VARIO
Vlaamse Adviesraad voor Innoveren & Ondernemen

Vlaanderen
is ambitieus

RAPPORT 3
bij Adviezen 12 en 22

EXPERT-RAPPORT

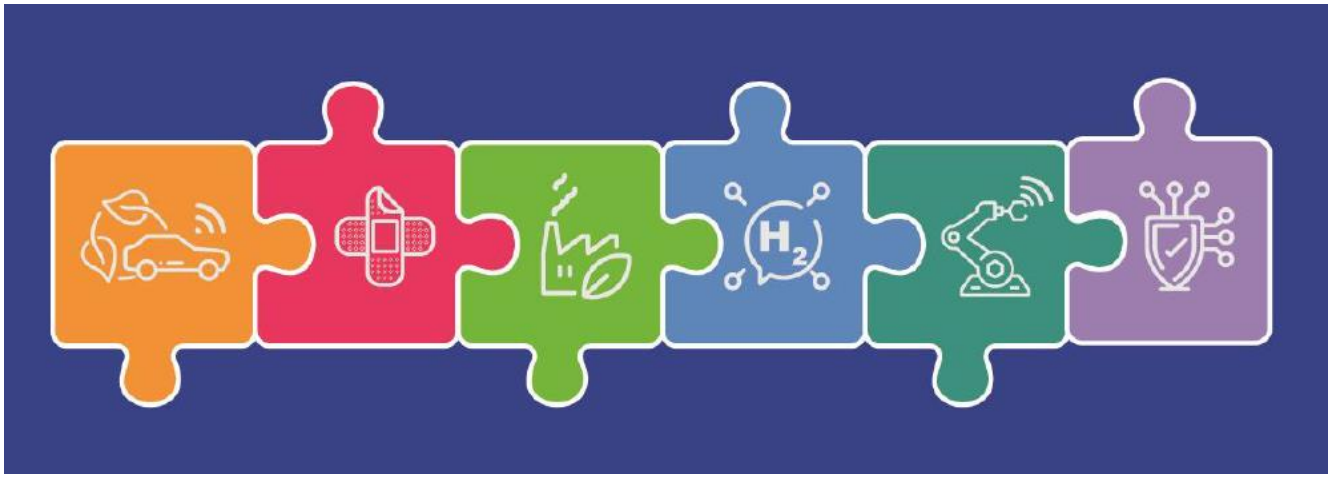
STRATEGISCHE ANALYSE VAN DE WAARDEKETEN

CYBERSECURITY

IN HET KADER VAN IPCEI

(IMPORTANT PROJECTS OF COMMON EUROPEAN INTEREST)

SEPTEMBER 2022



De Vlaamse Adviesraad voor Innoveren en Ondernemen (VARIO) adviseert de Vlaamse Regering en het Vlaams Parlement over het wetenschaps-, technologie-, innovatie-, industrie-, en ondernemerschapsbeleid. De raad doet dit zowel op eigen initiatief als op vraag. VARIO werd bij besluit opgericht door de Vlaamse Regering op 14 oktober 2016. VARIO werkt onafhankelijk van de Vlaamse Regering en de partijen in het werkveld. De voorzitter en de negen leden van VARIO zetelen in eigen naam:

Het secretariaat is gevestigd in Brussel:
Koning Albert II-laan 35 bus 9
1030 Brussel
+32 (0)2 553 24 40
info@vario.be
www.vario.be

EXPERT-RAPPORT

STRATEGISCHE ANALYSE VAN DE WAARDEKETEN

CYBERSECURITY

IN HET KADER VAN IPCEI

(IMPORTANT PROJECTS OF COMMON EUROPEAN INTEREST)

SEPTEMBER 2022

INHOUD

CONTEXT

1. VRAAG OM ADVIES

Begin 2020 werd VARIO door toenmalig minister voor Economie en Innovatie Hilde Crevits om advies gevraagd inzake de *Important Projects of Common European Interest* (IPCEI's): *"Via de IPCEI-projecten wil de EU de lidstaten de mogelijkheid geven om de vorming van Europese waardeketens te stimuleren met steun voor O&O, maar ook voor de eerste uitrusting van pilootfabrieken. De EC heeft een achttal domeinen geïdentificeerd waarbinnen ze projecten wil stimuleren gaande van batterijen voor de elektrische auto over waterstof tot cybersecurity.*

Ik vraag nu aan VARIO om een strategische verkenning en analyse uit te voeren van de sterktes en opportuniteiten die er zich voor Vlaanderen stellen voor de verschillende mogelijke IPCEI's.

- *Waar hebben we uitmuntende onderzoekers?*
- *Waar zijn de bedrijven die een cruciale schakel kunnen worden in een nieuwe EU-waardeketen?*
- *Waar zitten risico's als we niet zouden meedoen?*

We gaan immers keuzes moeten maken op welke projecten we met onze kennisinstellingen en industrie prioritair willen inzetten. Een ding is vandaag duidelijk: we kunnen niet op alles inzetten. Onze middelen moeten we focussen en daarvoor hebben we de nodige onderbouwing nodig. VARIO kan daartoe een belangrijke insteek leveren."

De acht domeinen waarnaar minister Crevits in haar adviesvraag refereert zijn: (1) Microelectronics, (2) Batteries, (3) Clean, connected and autonomous vehicles (CCAV), (4) Smart health, (5) Low CO_2 emissions industry, (6) Hydrogen technologies and systems, (7) Industrial internet of things (Industrial IoT) en (8) Cybersecurity (CS)

Deze vraag om advies bouwt verder op het politieke engagement voor IPCEI in het regeerakkoord 2019-2024 "*We hanteren een meer strategische aanpak van de Important Projects of Common European Interest (IPCEI), en voorzien hiervoor de nodige middelen.*"[1], en werd verder geëxpliciteerd in de beleidsnota Economie, Wetenschapsbeleid en Innovatie[2] van toenmalig Vlaams minister van Economie en Innovatie Hilde Crevits: "*Via IPCEI-projecten wil de EU de lidstaten stimuleren om middelen te bundelen in grote projecten die bijdragen aan de concurrentiekracht van de Unie. Europa voorziet de mogelijkheid tot een ruimere toekenning van staatssteun. We hanteren voor de IPCEI een Vlaamse strategische aanpak en ondersteunen voor Vlaanderen relevante projecten via de middelen voor innovatiebeleid. De deelname aan deze belangrijke projecten zorgt er immers voor dat Vlaamse bedrijven, en ook kmo's, kunnen aansluiten bij nieuwe Europese waardeketens voor toekomstgerichte innovaties. We willen van deze*

[1] Vlaamse Regering 2019-2024 regeerakkoord pp. 40. Oktober 2019
[2] Beleidsnota Economie, Wetenschapsbeleid en innovatie (2019-2024) ingediend door viceminister-president Hilde Crevits, Vlaams minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw, pp. 19-20. 8 november 2019.

mogelijkheid gebruik maken om het economisch weefsel in Vlaanderen te versterken en bedrijven hier te verankeren. We volgen het Europees beleid op en werken een strategisch kader uit voor deelname aan IPCEI's op basis van toegevoegde waarde voor Vlaanderen. Een eerste IPCEI waaraan we zullen deelnemen is de uitbouw van een waardeketen voor batterijen."

2. VARIO-AANPAK IPCEI-ADVIESTRAJECT

De vraag om advies kwam net nadat eind 2019 de IPCEI-batterijen voor elektrische auto's was gestart, de eerste IPCEI waaraan België en Vlaanderen participeert. De vraag om advies was ingegeven vanuit de nood aan onderbouwing om geïnformeerd beslissingen over deelname aan mogelijke toekomstige IPCEI's te kunnen nemen. De mogelijkheid om IPCEI's op te zetten is op zich niets nieuws. De communicatie van de Europese Commissie dateert van 2014. M.b.t. high-performance computing and Big Data Enabled Applications werd reeds in 2017 gekeken naar de opties om een IPCEI op te zetten. Er werd toen echter beslist om dit niet te doen en een andere formule te kiezen voor de ondersteuning van dit initiatief.[3] In december 2018 werd dan toch de eerste IPCEI gelanceerd; één rond micro-elektronica. België neemt evenwel geen deel aan deze IPCEI.

VARIO werd gevraagd een strategische analyse uit te voeren van de zes waardeketens die op 5 november 2019 door het *Strategic Forum on IPCEI* werden geïdentificeerd als potentiële toekomstige IPCEI's: (1) Clean, connected and autonomous vehicles (CCAV), (2) Smart health, (3) Low CO_2 emissions industry, (4) Hydrogen technologies and systems, (5) Industrial internet of things (Industrial IoT) en (6) Cybersecurity (CS).

Omdat ten tijde van de vraag om advies in het voorjaar van 2020 door de FOD Economie al een oproep werd gelanceerd voor het indienen van 'expressions of interest' voor een IPCEI 'Hydrogen Technologies and Systems' met juni 2020 als deadline, heeft VARIO prioriteit gegeven aan het in kaart brengen van de waterstofwaardeketen.

2.1 VARIO-advies 12: Strategische Verkenning IPCEI – deel I Waterstof

VARIO overhandigde haar advies 12 'Strategische Verkenning IPCEI – deel I Waterstof' in juli 2020 aan toenmalig Vlaams minister van Economie en Innovatie Hilde Crevits. Dit advies omvat een studie over de perspectieven voor een Vlaamse waterstofeconomie. Daaruit blijkt dat Vlaanderen alle troeven in huis heeft om een toonaangevende rol te spelen in Europa op het vlak van waterstof, mits de juiste ondersteuning. Ondertussen werden er ook reeds een aantal belangrijke stappen gezet:

- **13 november 2020:** In een mededeling aan de Vlaamse Regering stelt Hilde Crevits de Vlaamse Waterstofvisie 'Europese koploper via duurzame innovatie' voor. Met de opmaak van een Vlaamse Waterstofvisie geeft de Vlaamse Regering het startschot voor de uitrol van een waterstofbeleid en ook gehoor aan één van de aanbevelingen van VARIO.
- **17 juli 2020:** de Vlaamse Regering stemt in met deelname aan de IPCEI-waterstof en met een aantal bepalingen die een kader vormen voor deelname.
- **19 oktober 2021:** Vlaanderen selecteert 10 waterstof projecten voor de IPCEI waterstof van de Europese Commissie. De eerste reeks van 5 projecten wordt nu ter goedkeuring voorgelegd aan de Europese Commissie. De totale projectkost voor de 10 Vlaamse projecten bedraagt 1,025 miljard

[3] https://eurohpc-ju.europa.eu/index_en

euro. Vlaanderen zelf maakt voor de 5 projecten in de eerste IPCEI golf een totaal budget van 106,3 miljoen euro vrij.

- **15 juli 2022:** de Europese Commissie keurt 5,4 miljard euro publieke steun van 15 lidstaten goed voor een IPCEI in Hydrogen Technology genaamd 'Hy2Tech'.[4]

2.2 Expert-rapporten: Strategische analyse waardeketens IIoT, Smart Health, CS en CCAV

Omwille van de grote workload heeft VARIO na het uitvoeren van de strategische analyse van de waardeketen m.b.t. waterstof beslist om de analyse van de volgende vier waardeketens te laten uitvoeren door externe experten.

1. Industrial IoT – Filip Vandamme (Long Gamma bv.)
2. Smart Health – Frank Boermeerster, Bart Collet en Koen Kas (Healthskouts)
3. Cybersecurity – Ulrich Seldeslachts (LSEC)
4. Clean, Connected and Autonomous Vehicles – Sam Maddalena (Absolute Sensing)

De analyse van de waardeketen 'Low Carbon emissions industry' werd in samenspraak met het kabinet Innovatie voorlopig on hold gezet omwille van de onderzoeksopdrachten die in het kader van deze problematiek al werden en nog worden uitbesteed.

- De externe experten hebben voor de opmaak van de onafhankelijke expert-rapporten een beroep gedaan op hun eigen expertise, desk research en interviews (een lijst met geconsulteerde partijen werd telkens toegevoegd in bijlage van elk rapport). Deze rapporten werden opgemaakt tussen december 2020 en december 2021. Vervolgens werd een validatieproces toegepast op de externe expert-rapporten, via een validatieworkshop (van anderhalf uur via teams) met een brede groep stakeholders/experten.
- De input van de validatieworkshop werd verwerkt in het expert-rapport door de VARIO-staf, en opnieuw gevalideerd door de stakeholders/experten die deelgenomen hebben aan de workshop.

Het resultaat zijn vier rapporten opgemaakt door externe experten, waarop de eindredactie is gebeurd door de VARIO-staf.

De VARIO-raadsleden benadrukken dat de rapporten de visie en aanbevelingen van de externe experten weergeven, aangevuld met informatie uit de validatieworkshop.

In voorliggende publicatie wordt het expert-rapport CYBERSECURITY voorgesteld.

[4] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4544

2.3. VARIO-advies 22: Strategische verkenning IPCEI – deel II: afwegingskader om in te spelen op toekomstige opportuniteiten inzake IPCEI

Tijdens de uitvoering van de strategische analyses van voormelde vier waardeketens door de experten in de loop van 2021, werd al snel duidelijk dat nog andere waardeketens circuleren als mogelijke IPCEI's. De confrontatie met de Covidcrisis en daaraan gekoppeld de onderbrekingen in de toeleveringsketens en het gebrek aan strategische autonomie in bepaalde sectoren, maakte andere waardeketens meer prioritair: 2e IPCEI batterijen, 2e IPCEI micro-elektronica, IPCEI next generation cloud infrastructure and services, IPCEI health...

Om goed voorbereid te kunnen inspelen op de onverwachte toekomstige opportuniteiten inzake IPCEI, besliste VARIO een afwegingskader voor IPCEI te ontwikkelen wat resulteerde in VARIO-advies 22: 'Strategische verkenning IPCEI Deel II: IPCEI-afwegingskader' (september 2021). In dit advies werden de informatie en de inzichten van de expert-rapporten m.b.t. de strategische analyse van de waardeketens gebundeld met de resultaten van bijkomende analyses uitgevoerd door de VARIO-staf (deskresearch, interviews en benchmarkanalyse).

