensics Institute, Universiteit Van Amsterdam	DEFENCE

TITANIUM (2017-2020)	Tools for the Investigation of Transactions in Underground Markets	Methodes en technische oplossingen voor het onderzoeken en opvolgen van cybercrime, met specifieke aandacht voor virtuele currencies en dark markets	Ait Austrian Institute Of Technology Gmbh (AT) Coblue Cybersecurity (NL)	DEFENCE
SOCCRATES (2020-2023)	SOC & CSIRT Response to Attacks & Threats based on attack defence graphs Evaluation Systems.	Security automation en decision support voor versterking van SOC and CSIRT operations.		DEFENCE DESIGN
PROFILE (2018-2021)	Data Analytics, Data Sources, and Architecture for Upgraded European Customs Risk Management	Data analytics voor het bestrijden van transnational crime and terrorisme	Cross-Border Research Association (CH) Ministerie Van Financiën, Technische Universiteit Delft	DEFENCE
DEFRAUDify (ITEA, 2019-2022)	Detect Fraudulent Activities in dark web and clear web to protect your business	Methodes en technische oplossingen voor het onderzoeken en opvolgen van cybercrime, met specifieke aandacht voor virtuele currencies en dark markets	Coördinator: Hoffmann Bedrijfs-recherche Bunq bank, Target Holding, Almende BV, Web-IQ BV, TU Eindhoven, Coblue	DEFENCE

In het FP7 werkprogramma (2007–2013) heeft TNO o.a. deelgenomen aan SEGRID (Security for smart Electricity GRIDs), COURAGE (Cybercrime and cyberterrOrism (E)Uropean Research AGEnda), CAPITAL (Cyber security research Agenda for PrIvacy and Technology chALlenges) en CYSPA (European CYber Security Protection Alliance).

Daarnaast is TNO ook actief binnen de onderzoeksprogramma's van de European Defence Agency (EDA), zoals bijvoorbeeld in het MASFAD-1 en 2 project (military

Multi Agent System For APT Detection), in samenwerking met de Belgische Koninklijke Militaire Academie en Fraunhofer FKIE.

In Singapore wordt op de onderwerp Darkweb meerjarig samengewerkt met Ministry of Home Affairs (MHA) en INTERPOL (Cyber Space and New Technologies Lab). Op het onderwerp IoT vindt samenwerking plaats met de Cybersecurity Agency (CSA) en op het onderwerp Blockchain (Blockchain security Lab) met de Singapore University of Technology and Design (SUTD).

Zowel met MHA als met CSA is een MOU afgesloten tussen JenV/NCSC en voert TNO onder die vlag het onderzoek uit.

Voorts werkt TNO samen met INTERPOL op basis van een strategisch partnerschap en wordt op dit moment gewerkt aan een voorstel voor Law Enforcement en CSIRT.

De onderwerpen Darkweb, IoT en Law Enforcement en CSIRT dragen tevens bij aan de versterking van het Global Forum on Cyber Expertise (GFCE) via de HGIS gelden.

2.6 Onderzoeksfaciliteiten van wereldklasse

TNO heeft geen specifieke onderzoeksfaciliteiten ingericht voor cybersecurity research.

2.7 Huis voor talent

De afgelopen 5 jaar is er een grote instroom van nieuwe medewerkers geweest op het gebied van cybersecurity, hetgeen zich nog steeds voortzet. Dit geldt voor alle eerder genoemde afdelingen werkzaam in het cybersecurity werkveld.

TNO blijft continu op zoek naar nieuw talent: zowel mensen die net van de studie komen als mensen met ervaring op dit gebied in een andere werkomgeving. Dit is noodzakelijk omdat er ook mensen doorstromen vanuit TNO naar bedrijfsleven en overheid om daar de opgedane kennis en ervaring in praktijk te brengen. Ook dit is een functie die TNO graag wil vervullen: huis voor talent. Het opleiden van mensen die daarna in de maatschappij op andere plekken een waardevolle bijdrage kunnen leveren. Dit levert voor TNO een dubbel gevoel: het behouden van mensen voor de eigen projecten en tegelijkertijd het stimuleren van mensen ook om interessante functies buiten TNO te gaan bekleden.

Binnen TNO leert men in de projecten en van de meer ervaren professionals in de organisatie. Alhoewel er geen specifiek opleidingstraject voor cybersecurity is, zijn er de afgelopen jaren diverse initiatieven en activiteiten voor kennisdeling opgestart. Daarnaast studeren er gemiddeld 10 studenten per jaar - op het gebied van cybersecurity - af bij de verschillende afdelingen.

2.8 Technology transfer

Sinds een paar jaar voert TNO een actief spin-out beleid in de vorm van een centraal Tech Transfer programma. Dit programma is in 2018 gestart.

2.8.1 Aantal spin-outs met TNO cybersecurity technologie

Vanaf 2018 zijn er door TNO 2 spin-outs gerealiseerd:

- Sightlabs (2019). Deze spin-out richt zich op vermarkting van de DNS Ninja toolkit voor anomaliedetectie.
- TrustTester (2019). De software van TrustTester stelt mensen, organisaties of IoT-apparaten in staat om digitaal gedane beweringen over zichzelf te bewijzen, aan iemand of iets, peer-to-peer, met behulp van gegevens die de andere partij kan verifiëren

2.9 Impact

TNO scoort in de KPA's vanuit alle expertisegroepen hoog op de factor impact. Veel van de opgebouwde kennis wordt toegepast in andere opdrachten. TNO levert een zeer uiteenlopende set aan deliverables waarin haar kennis voor opdrachtgevers inzetbaar gemaakt wordt. Dit loopt van patenten, software, algoritmen, frameworks, maturity models, tot aan beschrijvingen van good practices Onderstaand een impressie van een aantal aansprekende recente voorbeelden van impact vanuit samenwerking & innovatie op het gebied van cybersecurity.

- **Het Shared Research Program (SRP) Cyber Securit**y
  Het SRP is een onderzoeks- en innovatieprogramma waarin TNO en haar partners samenwerken met als doel de cybersecurity te verbeteren door middel van innovatieve technologieën en processen. De huidige partners van het programma zijn TNO, ABN AMRO, Rabobank, ING, Achmea en de Volksbank. Afgelopen zomer is het eerste lustrum gevierd, en in het recente magazine staan diverse voorbeelden van de resultaten van deze samenwerking: https://www.tno.nl/nl/samenwerken/partners-van-tno/shared-research-program-srp-cyber-security/

- **Veilige data analyses zonder de onderliggende gegevens vrij te geven**
  Momenteel zijn er 15 miljoen patiënten met hartfalen in Europa. Het jaarlijkse overlijdensrisico van deze patiënten is 10% tot 20%. Met name patiënten met meerdere comorbiditeiten krijgen op dit moment niet de optimale medische behandeling en dat leidt tot veel ziekenhuisopnames. In het H2020 project Big Medilytics werken Achmea, Erasmus MC en TNO samen om gepersonaliseerde medische behandelingen aan te bieden op basis van veilige data analyses. Hierbij wordt gebruik gemaakt van multi-party computation (MPC), waarbij analyses op gecombineerde datasets gedaan worden zonder dat de privacy van individuen geschaad wordt. https://www.bigmedilytics.eu/pilot/heart-failure/

- **Betere analyses door veilig data delen**: uitwisseling van data kan ook belangrijk zijn voor o.a. de opsporing van verzekerings- of witwasfraude. Ook hier biedt multi-party computation (MPC) een uitkomst. Een aardige instructie (1min51) staat hier: https://www.tno.nl/nl/aandachtsgebieden/informatie-

communicatie-technologie/roadmaps/trusted-ict/secure-multi-party-computation-gezamenlijk-gevoelige-data-analyseren-zonder-deze-te-delen/

- **Betere analyses van (cyber) dreigingsinformatie**
  Het 'CTI Capability Framework' is een nieuw raamwerk voor het verzamelen en verwerken van Cyber Threat Intelligence (CTI) en praktische toepassing van CTI analyse- en visualisatietechnologieën die tactische (trend) analyses van dreigingsinformatie mogelijk maken. Referentie op ENISA website: https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cti-capability-framework/view. Publicatie TNO SRP 2017: https://www.thehaguesecuritydelta.com/media/com_hsd/report/140/document/innovating-in-cyber-security.pdf

- **Beoordeling van security producten**
  Security Tooling Assessment Methodiek (STAM) kent een focus op security monitoring & detectie. Monitoring- en detectieproducten zijn gericht op de detectie van kwaadaardige of verdachte activiteiten door een of meerdere gegevensbronnen in een infrastructuur te controleren (zoals netwerkverkeer of inloggegevens). Als dergelijke activiteit wordt gedetecteerd, kan een product een waarschuwing geven of onmiddellijk actie ondernemen om de activiteit te stoppen. In een volgende fase kan de STAM methodiek worden uitgebreid met andere domeinen binnen cybersecurity (incident response, deceptie technieken, breach management). Als resultaat is o.a. een (besloten) Wiki-pagina opgesteld waar eindgebruikers mee aan de slag kunnen.