In zijn advies 22 geeft VARIO aan dat het belangrijk is om eerst een duidelijk overkoepelend strategisch kader op te stellen, breder dan IPCEI. Het is tevens heel belangrijk om te kijken hoe IPCEI binnen het bestaande instrumentarium past – is IPCEI de beste keuze om een initiatief te ondersteunen? Een IPCEI-deelname moet volgens VARIO geanalyseerd worden aan de hand van het volgende afwegingskader:

Landen/regio perspectief:

- Sluit IPCEI aan bij de Vlaamse strategie en transities?
- Heeft Vlaanderen voldoende financiële draagkracht om aan te sluiten bij de IPCEI?
- Heeft de IPCEI voldoende impact voor Vlaanderen?

Bedrijfsperspectief:

- Hebben we bedrijven met unieke technologische expertise en innovatie?
- Hebben we voldoende kritische massa?
- Is er een marktfalen?
- Zijn onze bedrijven (en hun projecten) voldoende ingebed in een (internationaal) netwerk?
- Is er voldoende bereidheid om te (co-)investeren bij de Vlaamse bedrijven?

IPCEI - VOOR EEN GOED BEGRIP

Bij het lezen van de experten rapporten is het belangrijk om een goed begrip te hebben van wat IPCEI is. Daarom herhalen we in dit hoofdstuk een aantal elementen die belangrijk zijn en die reeds aan bod kwamen in het VARIO-advies 12 'Strategische verkenning IPCEI. Deel I: Waterstof' en VARIO-advies 22 'Strategische verkenning IPCEI. Deel II: afwegingskader. De invulling van IPCEI evolueert doorheen de tijd[5].

Waarvoor staat IPCEI?

'IPCEI's (Important Projects of Common European Interest) bieden een kans om het bestaande marktfalen te overwinnen en particuliere investeringen te stimuleren, er tegelijk voor zorgend dat het gelijke speelveld op de interne markt niet wordt verstoord.

Er zijn immers situaties waarin de markt alleen geen voldoende resultaten kan opleveren. Dit is het geval voor innovatieve, grensoverschrijdende, ambitieuze en complexe projecten, die een hoge mate van technologische, financiële of marktrisico's met zich meebrengen, coördinatie en samenwerking tussen meerdere marktdeelnemers binnen een waardeketen vereisen en positieve spill-over effecten genereren die verder reiken dan de investeerders. Deze projecten brengen vaak aanzienlijke risico's met zich mee, die particuliere investeerders niet zelf willen/kunnen dragen. Men spreekt dan van een marktfalen. In dergelijke gevallen kan overheidssteun van verschillende lidstaten die samenwerken noodzakelijk zijn om het marktfalen te ondervangen en de zgn. funding gap (zie sectie 3.3) *te dichten.*[6] In het licht van de beschikbare O&O&I-capaciteit kan marktfalen evenwel een hinderpaal zijn voor het bereiken van optimale uitkomsten en kan het om een aantal redenen zoals positieve externaliteiten, imperfecte en asymmetrische informatie en netwerkfalen tot een ondoelmatige uitkomst leiden.[7]

'IPCEI is een 'initiatief' van de Europese Commissie. De notie van IPCEI is opgenomen onder Art. 107(3)(b) TFEU als onderdeel van de regels m.b.t. staatssteun. De mededeling betreffende de IPCEI's werd reeds goedgekeurd in 2014, maar werd tot voor kort slechts heel beperkt gebruikt. IPCEI is zelf geen steunkader en de EC voorziet geen financiële ondersteuning in de context van IPCEI's - het betreft een specifieke rechtsgrondslag voor de EC om staatssteun verenigbaar te verklaren met de interne markt. IPCEI betreft dus enkel de toelating aan de lidstaten om de beperking die Europa oplegt wat het percentage staatssteun aan de (private)actoren betreft, te overschrijden. Een onderneming kan financiering aanvragen voor verschillende deelprojecten van een IPCEI in verschillende lidstaten van de EU. De goedkeuring van de EC is nodig omdat er mogelijks grote marktverstorende effecten zich kunnen voordoen'.[8]

[5] 25 november 2021 was er een update van de mededeling betreffende. IPCEI: Nieuwe staatssteunregels voor Important Projects of Common European Interest | VLEVA

[6] Zie VARIO-advies 12 'Strategische verkenning Imortant Projects of Common European Interest (IPCEI). Deel I: Waterstof' pagina 12-13.

[7] Mededeling van de commissie – kaderregeling betreffende staatssteun voor onderzoek, ontwikkeling en innovatie (2014/C 198/01) sectie 4.2.1 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52014XC0627(01)&from=NL

[8] Zie VARIO-advies 12 'Strategische verkenning Imortant Projects of Common European Interest (IPCEI). Deel I: Waterstof' pagina 12-13.

Type IPCEI-projecten

Drie 'type' projecten zijn mogelijk[9]:

- ***Art 22. O&O&I-projecten:*** *O&O&I-projecten moeten bijzonder innovatief zijn of qua O&O&I aanzienlijk toegevoegde waarde opleveren in het licht van de huidige stand van de techniek in de betrokken sector.*
- ***Art. 23.*** *First Industrial Deployment –* ***FID****: Projecten die een* ***eerste industriële toepassingen*** *omvatten, moeten de ontwikkeling mogelijk maken van een nieuw product of een nieuwe dienst met een sterke onderzoeks- en innovatiecomponent en/of ontwikkeling van een fundamenteel innovatief productieproces. Regelmatige bijwerkingen zonder innovatieve dimensie van bestaande faciliteiten en de ontwikkeling van nieuwe versies van bestaande producten kwalificeren niet als belangrijke projecten van gemeenschappelijk Europees belang. FID-projecten kunnen dus enkel in combinatie met een O&O-project.*
- ***Art. 25. Infrastructuurprojecten in de sectoren milieu, energie, vervoer, gezondheid of digitalisering*** *(voor zover ze niet onder art. 22 en 23 vallen) moeten hetzij van groot belang zijn voor de strategie van de Unie op het gebied van milieu, klimaat, energie (met inbegrip van de voorzieningszekerheid), vervoer, gezondheid, industrie of digitalisering, hetzij een aanzienlijke bijdrage leveren tot de interne markt, onder meer voor die specifieke sectoren, en kunnen na aanleg worden ondersteund tot zij volledig operationeel zijn.*

Voorwaarden voor IPCEI-projecten

'*IPCEI betreffen transnationale projecten van voor de EU strategisch belang. De projectsteun moet een duidelijke bijdrage leveren aan economische groei, banen en concurrentievermogen van de EU. Een IPCEI-project moet aan twee voorwaarden voldoen: (1) nut hebben voor de competitiviteit van de EU en (2) marktfalen opvangen. Projecten moeten aan de volgende voorwaarden voldoen[10]:*

- *Bijdragen aan strategische EU-doelstellingen;*
- *Meerdere lidstaten moeten er bij betrokken zijn;*
- *De begunstigden ervan moeten ook voor particuliere financiering zorgen;*
- *Het project moet positieve overloopeffecten in de hele EU opleveren;*
- *Project moet bijzonder ambitieus zijn in termen van onderzoek en innovatie (d.w.z. moet verder gaan dan wat over het algemeen als 'state-of-the-art' in betrokken sector geldt.*

Het betreft dus geen massaproductie of commerciële activiteiten. Steun aan IPCEI-projecten kunnen marktverstorende elementen omvatten. Daarom is het belangrijk dat aan bovenvermelde voorwaarden voldaan wordt.[11]

[9] Zie ook: Europese Commissie – mededeling van de commissie; Criteria voor de beoordeling van de verenigbaarheid met de interne markt van staatssteun ter bevordering van de verwezenlijking van belangrijke projecten van gemeenschappelijk Europees belang (2021) 8481 final). https://eur-lex.europa.eu/resource.html?uri=cellar:c6681395-4ded-11ec-91ac-01aa75ed71a1.0007.02/DOC_1&format=PDF

[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6705

[11] Zie VARIO-advies 12 'Strategische verkenning Imortant Projects of Common European Interest (IPCEI). Deel I: Waterstof' pagina 13-14.

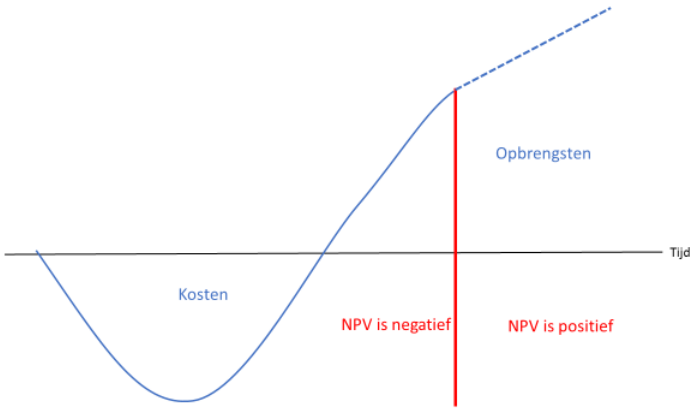
Cofinanciering en funding gap

De projectsteun ontvangen van de lidstaten vormt een aanvulling op de private investeringen die de bedrijven ondernemen; er wordt namelijk een zeer groot engagement voor cofinanciering gevraagd van de private actoren.

Er moet ook een zogenaamde 'funding gap'[12] *(zie Figuur 1) zijn. Op het einde van het project mag dit nog niet winstgevend zijn; de projectkosten moeten ruimer zijn dan de inkomsten binnen een bepaalde tijdsperiode. M.a.w. er moet een negatieve NPV (net present value) of negatieve netto contante waarde zijn. De funding gap komt overeen met het verschil tussen de negatieve en positieve NPV waarbij de Europese Commissie de steun wenst te beperken tot wat minimaal vereist is om het project te laten doorgaan, dus om de negatieve NPV tot nul te brengen. Dit dient ter verantwoording voor de toelating voor hogere staatssteun door de lidstaten. De staatssteun van de lidstaten mag maximaal 100% van de funding gap omvatten*[13] (voor meer informatie hoe de IPCEI-maatregel ingevuld wordt door Vlaanderen verwijzen we graag naar sectie 3.6).

Bij het notificatieproces van de bedrijven bij de Europese Commissie voor deelname aan IPCEI (zie sectie 3.5) vormt de funding gap oefening een belangrijk onderdeel.

Figuur 1: Voorstelling funding gap



Spillover-effecten

Daarnaast is er ook de specifieke vereiste van spill-overs, met de bedoeling om een deel van de resultaten en kennis ruimer te delen met het ecosysteem en de maatschappij. De bedrijven krijgen de mogelijkheid voor een verruiming van staatsteun, maar hiertegenover staat een engagement voor een bredere disseminatie en deling van kennis. Bij het notificatieproces moeten bedrijven duidelijk de spillovers weergeven.

[12] proces IPCEI-Hydrogen en stavaza sep20 update maart21_EDC-MS (2).pdf
[13] Zie VARIO-advies 12 'Strategische verkenning Imortant Projects of Common European Interest (IPCEI). Deel I: Waterstof' pagina 14

Meerwaarde van deelname aan IPCEI

In de context van de oproep rond de waterstof IPCEI werd door VLAIO het volgende gecommuniceerd[14]; '*Een deelname aan een IPCEI met notificatie is een interessante optie voor bedrijven bij:*

- *O&O&I-projecten met een omvang die ruimer is dan de maxima in de vrijstellingsverordening (20 miljoen euro steun per project bij onderzoek);*
- *Investeringen in milieu, energie of transport met een omvang die ruimer is dan de maxima in de vrijstellingsverordening (15 miljoen euro steun per project bij milieuprojecten);*
- *FID gekoppeld aan een innovatietraject: mogelijkheid voor financiering activiteiten die niet steunbaar zijn in de klassieke staatsteunregels'.*

Het meest vernieuwende aspect van IPCEI is de mogelijkheid om FID te steunen bij projecten met een belangrijke innovatiecomponent. De andere twee types projecten - O&O&I-projecten en investeringen voor milieu, energie, vervoer, gezondheid of digitalisering - kunnen ook gesteund worden onder de gewone staatssteunregels. IPCEI laat wel een ruimere invulling toe maar de activiteiten zijn op zich niet verschillend van wat anders mogelijk is.[15] Een andere belangrijke meerwaarde van een IPCEI-deelname is dat je als bedrijf deel uitmaakt van een strategische Europese waardeketen.

Er zijn echter ook een aantal specifieke vereisten verbonden aan een directe deelname aan IPCEI via notificatie. In sectie 3.3. werd reeds het belang voor spillover-effecten aangehaald. Hierbij is het expliciet de bedoeling om een deel van de resultaten en kennis ruimer te delen met het ecosysteem en de maatschappij. Voor investeringen voor milieu, energie, vervoer, gezondheid of digitalisering zijn ook non-exclusiviteit en toegang aan derden een vereiste. Daarnaast is de notificatie-procedure voor de bedrijven bij een IPCEI-deelname zeer veeleisend.[16]

Indirecte deelname (spillover groep)

IPCEI betreft grote uitdagende projecten met een hoog marktfalen en groot financieel risico. Deelname aan een IPCEI betreft een intensieve notificatie-procedure voor de bedrijven en vergt substantiële cofinanciering.