- **Inzicht in bedrijfsnetwerk**
  "De speld in de hooiberg vinden.". Anomaliedetectie op netwerkverkeer is belangrijk voor het verkrijgen van inzicht en overzicht van netwerkverkeer, en de mogelijke risico's daarvan op informatiebeveiliging. TNO en NetDialog zijn een samenwerking aangegaan op het gebied van cybersecurity om de groeiende complexiteit van security issues beter in kaart te brengen. Door samen onderzoek te doen, is gewerkt aan een hoger niveau van digitale weerbaarheid. Zo leveren TNO en NetDialog in de loop van volgend jaar innovatieve detectiemiddelen op (bijv. Netflow en Email Ninja) via (statistische) anomaliedetectie, AI en slimme combinaties van meerdere (netwerk) gegevensbronnen. In het H2020-project SOCCRATES zal worden gewerkt aan op AI gebaseerde aanvalstechnieken.
  https://www.infosecuritymagazine.nl/nieuws/tno-en-netdialog-werken-samen-op-het-gebied-van-cybersecurity
  https://www.computable.nl/artikel/nieuws/datamanagement/6597863/250449/netdialog-en-tno-bouwen-securitymonitor-met-ai.html

- **Cybersecurity informatiedeling**
  Om de Nederlandse samenleving weerbaarder te maken tegen cyberdreigingen en het 'niet vitale' bedrijfsleven van onafhankelijke cybersecurity informatie te voorzien, wordt een landelijk dekkend stelsel van informatieknooppunten nagestreefd. Het Digital Trust Center (DTC) van het ministerie van EZK heeft TNO gevraagd onderzoek te doen naar cybersecurity informatiedeling voor informatieknooppunten en om een schaalbare en herbruikbare cybersecurity informatiedeling toolbox te ontwerpen. In 2018 heeft hiervoor een pilot met het

Cyber Weerbaarheidscentrum Brainport plaatsgevonden. De bouwblokken, ontwikkeld door TNO, worden door het Cyber Weerbaarheidscentrum Brainport en het DTC als belangrijke instrumenten gezien voor het bevorderen van cybersecurity informatiedeling. In 2019 vindt het onderzoek voor de verdere invulling voor de cybersecurity informatiedeling toolbox plaats met bestaande samenwerkingsverbanden: Cybersecurity Center Maakindustrie, Cyber Security Programma Noordzeekanaalgebied, FERM en CYSSEC.

- **ISAC ontwikkelmodel**
  Op basis van intensieve ervaring met de ontwikkeling van Information Sharing and Analysis Centers (ISACs), een samenwerkingsvorm waarin vitale infrastructuurbeheerders in Nederland vertegenwoordigd zijn en gefaciliteerd worden door het Nationaal Cyber Security Centrum (NCSC) om cybersecurity informatie met elkaar uit te wisselen, heeft TNO een ISAC ontwikkelmodel ontworpen. Via een ‘challengetraject’ met vertegenwoordigers uit diverse ISACs is een basis gelegd voor een ISAC ontwikkel- en groeimodel. Deze basis is vertaald naar een handreiking die uitgegeven zal worden door het NCSC. Daarmee worden concrete handvatten geboden voor ISACs en andere geïnteresseerden om cybersecurity informatiedeling verder te ontwikkelen.

- **Cyber Workforce Development**
  TNO heeft als subject matter expert voor het Ministerie van Defensie op het gebied van Cyber Workforce Development een competentieraamwerk helpen ontwikkelen. Samen met vertegenwoordigers van het US Department of Defence is het bestaande National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (uitgegeven door NIST) omgezet tot een door de NAVO-leden internationaal geaccepteerd raamwerk. TNO heeft vervolgens in opdracht van het ministerie van Defensie geholpen om dit raamwerk tot geaccepteerd beleid te ontwikkelen binnen het ministerie van Defensie zodat het geïmplementeerd kan worden. Defensie wordt daarmee in staat gesteld haar medewerkers de benodigde competenties bij te brengen om taken in het cyberdomein te kunnen uitvoeren en tegelijkertijd weerbaar te zijn tegen dreigingen die uit het cyberdomein voortkomen.

Verdere voorbeelden van impact staan in bijlage 1.

2.9.1 Ingebruikname TNO-technologie

Met het volwassen worden van cybersecurity als onderzoeksgebied, vinden meer technologieën vanuit TNO hun weg naar de markt. Bijvoorbeeld:

- DNS Ninja (anomalie detectie technologie) door de Rabobank
- C2D2 framework (Cyber Competences framework for Dutch Defense) formeel geadopteerd door Defensie en wordt momenteel geïmplementeerd
- Darkweb Monitor
- Homomorfe encryptie bij TrustTester

TNO zet in op de groei als het gaat om het overbrengen van technologie naar de markt: ofwel door technologie direct bij eindgebruikers te introduceren, ofwel door cybersecurity-marktpartijen hiervoor te interesseren. De kennisbasis is hoog maar wordt niet breed ingezet c.q. toegepast.