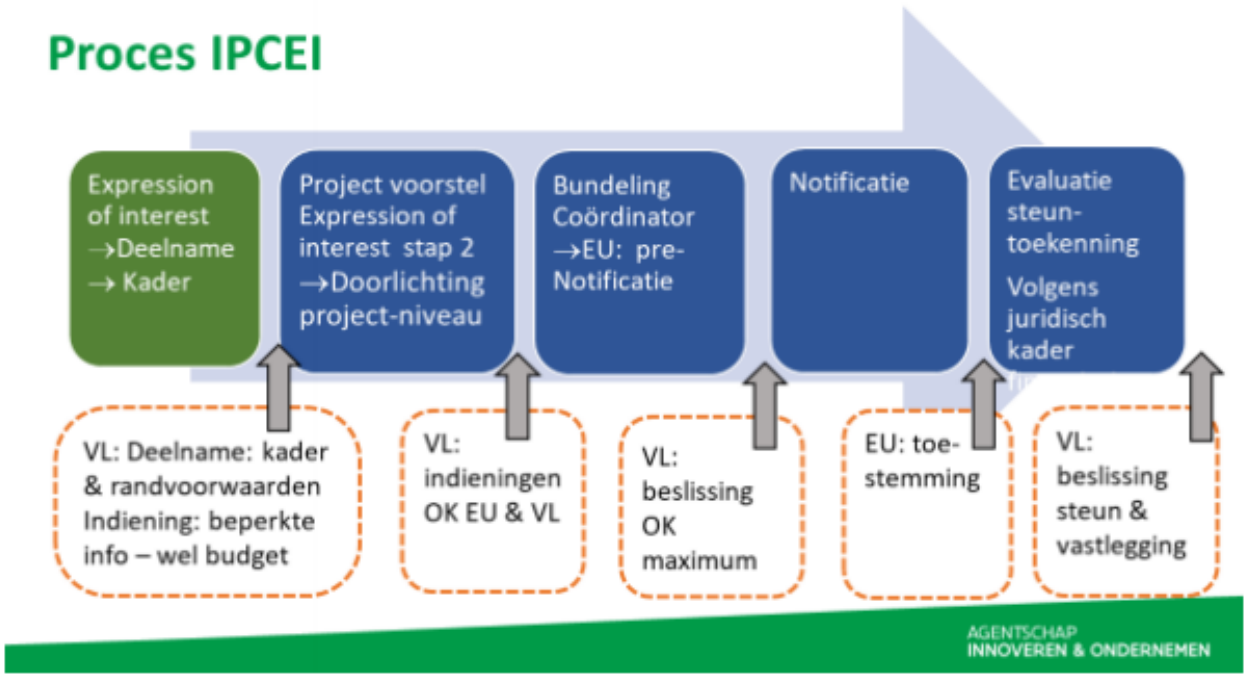
Om toch aan te sluiten bij het Europese netwerk en de strategische waardeketen zonder een notificatie-procedure te doorlopen kunnen bedrijven een indirecte deelname aan IPCEI overwegen. Activiteiten zoals O&O&I-projecten en milieu-, energie-, vervoer-, gezondheids- en digitaliseringsprojecten kunnen daarbij dan binnen het reguliere steunkader ondersteund worden (let wel, dit kan niet voor FID).

Procesverloop IPCEI

Het procesverloop van een IPCEI beschrijven is een moeilijke oefening, dit omdat er niet één vast procesverloop is. De lidstaten kunnen een aantal elementen binnen dit proces vrij invullen. In Figuur 2 wordt het procesverloop voor de IPCEI waterstof weergegeven. Voor een gedetailleerde beschrijving verwijzen we graag naar VARIO-advies 22.

[14] Nota kader IPCEI: IPCEI en deelname Vlaanderen (07/03/2020) https://www.vlaio.be/nl/media/1644
[15] Nota kader IPCEI: IPCEI en deelname Vlaanderen (07/03/2020) https://www.vlaio.be/nl/media/1644
[16] Nota kader IPCEI: IPCEI en deelname Vlaanderen (07/03/2020) https://www.vlaio.be/nl/media/1644

Figuur 2: Procesverloop IPCEI waterstof (vanaf de OIB – EOI)



Bron: IPCEI-hydrogen: proces en stand van zaken (04/09/2020, update 07/03/2020)[17]

Beleids- en financieringslandschap Vlaanderen

De beleidsvoorbereidende rol van het departement EWI

Het departement EWI staat in om het IPCEI-verhaal in te bedden in het Vlaams industriebeleid (o.a. smart specialisation strategy). Daarbij is het belangrijk om te kijken wat subsidies aan één bedrijf (of een beperkt aantal bedrijven) kunnen bijdragen aan de bredere economie (spillover effecten).

Afhankelijk van het technologiedomein van de IPCEI kan het departement EWI hiervoor in overleg treden met de verticale departementen bv. MOW, OMG… Het departement EWI legt ook op Europees vlak de linken tussen de verschillende initiatieven; bv. Horizon Europe, SET[18]-plan enz. in de context van waterstof.

De beleidsuitvoerende rol van VLAIO

Zoals aangegeven zijn er drie type projecten mogelijk binnen IPCEI. De invulling van deze projecten aan de hand van instrumenten gebeurt door de lidstaten/regio's zelf. De steun vanuit Vlaanderen wordt (tot nu toe) **beperkt tot 50% van de funding gap voor alle projecttypes**. In de communicatie vanuit VLAIO wordt aangegeven dat '*voor verschillende IPCEI's de modaliteiten evenwel kunnen* verschillen'[19].

[17] proces IPCEI-Hydrogen en stavaza sep20 update maart21_EDC-MS (1).pdf
[18] Strategic Energy Technology Plan https://ec.europa.eu/energy/topics/technology-and-innovation/strategic-energy-technology-plan_en
[19] Nota kader IPCEI: IPCEI en deelname Vlaanderen (07/03/2020) https://www.vlaio.be/nl/media/1644

- **Art. 22. O&O&I-projecten**: Vlaanderen heeft beslist om tot maximaal 50% van de funding gap te subsidiëren. De beslissingen worden genomen door het Fonds voor Innoveren en Ondernemen bij VLAIO.
- **Art. 23. First Industrial Deployment (FID)-projecten**: Vlaanderen heeft beslist om een FID-project (in het kader van de IPCEI-hydrogen) te financieren aan de hand van een subsidie. Hiervoor is een beslissing van de Vlaamse Regering nodig.
- **Art. 25. Milieu-, energie-, of mobiliteitsprojecten**: Vlaanderen heeft beslist om een art. 25-project (in het kader van de IPCEI-hydrogen) te financieren aan de hand van een subsidie. Ook hiervoor is een beslissing van de Vlaamse Regering nodig.

Er wordt momenteel in opdracht van VLAIO een project uitgewerkt 'Realising the full potential of IPCEI Hydrogen for Flanders' recovery and transition'[20] waarbij nagegaan wordt hoe een deelname aan IPCEI maximaal kan ingezet worden voor de transformatie in Vlaanderen (het instrumentarium dat gebruikt wordt voor IPCEI komt hier ook aan bod).

Zoals reeds werd aangegeven is het belangrijk dat een FID-project gekoppeld is aan een O&O&I-project. Een FID-project zonder O&O&I-project kan niet (een O&O&I-project zonder FID-project kan eventueel wel maar geniet niet echt de voorkeur; omdat deze ook terecht kunnen in het reguliere O&O-steunkanaal). Milieu-, energie-, vervoer-, gezondheids- of digitaliseringsprojecten kunnen wel zonder O&O- of FID-project. Voor meer informatie over de modaliteiten in het kader van de waterstof-IPCEI verwijzen we graag naar de VLAIO-communicatie[21].

Ook bij VLAIO wordt nagegaan wat subsidies aan één bedrijf/een beperkt aantal bedrijven kunnen bijdragen aan de bredere economie (spillover effecten). Voor de IPCEI-batterijen werden bijvoorbeeld ook harde valorisatie-eisen gezet door VLAIO.

Oorsprong Vlaamse middelen voor financiering IPCEI

De batterijen-IPCEI betreft een O&O&I-project in combinatie met FID-project. De projecten worden gefinancierd via reguliere middelen uit het Fonds voor Innoveren en Ondernemen.

De waterstof-IPCEI betreft zowel O&O&I-projecten, FID-projecten en milieu-projecten (art. 25-projecten), als combinaties ervan in eenzelfde project. Het is voorzien dat alle financiering vanuit de Europese relancemiddelen (RRF[22]) komt.

De toekomstige IPCEI m.b.t. micro-elektronica 2[23] en next generation cloud infrastructure and services[24] waarvoor in het voorjaar 2021 een EOI is gelanceerd bij FOD-economie zal enkel de combinatie O&O&I-projecten en FID-projecten omvatten (dus geen art. 25-projecten). Voor micro-elektronica zullen de middelen afkomstig zijn uit de (Europese) relancemiddelen, voor de IPCEI rond next generation cloud infrastructure and services is dit niet het geval.

Voor toekomstige IPCEI's is het onduidelijk van waar de mogelijke financiering zou komen.

[20] In het kader van het EU Technical Support Instrument.
[21] VLAIO - Kader deelname Vlaanderen in IPCEI-hydrogen (17/07/2020)
[22] Recovery and Resilience Facility https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
[23] https://economie.fgov.be/nl/themas/ondernemingen/projectoproepen/europese-ipcei-projecten/belangrijk-project-van-0
[24] https://economie.fgov.be/nl/themas/ondernemingen/projectoproepen/europese-ipcei-projecten/belangrijk-project-van-1

Rol van de federale overheid

In sectie 4.5 wordt het procesverloop voor een IPCEI binnen België beschreven. Daar werd reeds in detail ingegaan op de coördinerende rol die FOD-economie (kmo, middenstand en energie) opneemt in dit (complexe) proces.

Voor de IPCEI waterstof werd een deel van de investeringsprojecten (art. 25) via de federale overheid ondersteund (FOD economie, kmo, middenstand en energie). Tevens was het bij de oproep tot EOI rond next generation cloud infrastructure and services in het voorjaar 2021 ook mogelijk om projecten in te dienen (O&O- en FID-projecten) die betrekking hebben op de federale bevoegdheden (FOD Beleid en Ondersteuning).

ANALYSE VAN DE WAARDEKETEN CYBERSECURITY IN HET KADER VAN IPCEI (IMPORTANT PROJECTS OF COMMON EUROPEAN INTEREST)

SEPTEMBER 2022

Inhoud

1. Situering

Ulrich Seldeslachts, LSEC (Leaders in Security VZW), heeft in opdracht van VARIO een strategische analyse uitgevoerd van de waardeketen cybersecurity voor Vlaanderen. Daarbij werd gevraagd om een mapping te maken van de waardeketen en de actoren in deze waardeketen, om een SWOT-analyse uit te voeren en om een aantal aanbevelingen te formuleren.

De volledige analyse past in een groter geheel van '*een strategische verkenning en analyse van de sterktes en opportuniteiten die er zich voor Vlaanderen stellen voor de verschillende mogelijke Important Projects of Common European Interest (IPCEI's).*' De invalshoek van de oefening betreft O&O&I-actoren actief in de cybersecurity-waardeketen. Voor deze analyse heeft LSEC deskresearch gedaan, interviews uitgevoerd (voor lijst geconsulteerde personen zie bijlage 1) en voortgebouwd op hun expertise. Het resultaat is een onafhankelijk experten rapport. Vervolgens heeft VARIO via een validatieworkshop feedback en aanvullende informatie verzameld (voor lijst met deelnemers zie bijlage 2).

De VARIO-staf heeft steunend op het experten rapport van LSEC en de informatie uit de validatieworkshop voorliggend samenvattend rapport gemaakt.

2. Scope van Cybersecurity voor deze strategische analyse

Cybersecurity is het beveiligen van gegevens, transacties, systemen, toepassingen, technologie, mensen, producten en netwerken tegen digitale aanvallen. We hanteren in dit document een brede scope omwille van het rijke aanbod van cybersecurity-diensten en technologieën. Hierop zijn twee uitzonderingen, die we hieronder toelichten.

2.1. Data protection en privacy

Gegevensbescherming behoort tot het domein van Cybersecurity . Het afschermen en beveiligen van systemen en omgevingen waarin gegevens worden bewaard of bewerkt, maken deel uit van het informatiebeveiligingsbeleid. Persoonsgegevens worden sinds de Algemene Verordening voor Gegevensbescherming (AVG – GDPR) verwacht om voldoende beschermd te worden. De wetgeving en de bijhorende afdwingbaarheid zijn belangrijke drijfveren voor organisaties om zich beter te wapenen tegen mogelijk gegevensverlies. Verschillende bedrijven hebben zich gespecialiseerd in adviesverlening, praktische invulling en ontwikkelingen van toepassingen om de AVG – GDPR afdoende te kunnen ondersteunen. Data protection en privacy worden daarom meegenomen in de scope van Cybersecurity, maar dit beperkt zich tot ondersteuning en technische ontwikkelingen die privacy mogelijk maken (Privacy Enhancing Technologies – PETs). Er wordt niet dieper ingegaan op de juridische kant, de sociale impact en beleidsontwikkelingen hieromtrent. (informatie uit experten rapport LSEC)

2.2. Distributed ledger technologieën

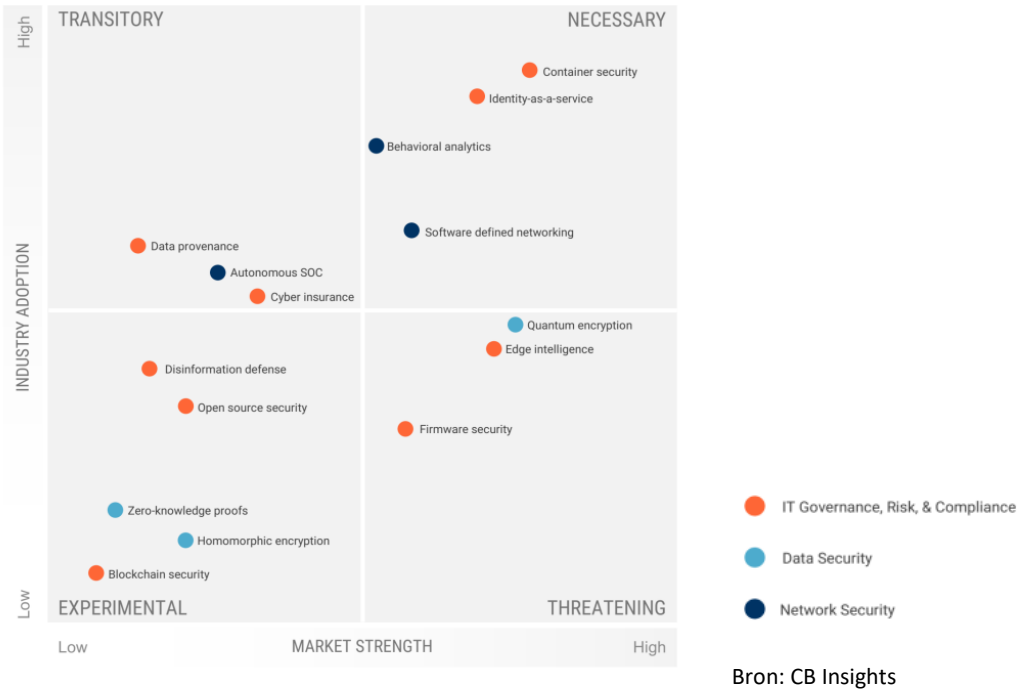
We merken nog op dat hoewel Distributed Ledger Technologieën (DLT) zoals Blockchain intensief gebruik maken van Cybersecurity technologie, zoals cryptoschema's en toegangscontrole, ze niet zijn opgenomen in deze studie. (informatie uit experten rapport LSEC)