2.9.2 Doorontwikkeling van kennisopbouw naar technologieontwikkeling

Voordat technologie naar buiten kan, moet het vaak eerst vanuit kennisopbouw worden opgewerkt tot een hoger TRL-niveau, bij voorkeur in samenwerking met het bedrijfsleven. De afgelopen periode (niet-limitatief) is dat o.a. gebeurt met:

- Secure multiparty computation t.b.v. fraudedetectie bij de banken
- Anomaliedetectie in netwerkverkeer (ABC tool)
- Command & Control support tooling voor het Defensie Cyber Commando (van doelfinanciering naar contractresearch voor een prototype)
- Cybersecurity monitoring & detectietechnologie (van TRL 5 NTP Cyber Assurance naar TRL 6/7 NTP Cyber Logging & Monitoring naar voornemen tot daadwerkelijke implementatie in grootschalige oefening in 2020)
- Kruisbestuiving tussen verschillende quantum key distribution (QKD) trajecten voor overheid en (internationaal) bedrijfsleven. Dit zorgt overigens wel voor juridische uitdagingen (wat mag onder welke voorwaarden worden hergebruikt)

3 Wat gaat goed en wat kan beter?

TNO vervult op het gebied van toegepast onderzoek een positie in het cybersecurity landschap gezien de verbondenheid met het kennis- en innovatie landschap én eindgebruikers, en haar rol om mensen en kennis te verbinden.

> *General observations and recommendations*
> *"Overall, the committee was impressed by the technology available and the way this is used for research, results and innovation. But technology as such is useless if the people using it are not empowered and motivated to use it. The committee is convinced that TNO has the unique capability to use the tension, friction and synergy that occurs when humans and technology interacts. And it is the people of TNO who makes this work with their great skills, commitment and passion."*

Quote uit KPA van HOM/DSS uit 2017

In deze sectie worden de kernpunten benoemd die eruit springen in de voorafgaande zelfanalyse van op het functioneren van TNO, in termen van 'Wat gaat goed' en 'Wat kan beter'.

Wat gaat goed?

1. Kwaliteit: over het algemeen hoge kwaliteit van het uitgevoerde werk (KTA score 4-5 uit 5) door omvangrijke pool (110+) hooggekwalificeerde medewerkers (onderzoekers en consultants) met grote betrokkenheid rond (maatschappelijke) vraagstukken op het gebied van cyberveiligheid (techniek, organisatie, mens).
2. Impact: strategisch partner van Defensie, Ministerie van JenV (NCTV, NCSC, Politie), **en** verschillende sectoren (bv. Nederlandse financiële sector en telecomsector). Goed ingebed in diverse cybersecurity-ecosystemen, waarbij de opgebouwde kennis wordt ontsloten. Dual use (civiel-militaire) technologieontwikkeling.
3. Vitaliteit: TNO sluit goed aan op de beleidsagenda's van de departementen en de onderliggende KIA's. De focus is belegd op een aantal onderwerpen en een mechanisme (PMC's) waardoor mee bewogen kan worden met externe ontwikkelingen.

Wat kan beter?

1. Kwaliteit: uitdaging bij het invullen van groei van de vraag naar goede experts.
2. Impact: nog niet voldoende structurele samenwerking met cybersecurity technologieleveranciers (vooral ad hoc samenwerkingsverbanden).
3. Vitaliteit: zichtbaarheid: profilering van de resultaten kan beter (deels door vertrouwelijk karakter van werk voor Defensie en het Veiligheidsdomein en ontwikkelen van 'technologie voor morgen'), waardoor de buitenwereld een beter beeld krijgt wat TNO allemaal doet

4 Conclusies

Aan de hand van de zelfevaluatie komt TNO tot de volgende conclusie:

4.1 Positie TNO

De markt voor cybersecurity technologie (in breedste zin des woords) is nog steeds groeiende. Gezien de sterke, structurele groei van het opdrachtenportfolio bij TNO is er ook substantiële behoefte aan toegepast (wetenschappelijk) onderzoek op dit domein.

De groei van de afgelopen jaren, afgezet tegen een krappe capaciteit (en arbeidsmarkt) heeft de al eerder onderkende noodzaak tot focus versterkt en zal deze blijven versterken. TNO gebruikt hiervoor de PMC's. Inhoudelijk liggen de speerpunten onder andere op resilient engineering, automated security, monitoring & detectie, cybercrime, societal cyber resilience, quantum safe en andere high assurance technologie en offensieve cybercapaciteiten.

TNO neemt hier een positie in tussen wetenschap, cybersecurity-industrie en eindgebruikersorganisaties. Daar waar de (binnenlandse of buitenlandse) industrie niet kan, wil of mag leveren, ligt er ook een rol voor TNO.