3. Tendensen in Cybersecurity

Zonder exhaustief te willen zijn worden hieronder de belangrijkste tendensen meegegeven die een impact hebben op de evolutie van Cybersecurity. Ze zijn essentiële aandachtspunten en vormen tegelijk opportuniteiten voor onderzoek, ontwikkeling, innovatie en economie. (extract experten rapport LSEC)

- ***Het aantal Cloud toepassingen neemt toe:***
  Cloud biedt fantastische mogelijkheden voor schalen, verdelen van gegevens en berekeningen, mogelijkheden om snel te starten (en te stoppen), economische verantwoord aan te passen en biedt garanties voor continuïteit en resilience en in vele gevallen een betere toepassing van cybersecurity. Maar cloud levert ook uitdagingen op het vlak van sleutelbeheer, het distribueren van confidentiële en persoonsgegevens (op publieke systemen, buiten Vlaanderen, buiten België, buiten Europa), soms niet versleuteld op systemen die beheerd worden door Chinese of Amerikaanse bedrijven. Met overheden die zich toegang kunnen verschaffen tot die systemen worden continu vragen opgeroepen m.b.t.de betrouwbaarheid en de noodzaak om soeverein te kunnen beschikken over gegevens in de cloud (zie Figuur 1 container security, Identity as a Service).
- ***Steeds meer toestellen en systemen worden verbonden (IoT/IIoT - Cyber Physical Systems)****: wasmachines, televisieschermen, sloten, bewakingscamera's, domotica, geluidssystemen … maar ook industriële machines (IIoT), medische toepassingen, wagens en andere voertuigen[1] en slimme meters.*
- ***De eenvoud om kwetsbaarheden van cybersecurity te exploiteren neemt toe****:*
  toenemend aantal mogelijkheden om zwakheden van systemen te kunnen exploiteren, toenemend aantal middelen om die zwakheden te kunnen exploiteren en toenemend gemak om die middelen te kunnen inschakelen (gemakkelijker te vinden, te gebruiken, aan te passen, …), toenemend aantal zwakheden die worden gevonden, toenemend aantal systemen die geconnecteerd worden (in Figuur 1 Autonomous SOC, Disinformation Defense, Zero-knowledge) …

Figuur 1: Emerging trends in cybersecurity in 2019



Bron: CB Insights

[1] Cfr. Zie experten rapport m.b.t. de analyse van de waardeketen van Industrial IoT, Smart Health en Clean, Connected and Autonomous Vehicles (in het kader van IPCEI).

- ***Virtualisatie van systemen en software gestuurde oplossingen (SDN) brengt nieuwe kwetsbaarheden**:*
  Deze maken het onder meer makkelijker om te schalen en aanpassingen snel door te voeren. Maar het kan het ook makkelijker maken om componenten toe te voegen die onder meer achterpoortjes mogelijk maken om ze vervolgens ongezien terug te verwijderen.
- ***Quantum en high performance computing hebben drastische impact op de beschikbare rekenkracht:***
  De verdere groei van beschikbare rekenkracht, in het geval van quantum computing met een sprong van meerdere grootteordes, is een bedreiging voor de huidige aanpak van Cybersecurity in het algemeen en voor de state-of-the-art versleutelingsalgoritmes in het bijzonder. Systemen met beperkte versleutelingscapaciteit (zoals smart health, automotive, IoT, IIoT en edge toestellen) zijn per definitie uitgesproken kwetsbaar. De uitdaging is dan ook om die systemen voor te bereiden op die nieuwe bedreiging (in Figuur 1 Quantum encryption, Homomorphic encryption).
- ***AI – Artificial Intelligence en automatisering bieden nieuwe opportuniteiten:***
  Machine Learning, Behavioral Analytics, Neural Networks, Natural Language Processing … zijn technologieën in volle ontwikkeling, waarbij veel wordt verwacht van cybersecurity. Meer specifiek zijn er verwachtingen m.b.t. het ondersteunen in het ontdekken van kwetsbaarheden, het ontdekken van mogelijke incidenten (ontdekken van malware, malafide transacties, virtuele identiteiten op systemen die niet stroken met de verwachtingen, ….) maar ook sneller kunnen reageren op mogelijke incidenten – op basis van verschillende al-dan-niet gerelateerde detecties (soortgelijk aan de manier waarop auto's vandaag ons ondersteunen met collusion avoidance, te snel naderen bij een stilstaan voertuig, sneller reageren dan de bestuurder mo op de rem te staan…) (in Figuur 1 Autonomous SOC, Behavioral analytics)
- ***Ubiqitous computing vereist betere beveiliging van eindgebruikers en netwerken**:*
  Sinds de transitie naar 3G/4G op publieke plaatsen en wifi in thuis- en bedrijfsnetwerken zijn we ons niet meer bewust wanneer we internet gebruiken. 5G en nieuwere vormen van communicatie zullen die trend bestendigen. Het resultaat is dat we steeds minder zichtbare verdedigingsmechanismen centraal kunnen opbouwen, dat we afhankelijker worden van de verdediging die wordt geboden door de "endpoints" en de netwerken waaraan ze verbonden zitten.
- ***High Performance Microcomputing en Data-opslag bieden nieuwe mogelijkheden**:*
  De steeds toenemende vormen van miniaturisering van performante processoren en toenemende capaciteit van lokale gegevensopslag bieden nieuwe mogelijkheden voor decentrale Cybersecurity. Verschillende Cybersecurity technologieën zoals firewalls, intrusion detection, endpoint protection, network inspection, whitelisting, encryptie … kunnen inderdaad ook decentraal worden toegepast. In combinatie met virtualisering en software gestuurde oplossingen, kunnen ze ook sneller worden ingezet. (Figuur 1 Data provenance)
- ***Intelligence en Situational Awareness worden steeds belangrijker:***
  Om snel te kunnen reageren op mogelijke bedreigingen worden naast technologie, expertise, processen en methodologie ook informatie, intelligence en inzichten steeds belangrijker. Eens het bekend is dat er kwetsbaarheden of specifieke bedreigingen zijn, is het een race tegen de tijd om ze zo snel mogelijk op een gepaste manier in quarantaine te plaatsen of bijkomende beschermingsmaatregelen te nemen. Dit om te vermijden dat ze verdere verspreiding mogelijk maken. Cyber Threat Intelligence en Situational Awareness worden steeds belangrijker. In "Fusion Centres" worden gegevens van verschillende bronnen (bijvoorbeeld camerabewaking, toegangscontrole en cybersecurity intelligence) samengevoegd om een beter zicht te krijgen op mogelijke bedreigingen. (in Figuur 1 Autonomous SOC, Disinformation Defense
- ***Human in the Loop blijft belangrijke schakel:***
  Zelfs al is de digitale transformatie afgerond, zelfs al worden alle processen geautomatiseerd, zelfs al staat de kunstmatige intelligentie eindelijk op punt, ook dan moet er met de menselijke factor rekening gehouden worden. Zowel tijdens het design en de ontwikkeling als bij de operationele

werking is het van belang te beschikken over voldoende opgeleide en ervaren medewerkers die als experten en supervisors werken en controle en overzicht behouden over de verschillende bestaande technologische middelen.

4. Waardeketen cybersecurity

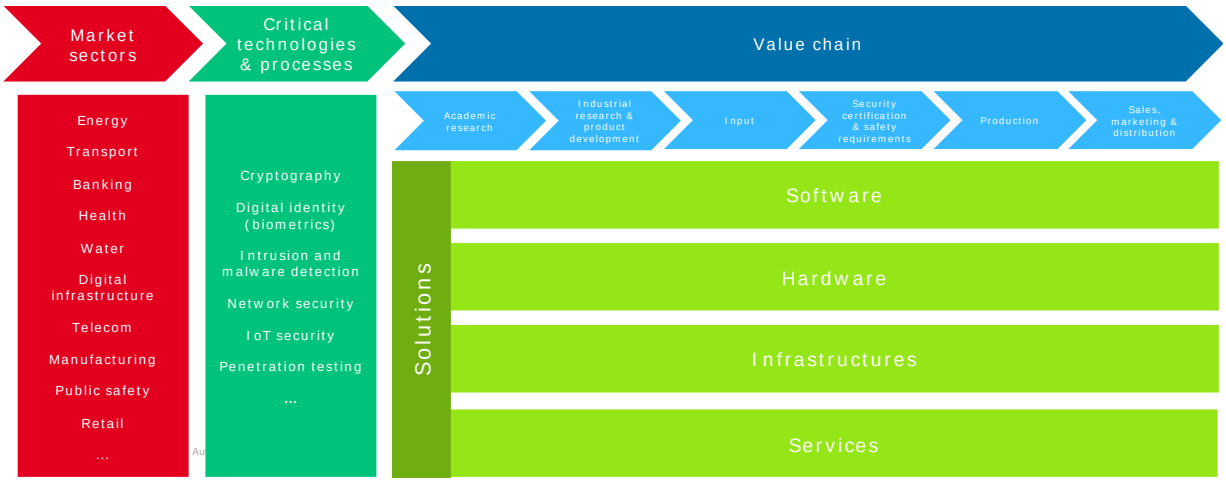
Het Strategic Forum on IPCEI heeft een beschrijving gemaakt van de Europese cybersecurity waardeketen. De resultaten van deze Europese oefening worden gebruikt als startpunt om de Vlaamse waardeketen te bekijken. In dit hoofdstuk wordt hier dieper op ingegaan.

4.1. Europese waardeketen Cybersecurity

De Europese waardeketen rond Cybersecurity bevat cybersecurity (1) software, (2) hardware, (3) infrastructure and (4) service solutions (zie Figuur 2). In het rapport[2] (uitgevoerd door Technopolis group) wordt het volgende meegegeven: '*De waardeketen heeft zijn uitgangspunt in marktsectoren. De toepassingscontext is van groot belang omdat de beveiligingsvraagstukken speciaal zijn voor elke sector en vanwege de grote verschillen in maturiteit tussen sectoren. Voor elke marktsector spelen andere kritische technologieën en processen, zoals cryptografie, inbraak- en malwaredetectie en IoT-beveiliging*.

De marktsectoren, kritieke technologieën en processen brengen op hun beurt software-, hardware-, infrastructuur- en dienstenoplossingen voor cybersecurity voort (bv. biometrische identificatie, encryptie, software om frauduleuze activiteiten op te sporen). Oplossingen krijgen vorm binnen waardeketens, die grosso modo bestaan uit: (1) academisch onderzoek, (2) industrieel onderzoek en productontwikkeling, (3) input, (4) beveiligingscertificering en veiligheidseisen, (5) productie en (6) verkoop, marketing en distributie.'

Figuur 2: Europese Cybersecurity waardeketen



Bron: Technopolis Group

4.2. Vlaamse waardeketen Cybersecurity

Hieronder wordt een beschrijving opgenomen van de Vlaamse waardeketen Cybersecurity zoals opgemaakt door LSEC en aangevuld met informatie uit de validatieworkshop.

De Cybersecurity waardeketen is traditioneel vergelijkbaar aan waardeketens in Informatie-technologie en in Security; waar haar oorsprong ligt.

De waardeketen vandaag bestaat nog steeds voornamelijk uit een reeks van technologie-aanbieders die producten en diensten via een distributeur-reseller-integrator-kanaal tot bij de eindgebruikers brengen. De selectie van de technologieën wordt daardoor vaak beperkt. De eindgebruiker-klant wordt vandaag benaderd door alle verschillende cybersecurity-actoren, en probeert voor zijn specifieke

[2] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

uitdagingen oplossingen te bekomen die kwaliteitsvol en betaalbaar, beheersbaar (hij moet kunnen beschikken over het juiste talent en middelen om ze te beheren), voldoende schaalbaar en toekomstgericht zijn.

De laatste jaren worden de Cybersecurity verschillende waardeschakels vaak onderbroken door een Software as a Service (SaaS), Platform as a Service (PaaS) of Infrastructure as a Service (IaaS)-model. Dit is een trend die zich in de komende jaren wellicht zal verder zetten. De disruptieve trend houdt in dat verschillende cybersecurity actoren proberen te bewegen naar meer toegevoegde waarde, wat voornamelijk inhoudt dat ze meer gepersonaliseerde diensten aanbieden die moeilijker te schalen zijn. (extract experten rapport LSEC). Andere trends die een invloed hebben op het landschap worden weergegeven in hoofdstuk 3.

4.2.1. Bedrijven die cybersecurity producten en diensten produceren en aanbieden

Er zijn verschillende startblokken in de waardeketen. In de context van deze studie worden de bedrijven die Cybersecurity producten en diensten produceren en aanbieden vooraan geplaatst. Het is moeilijk om een afgelijnde indeling te maken tussen het brede type bedrijven die actief zijn m.b.t. het produceren en aanbieden van cybersecurity producten en diensten. Er zijn namelijk verschillende dimensies:

- Ondernemingen die Cybersecurity-producten ontwikkelen/produceren en diensten aanbieden;
- Ondernemingen die Cybersecurity als enige business hebben of waar Cybersecurity onderdeel uitmaakt van hun portfolio;
- Ondernemingen die Cybersecurity-producten ontwikkelen of die producten ontwikkelen waar Cybersecurity heel belangrijk is;
- …

Dit betreft dus een ‘breed veld’ aan actoren.