4.2 Sturen op het geïmplementeerd krijgen van innovaties en samenwerking

Door het werken met PMC's wil TNO meer sturing brengen op welke middelen per speerpunt per fase (kennisopbouw / technologieontwikkeling / kennistoepassing) kunnen worden ingezet. De kennisbasis van TNO op de PMC's is hoog.

De PMC's en de daarin beschreven doelen zijn leidend voor de programmering van het onderzoek van TNO. Daarin is technologie-ontwikkeling in co-development met private en/of publieke partners en valorisatie ervan een belangrijke drijfveer, naast het organiseren van vraag en aanbod en participeren in innovatieketens van onderzoek naar toepassing.

Het cybersecurity veld kent een groot aantal spelers. Vanuit TNO wordt met alle spelers regelmatig samengewerkt. Toch is er nog ruimte voor verbetering op het gebied van samenwerking. Vraag en aanbod ontmoeten elkaar nog niet voldoende op *structurele* wijze.

Het opzetten van samenwerkingsverbanden ziet TNO overigens nadrukkelijk niet alleen in Nederlands verband, maar ook in Europees perspectief. Samenwerking met buitenlandse partijen en landen is gezien de schaarse expertise en snelle ontwikkelingen een logische, zij het soms moeilijk te operationaliseren stap.

Structurele, langdurige meerjarige samenwerkingsverbanden in gerichte programma's (zowel nationaal als internationaal), komen nog niet gemakkelijk op gang. Daardoor zijn er veel gelegenheidscoalities op projectbasis. Dit genereert wel aantoonbaar valoriseerbaar succes, maar met de meerjarige programma's die wel van de grond zijn gekomen (o.a. SRP met de banken) lukt dit nog beter. Op de

gekozen speerpunten streeft TNO dan ook naar meerjarige samenwerking. Vgl. het initiatief van TNO rond publiek private samenwerking op automated security en de participatie aan de Nationale Crypto Strategie.

4.3 Tot slot

De uitdagingen op cybersecurity vragen om een publiek-private aanpak, van fundamenteel onderzoek tot het naar de markt brengen van technologie en alles er tussen. TNO is goed en herkenbaar gepositioneerd in de keten en werkt met veel partijen samen. Een structurele samenwerking met de cybersecurity-leveranciers is er nog niet, waardoor samenwerking met deze partijen in de keten op projectniveau blijft. Hier is nog ruimte voor verbetering, waar TNO ook op inzet met haar programmering.

De Nederlandse schaal vraagt ook om beperking in de vorm van inhoudelijke focus en om internationale samenwerking met vertrouwde partners.

Bijlage 1: Voorbeelden impact

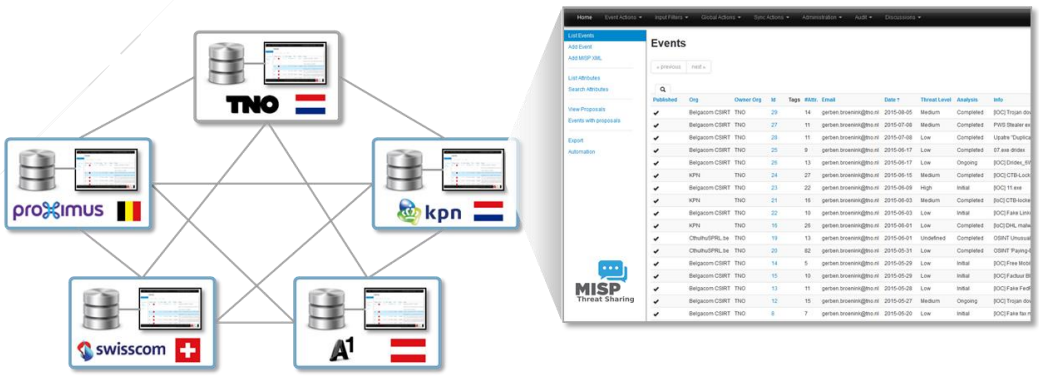
In dit hoofdstuk zijn enkele voorbeelden van onderzoek met wetenschappelijke en/of maatschappelijke impact weergegeven zoals die zijn beschreven in de KPA's van de diverse afdelingen. De voorbeelden zijn in het Engels en vonden plaats in de periode 2013 tot en met 2017.

Security assessments & innovations for European telecom operators
The telecommunications industry has undergone drastic changes in the past decade. Telecoms providers now operate full-IP infrastructures through which they deliver multi-play (voice, TV, internet) service portfolios and are constantly dealing with new developments such as the advent of cloud services and virtualization technologies (NFV/SDN). At the same time, the role and importance of telco services in society and business has rapidly increased. Services such as internet and e-mail have become vital for the economy in general, the continuity of businesses and even a country's national defence. From a (cyber) security perspective, these developments have presented telcos with a whole new landscape of risks and vulnerabilities. Correspondingly, telcos across Europe have been pursuing elevated levels of security within their infrastructures and services. TNO CSR has played a leading role in this process by establishing a Telco Security Benchmark.

This Telco Security Benchmark takes place annually under the umbrella of industry body ETIS (www.etis.org) and revolves around six security themes with distinct telco relevance, a.o. "security in development projects", "network & system security" and "security monitoring and incident response". The outcome encompasses formal maturity scores on each of the benchmark themes as well as a depiction of novel or otherwise interesting "successful practices" observed at individual participants that may serve as an example for others. Since 2009, a total of 23 European telcos took part in TNO CSR's benchmark endeavor. The participant base encompasses tier 1 (a.o. Deutsche Telekom, British Telecom, Orange, Telefónica), tier 2 (a.o. KPN, Proximus, Telenor, Teliasonera, Swisscom) and tier 3 providers, many of which take part on a bi-yearly basis to assess their development over time (e.g. the effects of dedicated security investments). Participating in TNO CSR's security benchmark essentially allows participating companies to determine whether they are still sufficiently aligned with the ever evolving security standards in the telco industry.

Figuur 4: Sample performance graph from annual telco benchmark

As a result of this benchmark activity, TNO CSR has become an authority for assessing the state of security in telco organizations. This is illustrated by the fact that it has led to strategically significant assignments at individual telcos, for instance a cyber maturity assessment project for Proximus (Belgian telecom provider) and Security strategy challenge for KPN.



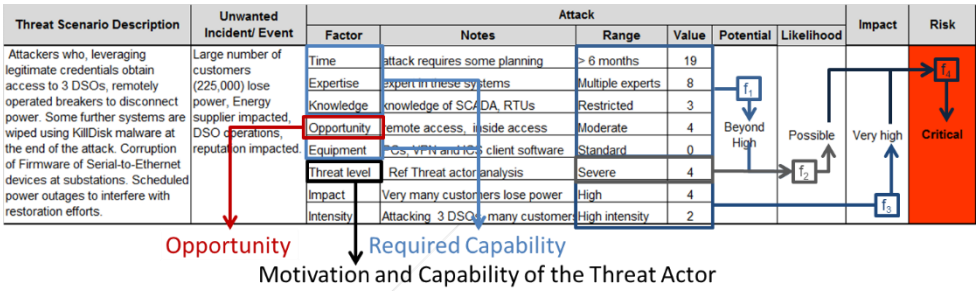
Figuur 5: Telco pilot infrastructure for CTI sharing & collaboration

Impact: CSR assessed and enhanced the state of cyber security and cyber resilience of 23 European telecom operators.

Leading FP7 SEGRID: making smart grids more secure

CSR is the overall coordinator of the FP7 project SEGRID (Security for Smart Electricity GRIDs, 2014-2017), with DSO's, manufacturers, knowledge institutions and universities from 5 European countries (www.segrid.eu). The main objective is to enhance the protection of smart grids against cyber-attacks. SEGRID has formulated privacy and security goals for the SEGRID use cases that were defined in the project and has performed a risk analysis of these use cases. The underlying risk analysis methodology is specifically suited for electricity grids and was enhanced by integrating approaches of risk propagation in value chains, introducing societal impact and by including

Threat Actor Capability and Motivation in the Threat & Vulnerability Analysis. This last enhancement was adopted by ETSI to be included in the next version of their TVRA standard. Although the results of applying the risk analysis to SEGRID use cases is classified as EU restricted, the enhanced risk analysis methodology itself will be published in 2017. Furthermore, an article on the SEGRID risk management method (SRMM) will be published in IEEE Computer Magazine, April 2017.

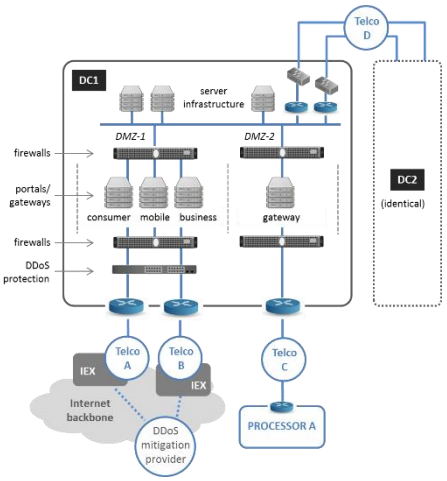


Figuur 6: The enhanced TVRA tool to assess risks.

Vulnerability assessment frameworks and tools to identify these risks in real systems have been developed and gaps in the currently available security solutions have been identified. Solutions for some of these gaps are under development and selected vulnerability assessment tools and novel security solutions will then be tested in the SEGRID Test Environment.