4.2.2. Advies en systeemintegratoren

De rol van Cybersecurity systeemintegratoren en adviseurs is in de Vlaamse waardeketen van ontzettend belang. De gespecialiseerde bedrijven werven werknemers aan met een zekere Cybersecurity-expertise of leiden ze (verder) op. De bedrijven groeien mee met de verwachtingen en vraag in de markt, en het aanbod van experten vanuit opleidingscentra, van bij eindgebruiker-bedrijven of het buitenland. Ze bouwen en ontwikkelen een systematiek waarbij ze eindgebruiker-bedrijven helpen bij het identificeren van mogelijke Cybersecurity-uitdagingen (pentesting, vulnerability-assessments, testing …) en gaan systematisch proberen de mogelijke problemen weg te werken of aan te passen. Meestal begeleiden ze de klanten in de selectie van mogelijke manieren van aanpakken, technologie, oplossingen en het selecteren van processen en partners voor de verdere Cybersecurity . Vaak leveren ze een Chief Information Security Officer gedurende een bepaalde of onbepaalde tijd om de interne werking voor Cybersecurity te begeleiden en te organiseren. Vervolgens leveren ze ook diensten voor het dagelijkse beheer en de controle van de Cybersecurity in de vorm van Security Operations Centers, Incident Management of Managed Security Services. Vlaanderen is werkelijk een domein van integratie en adviesdiensten (extract experten rapport LSEC).

4.2.3. Distributeurs en wederverkopers

Distributeurs vervulden vroeger een belangrijkere rol in Cybersecurity, voornamelijk omdat veel producten gerelateerd waren aan toestellen zoals firewalls, intrusion detection and prevention … (machines die Cybersecurity functies verrichten). Sinds de afgelopen tien jaren, onder meer door de digitalisering en de ontwikkelingen van de cloud, zijn er ondertussen ook veel meer Cybersecurity-

toepassingen die zich in de cloud afspelen of oplossingen waarvoor de rol van de waarde van de distributeurs vervaagt. Distributeurs proberen zichzelf opnieuw uit te vinden, door in de waardeketen op te schuiven naar een rol als adviseur, integrator of managed security services provider (MSSP).

Hun toegevoegde waarde is zeker niet verdwenen, maar komt steeds vaker onder druk te staan. Nochtans zullen internationale verkopers blijven kiezen voor distributeurs en wederverkopers om het klantencontact te blijven onderhouden, om te dienen als logistiek centrum binnen de groep. De uitdagingen voor lokale afhandeling en ook lokale ondersteuning blijven nog steeds van belang. (extract experten rapport LSEC)

4.2.4. Telecom, mobiele communicatie, 5G en Internet Services Providers

Cybersecurity uitdagingen zijn voornamelijk het gevolg van intensief gegevensverkeer dat wordt mogelijk gemaakt door telecommunicatiediensten. Internet Services Providers (ISPs) zijn voor het overgrote deel mee geïntegreerd in het dienstenaanbod van de telecomoperatoren. Internet is vandaag voornamelijk de basis voor alle telecommunicatiediensten. Die transformatie heeft in de afgelopen jaren plaatsgevonden en zet zich steeds verder door. Nieuwe technologieën zoals 5G en Software Defined Networking bouwen daar verder op door. Communicatiedienstenleveranciers bieden vandaag telefonie over internet, in plaats van internet over telefonie.

Communicatiedienstenleveranciers zijn vaak ook belangrijke spelers in het beveiligen van de informatiestromen en het beheren van gegevens. Ze zijn niet alleen het kanaal waarlangs het internetverkeer verloopt, ze connecteren ook de verschillende eindpunten en verspreiden op die manier - als medium - de mogelijke malware en andere cyberbedreigingen.

In de afgelopen decennia zijn de verschillende operatoren geëvolueerd van louter dienstdoend internetverkeerkanaal en verkeersregelaar naar ontwikkelaars en exploitanten van inhoud en ook zelf dienstenleveraars die hun klanten begeleiden in hun data-uitdagingen, zowel opslag als beveiliging. Operatoren blijven ook in de toekomst belangrijke spelers in het ecosysteem. We zien hen terug als wederverkopers van oplossingen, als integratoren, als MSSP, als adviseurs en als eindgebruikers. (extract experten rapport LSEC)

4.3. Intermediairen

De intermediairen bestaan uit een reeks van organisaties die bedrijven en overheden bijstaan in de ontwikkeling en beheersing van Cybersecurity . Dit betreft o.a. bedrijfsfederaties, collectieve centra, speerpuntclusters, SOC's... Ze sensibiliseren, verzamelen en verspreiden praktijkervaringen, coördineren werkgroepen met leveranciers en eindgebruikers, begeleiden afspraken tussen overheden en industrie, organiseren acties ter verbetering van het algemene Cybersecurityniveau, organiseren netwerkmomenten rond gespecialiseerde onderwerpen, vormen drukkingsmomenten, begeleiden de marktontwikkeling en innovatie-ontwikkeling, verzamelen de gezamenlijke eigenschappen en uitdagingen en coördineren gezamenlijke acties ter ondersteuning van een respectievelijke sector, of belangengroep. (extract experten rapport LSEC)

4.4. Kennisinstellingen

Vlaanderen staat op het vlak van Cybersecurity vooral bekend om zijn wereldvermaarde experten, leidinggevend onderzoek en technologische ontwikkelingen. De universiteiten, hogescholen en SOC's staan in voor aanzienlijke O&O&I-activiteiten in Cybersecurity. Daarnaast zijn de universiteiten en hogescholen ook belangrijk voor het organiseren van opleidingen. Deze komen verder uitgebreid aan bod in hoofdstuk 5 Actoren.

4.5. Eindgebruikers; bedrijven en overheden

De uiteindelijke bestemming van Cybersecurity technologie zijn organisaties: bedrijven en publieke instanties.

Bedrijven

Bedrijven zijn de belangrijkste afnemer op vlak van volume en als aanjager van de leveranciers om hun noden en verwachtingen te definiëren.

- *Vlaanderen heeft maar een beperkt aantal (maar belangrijke lokale) technologie-ontwikkelaars die Cybersecurity-expertise ondersteuning lokaal kunnen gebruiken.* Dit maakt dat er maar een beperkt aantal afnemers zijn van belangrijke omvang.
  Het is ook zo dat de vraagzijde onevenwichtig is; slechts een beperkt aantal bedrijven bepaalt het grootste deel van de marktvraag. Grote bedrijven, binnen de meer Cybersecurity mature sectoren, beschikken relatief gezien over grote(re) budgetten om aan Cybersecurity te spenderen en hebben vaak ook meer interne middelen (extract experten rapport LSEC). Vlaamse bedrijven zijn echter in hoofdzaak KMO's.
- *Een hindernis voor verschillende Vlaamse Cybersecurity-technologie-ontwikkelaars is dat hun innovatieve oplossingen moeilijk ingang vinden bij Vlaamse bedrijven. Cybersecurity-experten wijzen erop dat Vlaamse technologiebedrijven het vaak moeilijker hebben om hun aanbod te laten landen in het Vlaamse industrieel netwerk. Bedrijven aarzelen om dergelijke investeringen te maken en vertrouwen blijkbaar onvoldoende dat Vlaamse technologiebedrijven voldoende kennis, expertise, ervaring, specialisatie of algemeen een afdoende oplossing zouden kunnen leveren voor hun uitdagingen.* (extract experten rapport LSEC). Tijdens de validatieworkshop wordt aangegeven dat in sommige landen (bv. Nederland) bedrijven bereid zijn om iets meer risico te nemen bij de aankoop van hun cybersecurity goederen en diensten.
- Het is echter belangrijk dat breder gekeken wordt dan alleen de technologie-ontwikkelaars. IIoT security ontwikkelingen kunnen namelijk ingezet worden in hoogtechnologische producten in bv. de gezondheidszorg, industrie enz. *Vlaanderen beschikt namelijk over unieke expertise van technologie, sectoren, en markten door technologische ontwikkelingen die plaatsvinden bij machinebouwers, in micro-elektronica, in consumentenelektronica, sensorsystemen, elektronica voor bedrijfstoepassingen en het toevoegen van communicatiemogelijkheden aan bestaande toestellen voor verschillende toepassingen.* (extract experten rapport LSEC)

Publieke (internationale) instellingen

Een aantal internationale instellingen zoals de EC, de Raad van Europa, het Europees Parlement, NATO, ESA, Eurocontrol … zijn in België gevestigd.

1) De aanwezigheid van internationale instellingen vergroot de afzetmarkt voor de aanbieders van Cybersecurity goederen en diensten. (experten rapport LSEC)
2) Daar tegenover staat dat er in België/Vlaanderen zelf, in vergelijking met de US, UK, Israël… geen intensieve samenwerking is tussen de 'intelligence services' en de innovatieleiders. Dit vormt een beperking voor onze innovatieleiders. (informatie validatieworkshop, zie ook sectie 7.2)

5. Vlaams Cybersecurity actoren

De Vlaamse cybersecurity waardeketen is opgebouwd uit een hele reeks actoren. Hieronder wordt een overzicht gegeven van de bedrijfsactoren, intermediairen en kennisinstellingen die een breed spectrum bestrijken en wijzen op de aanwezigheid van een rijk ecosysteem We verwijzen hier nog graag naar de scope van de studie die uitgevoerd is in het kader van IPCEI – important projects of common European Interest – namelijk O&O&I-actieve actoren. Daarnaast mag het belang van de eindgebruikers – bedrijven en overheden - niet onderschat worden.

Onderstaande informatie werd verzameld door LSEC in het kader van het experten rapport. Deze oplijsting werd aangevuld met informatie uit de validatieworkshop met externe experten.

5.1. Bedrijfsactoren

Er kunnen verschillende bedrijfsactoren geïdentificeerd worden binnen de waardeketen van Cybersecurity :

- Bedrijven die cybersecurity-producten en diensten produceren en aanbieden;
- Advies en systeemintegratoren;
- Distributeurs en wederverkopers;
- Telecom, mobiele communicatie, 5G en Internet Service Providers (ISP's).

Er zit echter wel overlap tussen de verschillende 'categorieën'; niet elke onderneming is exclusief aan één categorie toe te wijzen.

Bedrijven die cybersecurity producten en diensten produceren en aanbieden

Het is moeilijk om een afgelijnde indeling te maken tussen het brede type bedrijven die actief zijn m.b.t. het produceren en aanbieden van cybersecurity producten en diensten. Met onderstaande lijst is het de bedoeling om vooral de breedte van het veld aan te tonen. Het betreft een veelzijdige community.

Tabel 1: Overzicht Cybersecurity product- en/of diensten bedrijven (alfabetische volgorde)

ABLE AxsGuard	Lansweeper
Aloxy	MIXX
Atayapartners	Mr. Franklin
AXTRAX	nAuth
Awarity	Netcure
Awingu	Newtec
BA	NGRAVE
BARCO	NIKO
Belgian Mobile ID	NVISO
Ceeyu	NXP semiconductors
Cegeka	Nynox
Combell	OneSpan
CO-DEX.eu	Orange Cyberdefense
Connective	Outkept
Cranium	Phished
Crescent Option – Cloudgate	Play it
CSI	Resilient
Cyberminute	Rombit
Deepwatch	Scaled Access
eLimity	Sectricity

Engie Laborelec	Secudea
Excellium	SecureCodeWarrior
Firmalyzer	Secure IT
Fortinet	Secutec
G DATA Belgium	ShiftLeftSecurity
GDPRSquare	Sign2Pay
Guardsquare	Skyforce
Huawei Cybersecurity Transparency Centre	Skyline
Hypervault	STM
IBM	Synergics SpotIT
Infosentry	Sweepatic
Infradata	Televic
Intigriti	Toreon
IntrinsicID	Trustbuilder
IPMetro	Ubora
IS4U	UnifiedPost
Itsme	Westpole Benelux
Jarviss	Workline Global
Jimber	XMConsulting
Keysight	…

Bron: Informatie uit experten rapport LSEC aangevuld met informatie van VLAIO

Advies en systeemintegratoren

De rol van Cybersecurity systeemintegratoren en adviseurs is in de Vlaamse waardeketen van ontzettend belang. In onderstaande tabel wordt een overzicht gegeven:

Tabel 2: Overzicht van advies en systeemintegratoren (alfabetische volgorde)

Accenture	Master Labs
Alstom	NTT Group
Apogado	NVISO
ATOS	Orbid
Axias	Ordina
Cegeka	Phoenix Contaxt
Deloitte	Prodata
CapGemini	Proximus
Conxion	PwC
Cronos	RHEA
Devoteam	Savaco
Dilaco	Siemens
EASI	Simac
E&Y	Sopra Steria
Fuijtsu	Thales
Hapbit	Toreum
IBM Services	Tobania
I-Care	Van Roey
IKOS group	Xylos
KPMG Advisory	3it…

Bron: Informatie uit experten rapport LSEC

Distributeurs en wederverkopers

De distributeurs in Vlaanderen bestaan enerzijds uit Vlaamse ondernemers en anderzijds uit internationale groepen die zich door acquisities of als filialen in Vlaanderen zijn komen vestigen. Het zijn voornamelijk distributeurs die ook andere ICT-producten leveren. Enkele distributeurs houden er ook een specifieke focus op Cybersecurity op na (voorbeelden zoals InfraData, KappaData, Exclusive Networks, Arrow, Secutec, Switchpoint, Orange Cyberdefense ….). Veel distributeurs hebben (al dan niet) exclusieve overeenkomsten met Amerikaanse, Engelse, Israëlische technologieleveranciers. Ze kennen de lokale markt, de lokale kopers en hebben een vertrouwenspositie weten onderhouden in de afgelopen jaren. Soms voorzien ze ook bijkomende diensten zoals installatie en integratie. Slechts in beperkte mate hebben ze ook Vlaamse producten in hun portfolio van Cybersecurity-diensten. (extract experten rapport LSEC)

Tabel 3: Overzicht distributeurs en wederverkopers van cybersecurity goederen en diensten (alfabetische volgorde)

Abbakan – Ingram	Infradata
Arrow	KappaData
Copaco	SaasForce
DB Becton Dickonson	Secutec
DCB – Nuvias	Sertalink
Deltalink	Switchpoint
DSD	Techdata
Exclusive	**…**

Bron: Informatie uit experten rapport LSEC

Telecom, mobiele communicatie, 5G en Internet Services Providers

Operatoren zoals Proximus,Orange, Telenet en anderen hebben een uitgebreid aanbod aan beveiligingsdiensten. (extract experten rapport LSEC)

5.2. Intermediairen

De intermediairen bestaan uit een reeks van organisaties die bedrijven en overheden bijstaan in de ontwikkeling en beheersing van Cybersecurity . Ze nemen een belangrijke rol op in het Vlaamse Cybersecurity-landschap.