Impact: improving current risk assessment standards, identifying the risks of emerging smart grids, and making the current and future smart grids more secure.

Cyber resilience & dependence of the Dutch financial services on telco infra



Financial services rely heavily on telecommunications infrastructure, and crucial financial processes only run smoothly if the underlying in-house ICT and external telecommunications infrastructure are reliable and robust. TNO has been commissioned by seven Dutch financial institutions (DNB, ABN AMRO, Rabobank, ING, SNS Bank N.V., RBS, Equens) to investigate the current state of this dependence and robustness, in close cooperation with these seven financial institutions and their main telecom providers. A total of ten telecoms providers took part in the project. The project was led by CSR. The key research question was: ‘Are the

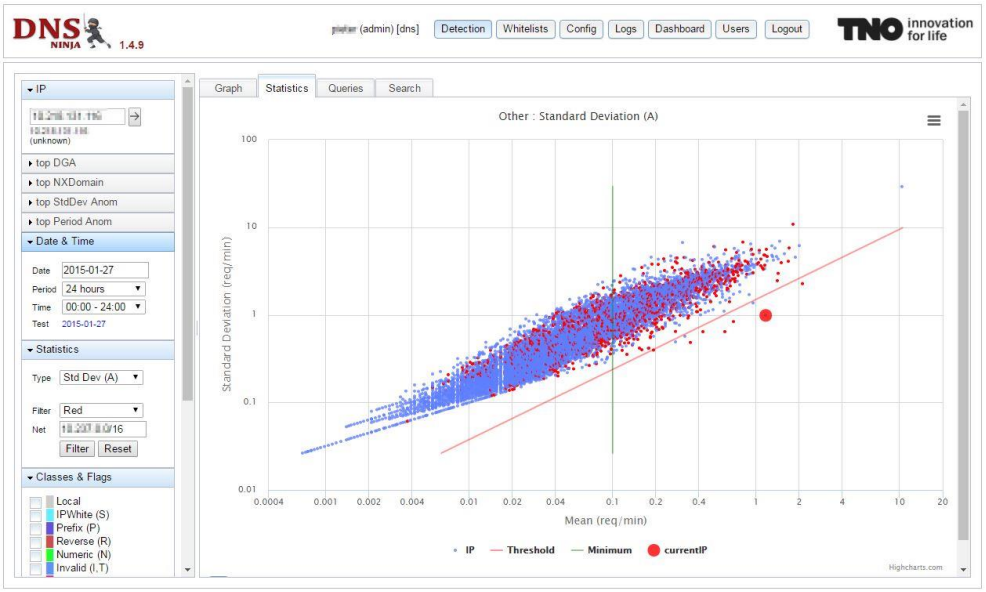
telecommunications infrastructures used in vital payment processes sufficiently robust and how can this be demonstrated?'
To answer this question, TNO assessed the dependency on telecommunication infrastructures for two financial services: 'transfers using online and mobile banking' and 'debit card payments'. Pre-designed questionnaires (covering both technical and process aspects) were used to interview the expert staff of all 17 parties involved in the study. The analysis and outcomes of this information are set down in a generic report for all participants and in 20 specific reports, i.e. one per pair of institution - telecoms provider, of course, only made available to the specific pairs of financial institutions and telecoms providers.

Impact: this unique cross-sector project assessed the dependencies between two vital sectors (telecom & finance) and significantly improved the reliability of the financial services in the Netherlands.

DNS Ninja: real-time anomaly detection of (Rabobank) DNS traffic
DNS traffic is a blind spot in the (internal) security monitoring of many organizations. However, infections and attacks (botnets, ransomware, key loggers etc.) may be detected better or quicker if we monitor their DNS queries: when malicious software tries to contact some external server(s), DNS is commonly used for finding their IP addresses. CSR has developed DNS Ninja as an extra line of defense, complementing existing security products (e.g. anti-virus, IDS/IPS, DNS blacklists). Because DNS Ninja is based on Anomaly Detection techniques, it is able to detect threats that have not been seen before ("zero day attacks"). Its main functions are:

- Real-time filtering and classification of DNS queries.
- Detecting anomalies in statistical properties of DNS traffic of individual workstations.
- Real-time detection of "suspicious" host and domain names.
- Sending alerts with "anomaly-scores" to a Security Information and Event Manager (SIEM) for correlation with other information and events.
- Inspection and analysis of DNS traffic and detected anomalies (forensics) through a web-based user interface.

DNS Ninja is developed over several years in close collaboration with Rabobank SOC and it is already integrated in Rabobank's daily cyber security operations. CSR is further improving the DNS Ninja algorithms and functionality, and also carrying out POCs with other parties in the Dutch financial sector (as well as TNO Information Services and Defense). In addition, international customers have already expressed interest and a spin-off is being investigated for further technology commercialization.