Er zijn slechts een paar intermediairen die Cybersecurity als primair onderwerp behandelen (LSEC, Cybersecurity Coalition, OWASP), en zich vervolgens richten naar verschillende sectoren. (extract experten rapport LSEC). Door de deelnemers van de validatieworkshop wordt dit zeker niet als een beperking binnen het ecosysteem aanzien. Voor bepaalde doelgroepen zijn ook andere intermediairen heel goed geplaatst om advies en begeleiding te bieden. Er werd aangegeven dat er vaak een aantal trekkende actoren zijn onder de intermediairen (bv. Agoria, Sirris, VOKA…) die dan vervolgens andere intermediairen ondersteunen om specifieke activiteiten en acties in bepaalde sectoren te initiëren.

In sectie 5.3 wordt ingegaan op de kennisinstellingen die academisch en toegepast onderzoek uitvoeren. Sommige van de intermediairen in Vlaanderen voeren echter ook toegepast onderzoek uit.

Tabel 4: Overzicht van intermediaire actoren actief in het domein van Cybersecurity (alfabetische volgorde)

Agoria	Flanders Make
BeCode.be	GAIA X Belgium
BeCommerce	IE.net
BELTUG	ISACA
Catalisti	LSEC

Centexbel	OWASP
Cybersecurity Coalition	Safeshops
Digital SME Association	SAI
DPOpro	The Beacon
ECSO	TLV
EEMA	Unizo
EFFRA	VBO
Essenscia Vlaanderen	VITO
Energyville	VOKA
Febelfin	Sirris
Feweb	Startups.Be
Flanders Food	**…**

Bron: Informatie uit experten rapport LSEC

5.3. Kennisinstellingen

Hieronder wordt een overzicht gegeven van het academisch en toegepast onderzoek aan de universiteiten, het toegepast onderzoek aan de hogescholen, het onderzoek aan de SOC's en de opleidingsmogelijkheden aan de kennisinstellingen. Dit overzicht is gebaseerd op het experten rapport van LSEC en aangevuld met additionele informatie uit de validatieworkshop.

In bijlage 3 worden de resultaten van een analyse van FRIS m.b.t. de O&O&I-activiteiten van (bepaalde) kennisinstellingen in cybersecurity (Flanders Research Information Space) uitgevoerd door EWI opgenomen.

5.3.1. Academisch en toegepast onderzoek aan universiteiten

De KU Leuven, UGent en VUB zijn verbonden aan het Onderzoeksprogramma Cybersecurity.

KU Leuven

In KU Leuven zijn er verschillende departementen en afdelingen actief in het domein Cybersecurity . Samen vormen ze de grootste en de oudste groep van Cybersecurity in het Vlaamse en Belgische onderzoekslandschap. De groepen bestaan uit:

- *DISTRINET[3]: afdeling van het departement Computerwetenschappen, met verschillende spinoffs, industriële samenwerkingen, Europese en andere internationale onderzoeksprojecten en een breed gamma aan Vlaamse projecten types SBO, TETRA, COOCK en ICON. DISTRINET heeft specialisaties in de domeinen van software-ontwikkeling en daaraan gerelateerde automatisatie, proces- en methodes gerelateerd aan security en privacy.*
- *COSIC[4]: afdeling van de het departement Electrotechniek, met verschillende spinoffs, industriële samenwerkingen, Europese en andere internationale onderzoeksprojecten en een breed gamma aan Vlaamse projecten types SBO, TETRA, COOCK en ICON. De groep beschikt over een uitgebreide expertise op het vlak van crypto, zowel naar de methodes die encryptie mogelijk maken als de implementatie, de evaluatie en het gebruik ervan..*
- *CITIP[5]: het Centrum voor Informatie Technologie en Intellectuele Eigendom (Property) is een groep van juristen die zich hebben toegelegd op ontwikkelingen in informatietechnologie, om op die manier te onderzoeken op welke manier de technologie een impact heeft op de wetgeving, en wetgeving dient te veranderen, of toegepast kan worden ter ondersteuning van technologie of ter bescherming van de maatschappij en haar burgers en rechtspersonen*

[3] https://distrinet.cs.kuleuven.be/
[4] https://www.esat.kuleuven.be/cosic/
[5] https://www.law.kuleuven.be/citip/en

- *Ook andere groepen en departement werken aan Cybersecurity, maar zijn minder voltallig dan de bovenstaande: KU Leuven Industriële Wetenschappen Hasselt en Leuven, Bedrijfseconomie, Werktuigkunde, Psychologie, …*

VUB

- *Het Cyber and Data Security Lab[6] van de VUB brengt de expertise van de onderzoeksgroep van Law, Science, Technology & Society (LSTS) als onderdeel van de Rechten en Criminology Faculteit. De groep brengt een belangrijke groep onderzoek gerelateerd aan privacy en security en criminologie bij mekaar, die baanbrekend werk verrichten op het vlak van de respectievelijke domeinen.*
- *De Artificial Intelligence Research Group brengt de expertise van multi-agent systems, reinforcement learning, evolutionary & hybrid AI, cognitive AI, computational creativity and knowledge representation and reasoning bij mekaar om toe te passen in een reeks van Cybersecurity uitdagingen[7]*
- *Het SOFT Lab van VUB beschikt over een reeks expertises rond Programming Technology en System and Software Engineering, en is actief in een aantal Europese en lokale Cybersecurity technologie-projecten en ontwikkelingen.*
- *Het SMIT[8] onderzoekt de ontwikkelingen en uitdagingen van nieuwe media op het van socio-economie, werk-leef-omgeving, sociale en audiovisuele media, beleid en de verschillende kruisbestuivingen tussen ICT en media.*

UGent

- *Het Computing Systems Lab van UGent, meer specifiek het departement elektronica en informatiesystemen (ELIS)[9] onderzoekt nieuwe ontwikkelingen, methodes en specifiek nieuwe security oplossingen en software bescherming voor Computing Systemen. Er is onderzoek tegen fysieke aanvallen, beveiligde computing architecturen, software bescherming evaluaties, anti-tampering en obfuscation.*
- *Het IDLab[10] – Internet Technology and Data Science Lab van de Faculteit Ingenieurswetenschappen en Architectuur brengt verschillende technologieën samen zoals draadloze en bedrade netwerking, AI, Robotics en IoT. Ze beschikt over een uitgebreide infrastructuur, die nieuwe ontwikkelingen op het vlak van cybersecurity kan uittesten en faciliteren. Het IDLab is een samenwerking met Universiteit Antwerpen en IMEC.*
- *Het expertisecentrum industriële automatisering XiaK beschikt over een jarenlange ervaring.*

5.3.2. Toegepast onderzoek aan hogescholen[11]

HOWEST – onderzoeksgroep Security & Privacy

- Howest beheert samen met campus Kortrijk van de UGent de activiteiten van IC4- proeftuin innovatieve cyberveiligheid. Er wordt aan toegepast onderzoek gedaan in samenwerking met de industrie, waarbij de resultaten onmiddellijk worden gevaloriseerd. Dankzij het project beschikt IC4 over een testfaciliteit voor industriële use-cases om een technische evaluatie te doen[12]. Dit initiatief draagt actief bij aan het sensibiliseren en activeren van meer en meer bedrijven rond het thema cybersecurity (Dit betreft dus innovatieve cybersecurity voor industrie 4.0.)

[6] https://cdsl.research.vub.be/en/home
[7] https://ai.vub.ac.be/
[8] https://smit.vub.ac.be/
[9] https://www.ugent.be/ea/elis/en
[10] https://www.ugent.be/ea/idlab/en
[11] Informatie over toegepast onderzoek aan andere hogescholen werd opgevraagd maar werd niet ontvangen.
[12] Proeftuin ICI 4.0 | Innovatieve cyberbeveiliging voor de industrie! (industrie40vlaanderen.be

- Howest specialiseert zich in ‘Gedrag gebaseerde Artificiële Intelligentie inzetten tegen Cyber Industriële Aanvallen’. (AI inzetten om de bedrijven cyberveiliger te maken.)
- Howest is partner bij Europese projecten rond ‘Strategische en case-specifieke cyberbeveiliging voor Industrie 4.0 van Kmo’s ’.
- Howest doet inspanningen rond het voorbereiden van ondernemingen en hun werknemers op de implementatie en het gebruik van Cybersecurity.
- Een aantal nieuwe onderzoekdomeinen werden opgestart :
  - Agile security architecture and threat modelling tools and approaches
  - Intelligent cyber security for offshore wind farms
  - Intelligent zero trust architecture for 5G networks
  - Cybersecurity in The Metaverse
  - Secure blockchain development

5.3.3. Fundamenteel en toegepast onderzoek in de Strategische Onderzoekscentra

IMEC

Het strategisch onderzoekscentrum (SOC) IMEC heeft een nauw samenwerkingsverband opgezet met KU Leuven om onderzoeksresultaten rond cybersecurity te valoriseren bij grote internationale spelers. IMEC werkt hier o.a. samen met KU Leuven rond hardware security, bv. aan een true random number generator, een instrument dat cruciaal is in de informatiebeveiliging - o.a. voor encryptie.

5.3.4. Opleidingen cybersecurity universiteiten en hogescholen

Er is een toenemend aanbod aan Cybersecurity opleidingen aan de universiteiten en hogescholen. Het Centrum voor Cybersecurity in België voorziet een lijst met cyberopleidingen: ICT security opleidingen in België | Centrum voor Cybersecurity België (belgium.be). Een ander overzicht voor Vlaamse Cybersecurity-opleidingen kan gevonden worden op: https://cybersecurity-bites.be/opleiding/

5.4. Belang van eindgebruikers; bedrijven en overheden

Bedrijven

Belangrijkste afnemers vandaag zijn sectoren waar er traditioneel veel ICT wordt gebruikt en waar het belang van informatie en transacties, alsook de bescherming van de persoonsgegevens van klanten uitermate belangrijk zijn. ICT wordt vaak gevolgd door financiële diensten, die natuurlijk ook betrokken partij zijn in het Cybersecurity-landschap. bv. bedrijven zijn Swift, Euroclear, Mastercard… *Vervolgens komen meestal kritische infrastructuur, publieke dienstverlening zoals elektriciteit, gas en water. De publieke dienstverlening volgt snel, alsook de transportsector, en andere infrastructuur.* (extract experten rapport LSEC)

Publieke (internationale) instellingen

Een aantal internationale instellingen zoals de EC, de Raad van Europa, het Europees Parlement, NATO, ESA, Eurocontrol … zijn in België gevestigd.

6. Beleidscontext

6.1. Cybersecurity in Vlaanderen in de context van het beleid en eerdere studies

Vlaams Beleidsplan Cybersecurity

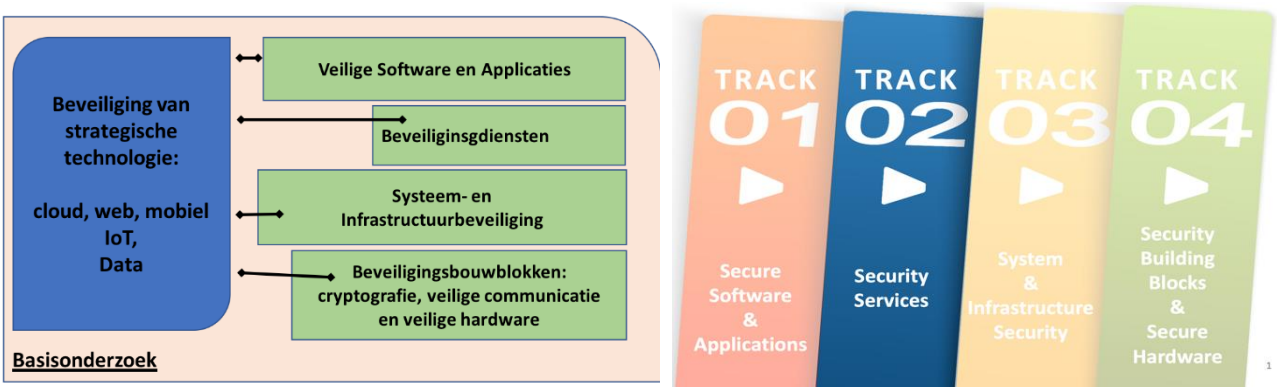
De Vlaamse Regering keurde op 22 maart 2019 het Vlaams Beleidsplan Cybersecurity[13] goed om onze kritische massa significant te versterken en de Vlaamse CS-maturiteit te vergroten. Het beleidsplan voorziet in een jaarlijkse investering van € 20 miljoen. Het plan steunt op een benchmark studie[14] die PWC in 2018 uitvoerde. Het Vlaams Beleidsplan Cybersecurity omvat drie luiken[15] 1) het uitvoeren van top strategische basisonderzoek, 2) een centrale focus op de implementatie van Cybersecurity-toepassingen in het bedrijfsleven en een 3) sterk flankerend beleid dat zich richt op bewustmaking, opleiding en ethische omkadering.

1) Uitvoeren van top strategisch basisonderzoek

'Vlaanderen behoort tot de internationale top op vlak van onderzoek naar relevante Cybersecurity-domeinen zoals cryptografie en het beveiligen van gedistribueerde systemen.

Een belangrijk onderdeel van het beleidsplan is het "Onderzoeksprogramma Cybersecurity Vlaanderen"[16] dat een aantal belangrijke kennis- en ontwikkeldomeinen omvat, die Vlaanderen en het Vlaamse onderzoek op het vlak van Cybersecurity duidelijker op de Europese en globale kaart positioneren. Er zijn vier onderzoekslijnen op lange termijn namelijk (1) software- en applicatiebeveiliging, (2) kritische beveiligingsdiensten voor diverse platformen (3) systeem- en infrastructuurbeveiliging en (4) technologische bouwblokken zoals veilige hardware, cryptografie en veilige communicatie (zie figuur 3). Het basisonderzoek wordt gecoördineerd door de KU Leuven[17].

Figuur 3: top strategisch basisonderzoek, als onderdeel van het Vlaams Beleidsplan Cybersecurity.



Het is in de context van deze opdracht belangrijk om vast te stellen dat belangrijke thema's zoals aangeduid in de Onderzoekslijnen[18] nog steeds overeenkomen met prioriteiten voor onderzoek en ontwikkeling voorgesteld op Europees niveau[19].

Hoewel die Europese prioriteitenlijst opgebouwd is op basis van een combinatie van discussies met verschillende onderzoekgroepen uit verschillende Europese lidstaten, eindgebruikers en overheden van

[13] https://www.vlaio.be/nl/andere-doelgroepen/vlaams-beleidsplan-cybersecurity
[14] https://www.ewi-vlaanderen.be/sites/default/files/bestanden/departement_economie_wetenschap_en_innovatie_-_benchmark_studie_over_cybersecurity.pdf
[15] VR 2019 2203 DOC0317/1QAUTER https://www.ewi-vlaanderen.be/sites/default/files/quaternota_aan_de_vlaamse_regering_-_vlaams_beleidsplan_cybersecurity.pdf
[16] onderzoeksprogramma_cybersecurity_vlaanderen_-_nota_aan_de_vlaamse_regering.pdf (ewi-vlaanderen.be) en https://cybersecurity-research.be/
[17] Vlaams Beleidsplan Cybersecurity | Agentschap Innoveren en Ondernemen (vlaio.be)
[18] Nota aan de Vlaamse Regering, VR 2019 1312 DOC 1235/1 : Onderzoeksprogramma Cybersecurity Vlaanderen
[19] https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

meerdere lidstaten en de Europese Commissie – en vertrekt vanuit een andere uitgangspunt - sluiten verschillende onderzoeksactiviteiten uit het Vlaamse Onderzoeksprogramma Cybersecurity aan bij de activiteiten op Europees niveau. Dat blijkt trouwens ook uit de talloze projecten, waarbij de Vlaamse onderzoeksgroepen een samenwerking hebben met andere Europese onderzoekscentra en Europese industriële partners in verschillende domeinen en sectoren.

2) Centrale focus op de implementatie van cybersecurity toepassingen voor het bedrijfsleven

'De absolute prioriteit van het beleidsplan is om de CS-maturiteit van de Vlaamse ondernemingen te verhogen door gebruik te maken van innovatieve CS-technologieën. Dit luit wordt geleid door VLAIO. Om deze doelstelling bij de bedrijven te bereiken, volgt VLAIO een aanpak die zowel gericht is op de koplopers als de innovatievolgers. Een belangrijke rol is weggelegd voor de actoren uit het VLAIO-netwerk die ondernemingen inspireren, sensibiliseren en informeren over het belang van cyberveiligheid. Het doel is om ondernemingen aan te zetten om verdere actie te ondernemen. Deze vervolgactie kan afhankelijk van de onderneming de vorm aannemen van het volgen van een masterclass, deelname aan een collectief traject bij een kennisinstelling of het opstarten van een eigen CS-verbetertraject.

Verder zet VLAIO bestaande subsidie-instrumenten (onderzoeksproject, ontwikkelingsproject, ICON-project, Baekeland-mandaten, …) in om bedrijven te ondersteunen die zelf CS-technologie ontwikkelen en/of in hun innovatieprojecten aspecten van cyberveiligheid willen integreren'[20].

3) Sterk flankerend beleid dat zich richt op bewustmaking, opleiding en ethische omkadering

'Cyberveiligheid eindigt niet met de implementatie van innovatieve technologieën. Er is eveneens nood aan een sterkere bewustwording en kennis rond cyberveiligheid bij werknemers en de brede bevolking. Naast de opleiding van IT-specialisten gaat het hierbij ook om het verhogen van basiscompetenties en vaardigheden bij werknemers die nog geen voorkennis hebben rond cyberveiligheid.

Hiervoor slaan het Departement Economie, Wetenschap en Innovatie en Agentschap Innoveren & Ondernemen (VLAIO) de handen in elkaar, samen met de hogeronderwijsinstellingen en andere stakeholders uit het VLAIO-netwerk.'[21]

Investeringen in awareness creatie

Vlaanderen heeft ook geïnvesteerd om de awareness m.b.t. Cybersecurity te verhogen. VLAIO heeft met verschillende van zijn structurele partners in het kader van het contract ondernemerschap en innovatieversnelling de afspraak om activiteiten op te zetten m.b.t. het thema cyberbeveiling. Dit gaat om partnerschappen met o.a. Agoria, Sirris, VOKA, UNIZO, VCB, NSZ, VERSO enz.

Flanders Investment & Trade heeft cybersecurity als prioriteit in de Verenigde Staten met groeiende aanwezigheid op de RSA conferentie. In 2022 resulteerde dit voor de eerste maal in een groepsstand met plaats voor 10 Vlaamse organisaties[22]. FIT is actief op de RSA sinds 2015. Cybersecurity was ook een belangrijke prioriteit op de Vlaamse-Nederlandse missie naar Atlanta in 2015 en op de Belgische Economische missie naar de Verenigde Staten in 2022.

6.2. Federale overheidsinitiatieven

In Vlaanderen zijn organisaties voornamelijk gebonden aan Belgische wetgeving en reglementering. In de huidige bevoegdheidsverdeling valt de Cybersecuritystrategie onder het federaal beleid, gerelateerd aan de beveiliging van de belangen van de Staat, haar diensten en haar burgers. Net zoals de Veiligheidsdiensten wordt het Cybersecurity beleid voornamelijk gestuurd vanuit het kabinet van de

[20] Vlaams Beleidsplan Cybersecurity | Agentschap Innoveren en Ondernemen (vlaio.be)
[21] Vlaams Beleidsplan Cybersecurity | Agentschap Innoveren en Ondernemen (vlaio.be)
[22] Door COVID kon de eerste groepsstand in 2020 niet doorgaan.

Eerste Minister. Verder is het ook van belang voor Justitie, Binnenlandse Zaken, Buitenlandse Zaken en Defensie.

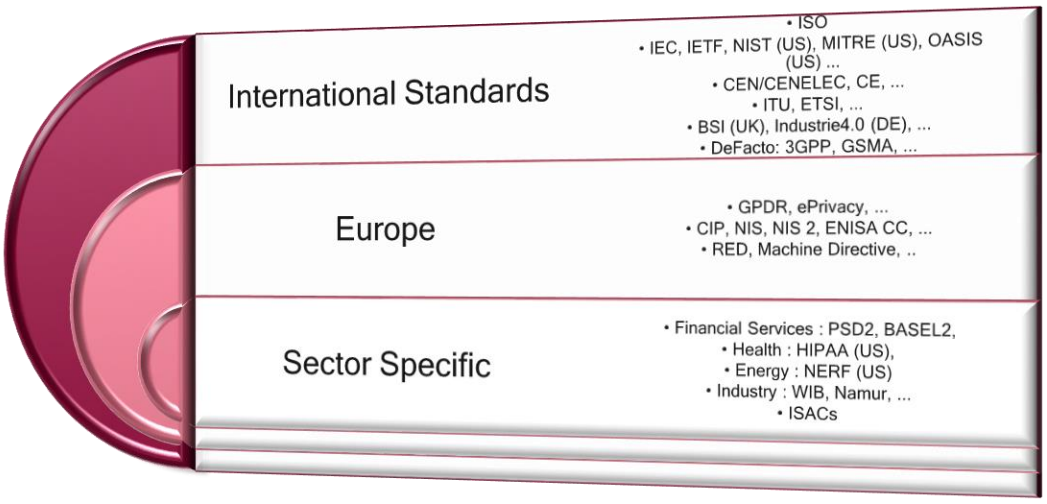
Op federaal niveau is het Centrum voor Cybersecurity België (CCB) het belangrijkst. Het centrum dat sinds begin 2021 onder de bevoegdheid van de Eerste Minister valt, sensibiliseert naar burgers en organisaties via SafeOnWeb[23]. Het organiseert CERT.be, een centraal meldpunt voor verdachte elektronische berichten en incidenten voor Belgische organisaties. Er is geen meldingsplicht, behalve voor kritische infrastructuren en essentiële diensten die dusdanig gedefinieerd zijn geweest. Overheidsorganisaties kunnen gebruik maken van CERT.be om hun Cyberincidenten te rapporteren en ondersteuning te vragen in de afhandeling ervan (onderzoek, begeleiding en samenwerking met politiediensten).

Het CCB wordt gefinancierd door de federale overheid en kan eventueel ondersteuning vanuit Europa bekomen voor specifieke projecten en activiteiten. Het CCB werkt ook samen met verschillende onderzoeksinstellingen en ondersteunt projecten en het middenveld voor een verbetering van het Cybersecurity landschap in België. Verschillende nieuwe projecten en activiteiten, zoals een centraal intelligence platform zijn afhankelijk van de verdere financiering van het centrum op federaal niveau. (extract experten rapport LSEC)

6.3. Internationale beleidscontext

Fundamenteel voor de toepassing van Cybersecurity in globale, Europese en Belgische context is de verplichting voor bedrijven om te beantwoorden aan wetgeving en regelgeving. Er bestaat echter geen eenduidige Cybersecuritywetgeving. De belangrijkste wetgeving wordt hieronder opgesomd. (extract uit het experten rapport van LSEC)

Figuur 4: Cybersecurity in een internationale context van beleid, regelgeving, standaarden en industriële verwachtingen



Bron: Experten rapport LSEC

GDPR - AVG

Het belang van Cybersecurity in het Europees beleid is in de afgelopen jaren alleen maar toegenomen. Naast de GDPR[24] - AVG die voorziet in specifieke bescherming van persoonsgegevens, is er ook de Directive on Security of Network and Information Systems (NIS)[25].

[23] https://safeonweb.be/nl/home
[24] https://ec.europa.eu/info/law/law-topic/data-protection_nl
[25] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2019040715&table_name=wet

NIS Directive

Het belang van de NIS-directieve zal in de komende jaren ook voor Vlaamse bedrijven verder toenemen. De NIS-Directieve is vandaag voornamelijk van toepassing op operatoren van essentiële diensten. Hoewel die in België door een federale wet (de NIS-wet[26]) wordt bekrachtigd, is ze van toepassing op verschillende Vlaamse organisaties en heeft ze een belangrijke impact op de Cybersecurity van Vlaanderen. Het belang van de directieve in Europa heeft te maken met Cybersecurity van infrastructuur zoals energie, transport, gezondheid, digitale diensten, financiële diensten en telecom. Operatoren worden geacht om hun Cybersecurity te kunnen aantonen. Van belang daarbij zijn de systemen die ze gebruiken om Cybersecurity mogelijk te maken, en om de onderliggende regelgeving aan te tonen. In 2021 wordt de NIS directieve op Europees niveau en met de lidstaten herbekeken. Het is een gelegenheid voor Vlaanderen om mee de discussie aan te gaan en vorm te geven aan een aantal sectoren die voor Vlaanderen van strategisch belang zijn, de nodige Cybersecurity ondersteuning en innovatiemogelijkheden lokaal te onderzoeken en op Europees niveau een diepe expertise in het domein mee te helpen vormgeven.

Cyberact

Met de EU Cybersecurity Act (de Cyberact)[27] wordt onder meer aan ENISA[28] vanuit de Europese Unie een mandaat toegekend dat de organisatie versterkt en nieuwe opdrachten toekent, waaronder het inrichten van een EU-brede certificatie framework voor digitale producten, diensten en processen. Dat betekent in concreto dat ENISA vandaag geacht wordt om certificatie schema's, voorwaarden en certificaten in te richten.

Digitale soevereiniteit

De Datastrategie[29] is één van de eerste fundamenten van de digitale strategie van de Commissie. Met de Europese datastrategie wil Europa een eenheidsmarkt voor gegevens dat de wereldwijde competitiviteit en data soevereiniteit verzekeren. Europa erkent hiermee dat gegevens de voedingsbodem zijn voor economische groei, innovatie, jobcreatie en maatschappelijke vooruitgang in het algemeen. In het voorstel voor verordening[30] van December 2020 voor Europese gegevensbeheer, de Datagovernanceverordening – worden maatregelen voorzien om het delen van gegevens te faciliteren tussen sectoren en grenzen en het recht om gegevens te vinden voor het juiste doel.[31]

Programma Digitaal Europa

Het Programma Digitaal Europa voorziet in financiering voor projecten op vijf cruciale gebieden: (1) supercomputing, (2) kunstmatige intelligentie, (3) cyberbeveiliging, (4) geavanceerde digitale vaardigheden en (5) promoten van het brede gebruik van digitale technologieën in de hele economie en samenleving.