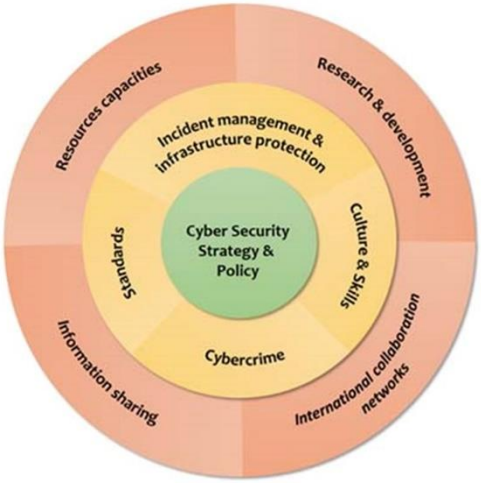
Impact: new detection technology, complementing existing security products, is deployed at a major international bank. It provides an extra line of defense for the detection of malware-infected systems. Many other parties from the financial sector have expressed great interest.

Development military Cyber Operations (2012-ongoing)
Because of the strategic relation with the MoD Research Group NO was part of the start of the Task Force Cyber five years ago and was instrumental in establishing the Defence Cyber Command (DCC). For starters, the development of the Education, Training and Knowledge (OTK in Dutch) Policy that describes and rates the impact of 'working in the cyber domain' in the project OTK cyber. Research Group NO developed the methodology and made the process tangible and accessible for non-cyber experts, closely working together with MoD representatives. The OTK Cyber was officially published by Brig.Gen. Folmer in March 2016. All 7 Defence departments are currently involved in implementing this policy process. Research Group No facilitates the implementation of the OTK Cyber within these seven Defence departments.

In 2014-2015 Research Group NO supported the Royal Netherlands Marechaussee (KMAR) in specifying their Cyber Capability Development Framework and the accompanying specification of the OTK Cyber. The KMAR is currently implementing the framework and the process to integrate cyber in their education processes and their daily tasks. In 2016 the OTK cyber was further developed and linked to the cyber education course, resulting in an Education Plan. In all projects and activities Research Group NO has either a facilitating or cyber education & training role and works closely with MoD representatives to guarantee project success. By using extensive knowledge of cyber and experience in the Defence domain, Research Group NO has created a unique role to support the MoD in a wide variety of cyber related (policy) issues. Because of our strategic relation with

the MoD, Research Group NO was part of the start of the Task Force Cyber continues to be a reliable innovation partner to guarantee success of the DCC in the future.

Global Cybersecurity Agenda and Good Practice Guides for the GFCE
The development of the first Global Agenda on Cyber Capacity Building, as commissioned by the Global Forum on Cyber Expertise (GFCE) has been facilitated by TNO. Members, partners and advisory board of the GFCE used the opportunity of the Global Conference on Cyberspace 2017 in New Delhi, India, to announce the GFCE Global Agenda for Cyber Capacity Building, which derives from best practices and lessons learned in the development, security and technical communities. Nations committed to work with the Global Agenda, as stated in the 'Delhi Communiqué'.



Cyber Capacity Building (CCB) concerns the development and reinforcement of processes, competences, resources and agreements that allow communities, businesses and governments to cope with the rapid changes and challenges of our digital society – with a strong emphasis on preserving the safety, security and openness of cyberspace. As cyberspace transcends national borders, it is important for nations to align efforts and build partnerships.
The Global Agenda provides guiding principles and key capacity building themes that help to streamline CCB activities within and across nations.

TNO and the GFCE have identified key topics and capacities in these thematic areas. The themes and principles in the Global Agenda on CCB are based on contributions from a wide range of stakeholders, including non-governmental organizations, private companies, governments, international governmental organizations, and think-tanks from around the globe.

The endorsement of the Global Agenda during GCCS 2017 is an essential step in worldwide coordination of CCB efforts and aligns a diverse set of worldwide stakeholders. The next step is the action plan in which GFCE and GCCS members commit to mobilize CCB capacities and coordinate initiatives.

In collaboration with knowledge institutes, private stakeholders, policy makers and the technical community GFCE has published Good Practice Guides for all stakeholders involved in cyber capacity building.

- National Computer Security Incident Response Teams (CSIRTs)
- Critical Information Infrastructure Protection (CIIP).
- Coordinated Vulnerability Disclosure (CVD).

- Internet Infrastructure Initiative (III).
- The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.
- Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.
- Sharing cyber security information (GCCS 2015).
- Cyber security of industrial control systems (GCCS 2015).

The GFCE is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The secretariat aims to identify successful policies, practices and ideas and multiply these at a global level.

More information about the Global Agenda on Cyber Capacity Building and Global Good Practices: www.thegfce.com