Het programma is bedoeld om de kloof tussen onderzoek op het gebied van de digitale technologieën en marktintroductie te overbruggen. Het zal de Europese burgers en bedrijven, met name kleine en middelgrote ondernemingen, ten goede komen. Investeringen in het kader van het programma Digitaal Europa ondersteunen de tweeledige doelstelling van de Europese Unie, namelijk een groene transitie en een digitale transformatie, en versterken de veerkracht en de technologische soevereiniteit van de Unie[32].

[26] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2019040715&table_name=wet
[27] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[28] https://www.enisa.europa.eu/
[29] https://ec.europa.eu/digital-single-market/en/european-strategy-data
[30] https://tinyurl.com/1c08owhc
[31] Datagovernanceverordening, p14
[32] Programma Digitaal Europa | Europese Commissie

7. SWOT-analyse

Onderstaande SWOT-analyse werd samengesteld op basis van het experten rapport van LSEC en de bevindingen van de validatieworkshop.

7.1. Sterktes

- **Internationaal erkende onderzoek- en ontwikkelingscompetenties en experten**

In bijna elk gesprek met mensen uit de Cybersecurity en informatiebeveiligingssector in Vlaanderen, of Vlamingen in het buitenland wordt gerefereerd naar de erkenning van Vlaamse onderzoekers, onderzoeksgroepen en universiteiten. Vlaanderen staat voornamelijk bekend als Cybersecurity-expert-regio dankzij het leidinggevend onderzoek, technologische ontwikkelingen, de wereldvermaarde expertise en de maatschappijkritische houding van enkele van onze experten. Verschillenden onder hen hebben inderdaad een meer dan verdiende erkenning gekregen voor baanbrekend werk, en hun bijdragen tot de wereldwijde ontwikkeling van de sector en internetbeveiliging.

Cybersecurity-experten die vanuit Vlaanderen in andere landen in de wereld actief zijn, nemen vaak belangrijke en strategische rollen in bij internationale topbedrijven. Vlamingen actief bij bijvoorbeeld Zendesk, Amazon, Google, Microsoft, DXC, … worden in hun industrie erkend omwille van hun vak-expertise.

IMEC wordt vaak geduid als een referentiekader en een belangrijke troef voor huidige en verdere toekomstige Cybersecurity-ontwikkelingen. Voor verschillende deelnemers aan de interviews wordt IMEC als een sterkte voor Vlaanderen geprezen, en ook beschouwd als een mogelijk lanceringsplatform voor nieuwe Cybersecurity-ontwikkelingen. Verschillende waarnemers duiden ook op het belang van micro-elektronica in het bestrijden van Cybersecurity incidenten en uitdagingen in de toekomst. De eerder beschreven toenames in volumes, complexiteit en origine van cybercriminaliteit nopen de vraag naar snellere, meer performante en "dedicated" Cybersecurity-componenten, die snelle berekeningen kunnen doen – of die bijkomende beveiliging en vertrouwen kunnen garanderen als onderliggende systemen.

- **Vlaamse beleidsagenda cybersecurity geeft duidelijke richting**

De recente jaren is Vlaanderen erin geslaagd om te groeien op het vlak van cybersecurity. Met het opzetten van de beleidsagenda Cybersecurity (zie eerder 6.1) werd er vanuit de overheid (in samenspraak met het ecosysteem) een duidelijke richting vooropgesteld. Er wordt heel actief nagedacht over het cybersecurity-ecosysteem. Landen zoals Nederland en het Verenigd Koninkrijk benijden ons daarvoor. Duitsland blijft wel de richtlijn m.b.t. Cybersecuritybeleid.

- **Vlaamse Cybersecurity aanbieders zijn vooral sterk in niches**

De (van oorsprong) Vlaamse Cybersecurity bedrijven zijn vandaag nichespelers in een wereldmarkt die wordt gedomineerd door Noord-Amerikaanse en Israëlische technologieleveranciers. Het is een sterkte, omdat ze in hun respectievelijke domeinen als belangrijke spelers worden beschouwd. Bedrijven zoals Guardsquare, SecureCodeWarrior, IntrinsicID, Sweepatic en Intigriti dragen het vaandel van Vlaamse Cybersecurity-bedrijven en effenen de weg voor Scaled Access, Firmalyzer, Elimity, Ceeyu, CO-DEX.eu, Cranium, nAuth en verschillende anderen.

Cybersecurity technologie van Vlaamse oorsprong is ook terug te vinden in andere specifieke niches, waarbij het deel uitmaakt van een breder technologie-aanbod zoals versleutelingstechnologie, beveiligingscomponenten voor micro-elektronica zoals mobiele telefonie, draadloze communicatie, satellietsystemen en andere vormen van telematica en telecom.

- **België en Vlaanderen in top 10 van de Europese Cybersecurity-afnemers door aanwezigheid van grote internationale instellingen**

Met een zesde plaats in EU27 (zonder het Verenigd Koninkrijk) is België een belangrijke Cybersecurity afnemer van producten en diensten in absolute waarde. België beschikt met onder meer de internationale instellingen zoals de EC, de Raad van Europa, het Europees Parlement, NATO, ESA, Eurocontrol, … over een belangrijke publieke bijdrage aan de Cybersecurity-industrie. Vooral ook omdat al die instellingen ook in België (Brussel – Vlaanderen) een belangrijk Cybersecurity-expertisecentrum coördineren.

- **Clusterwerking, innovatie-ondersteuning en marktontwikkeling**

Vlaanderen wordt geprezen voor zijn rijk en stevig intermediair weefsel van sectorfederaties, clusters, strategische onderzoekscentra, gebruikersorganisaties en netwerkorganisaties die de brug slaan tussen sectoren en onderzoek- en ontwikkeling.

7.2. Zwaktes

- **Gebrek aan intensieve samenwerking tussen de intelligence services en Cybersecurity-innovatieleiders**

In vergelijking met omringende ecosystemen (zoals de US, UK, Israël) is er in Vlaanderen geen intensieve samenwerking tussen de politie, intelligence en defensie services en Cybersecurity-innovatieleiders. Zo'n samenwerking is een grote stimulans voor de Cybersecurity sector en het ontbreken ervan in Vlaanderen vormt een belemmering voor onze innovatieleiders.

- **Beperkte markt van grote afnemers-bedrijven en gebrek aan leiderschap van 'dominante klanten'**

Vlaanderen heeft maar een beperkt aantal (maar belangrijke lokale) technologie-ontwikkelaars die Cybersecurity-expertise ondersteuning lokaal kunnen gebruiken. Dit maakt dat er maar een beperkt aantal afnemers zijn van belangrijke omvang.

De waardeketen in Vlaanderen is niet volledig; we hebben weinig technology providers. Maar dit hoeft geen zwakte te zijn. Wat wel ontbreekt is het leiderschap van dominante klanten. Zij zijn in andere landen vaak een accelerator, zijn sterk aanwezig in de omgeving en hebben een invloed op leveranciers/regelgeving.

- **Eindgebruiker slechts in beperkte mate bereid tot innovatie-ontwikkeling**

Een moeilijkheid voor verschillende Vlaamse Cybersecurity-technologie-ontwikkelaars is dat hun innovatieve oplossingen moeilijk ingang vinden bij Vlaamse bedrijven. Cybersecurity-experten duiden op een soort van natuurlijke resistentie dat Vlaamse technologiebedrijven onvoldoende kennis, expertise, ervaring, specialisatie of algemeen een afdoende oplossing zouden kunnen leveren voor uitdagingen van de Vlaamse bedrijven. Ze wijzen erop dat Vlaamse technologiebedrijven het vaak moeilijker hebben om hun aanbod te laten landen in het Vlaamse industrieel netwerk (in vergelijking met bv. Nederland of het Verenigd Koninkrijk).

- **Sterke competitie met het buitenland voor het aantrekken van buitenlandse investeringen**

Bij de sterktes werd aangegeven dat Cybersecurity-experten die vanuit Vlaanderen in andere landen in de wereld actief zijn vaak belangrijke en strategische rollen innemen bij internationale topbedrijven. Bij het aantrekken van buitenlandse investeringen blijkt de concurrentie met bv. Nederland bikkelhard, dit omdat er een groter aantal Nederlanders op cruciale plaatsen in het buitenland actief zijn. Ook al is Vlaanderen er dikwijls vroeger bij en hebben we sterke troepen op het vlak van O&O-talent, toch lopen we soms investeringen mis. Als voorbeelden worden aangehaald Palo Alto Networks en Fortanix.

Met de sterktes die Vlaanderen heeft in digitale technologie, is het belangrijk dat dit internationaal meer als prioriteit in de markt gezet wordt zoals bv. voor biotech en cleantech het geval is. Daarnaast

wordt het gebrek van een rechtstreekse vlucht naar de west kust van de USA als belemmering aangehaald.

7.3. Opportuniteiten

- **Cloud-security – Secure cloud**

Onze uitzonderlijke expertise en competentie in Vlaanderen in dit domein wordt door verschillende experten beschouwd als een sterkte en een opportuniteit. De expertise in Cloud Security is verdeeld over verschillende onderzoeksgroepen en -instellingen (KU Leuven, VUB, UGent, UAntwerpen …), is een domein in volle ontwikkeling en biedt ook mogelijkheden aan verschillende Vlaamse en Belgische cloud- en technologie-aanbieders zoals Combell, Cegeka, Proximus, Awingu, ABLE, UnifiedPost, Telenet …

Maar ook op Europees niveau wordt de oproep voor oplossingen en ontwikkelingen voor beveiliging steeds duidelijker[33], vaak ook gedreven vanuit de idee om opnieuw voldoende onafhankelijk te worden van de niet-Europese cloud-leveranciers (AWS, Microsoft Azure, Google-cloud, Alibaba, …). Verschillende experten wijzen op de unieke Vlaamse expertise in het domein van Computing on Encrypted Data, een combinatie van MPC en FHE[34].

- **Identity, Access, Authentication, Authorisation, … Vlaamse expertise is kritisch**

Verschillende Cybersecurity technologiespelers in Vlaanderen zijn in verschillende vormen actief in het domein van cyber-identiteit. Identiteiten zijn een belangrijk onderdeel van de toekomstige cyber-veiligheidsinfrastructuur, en vooral ook in toepassingen in de cloud en voor industriële doeleinden. Vlaamse bedrijven zoals nAuth, ScaledAccess, eLimity, Trustbuilder, Belgian Mobile ID (itsMe), … en de verschillende dienstenleveranciers kunnen verder bouwen op de unieke expertise waar we in Vlaanderen over beschikken. De Vlaamse overheid maakt intensief gebruik van identiteitsbeheer en toegangscontrole op hun systemen. (Meer dan twintig jaar geleden werd België internationaal erkend omwille van de elektronische identiteitskaart. Het was toen een belangrijke innovatieve ontwikkeling.)

- **IIoT security ontwikkelingen kunnen worden toegepast in hoogtechnologische toepassingen zoals gezondheidszorg en industrie (pharma, petrochem,…)**

Vlaanderen beschikt over unieke expertise van technologie, sectoren, en markten door technologische ontwikkelingen die plaatsvinden bij machinebouwers, in micro-elektronica, in consumentenelektronica, sensorsystemen, elektronica voor bedrijfstoepassingen en het toevoegen van communicatiemogelijkheden aan bestaande toestellen voor verschillende toepassingen.

Het toevoegen van Cybersecurity aan die ontwikkelingen is zowel een opportuniteit voor de ontwikkelaars van de toepassingen, de ontwikkelaars en integratoren van de componenten voor de micro-elektronica, voor de exploitanten en het hele IoT en IIoT-ecosysteem, als het een opportuniteit betekent voor Cybersecurity-technologie-ontwikkelaars en de respectievelijke ecosystemen waartoe ze behoren. Ook eerder hebben we verwezen naar de impact op de ontwikkelingen, de benodigde certificaties – en verwachtte technologische invulling om voor de certificaties te kunnen instaan. Maar ook in een breder maatschappelijke context is de bescherming van IoT en IIoT relevant en belangrijk. Smart cities en regio's zullen pas succesvol zijn als er geen vervelende Cybersecurity incidenten ontstaan, waardoor de toestellen bijvoorbeeld persoonsgegevens laten lekken.

- **Belangrijke lokale technologie-ontwikkelaars die cybersecurity-expertise ondersteuning lokaal kunnen gebruiken (bv. picanol, Cochlear, Colibra…)**

De sterkte van specifieke Vlaamse technologiespelers wordt geprezen. Er is een opportuniteit voor Vlaamse technologie-ontwikkelaars (zoals Picanol, Colibra, Niko, Cochlear) om hun producten en diensten beter te beveiligen, dit door een nauwere samenwerking met Cybersecurity bedrijven en door experten in te schakelen voor de producten- en dienstenverbetering. Op die manier kunnen

[33] Getuige de initiatieven die opgezet worden m.b.t. een IPCEI Cloud: Vlaanderen neemt deel aan IPCEI-Cloud! | Agentschap Innoveren en Ondernemen (vlaio.be)
[34] Multiparty Computation (MPC) houdt in dat er door verschillende partijen tegelijkertijd op gegevens kan worden gewerkt. Fully Homomorphic Encryption voegt er de encryptie aan toe.

Cybersecurity-bedrijven betere niche-competenties opbouwen en die specifieke competenties vervolgens ook aanbieden aan andere technologie-ontwikkelaars, in de rest van de wereld.

7.4. Bedreigingen

- **Verlies aan soevereiniteit**

In het afgelopen decennium zijn de schaarse Vlaamse Cybersecurity-bedrijven het onderwerp of het voorwerp van overnames, mergers en acquisities geworden. Cybertrust is gevormd op de basis van Ubizen – Netvision en uiteindelijk overgenomen door Verizon Business. Ascure en C-Cure zijn respectievelijk overgenomen door PwC en Telenet. Ook de overname van Telindus door Proximus, en de overnames van Zion Security en Securelink door Orange Cyberdefense zijn voorbeelden. Vandaag is de uitdaging en de problematiek nog niet echt aan de orde. Maar het mogelijke verlies van expertise en technologie, al dan niet door de internationale exploitatie van Vlaamse Cybersecurity-technologie als resultaat van internationale overnames, is een punt van aandacht voor Vlaanderen.

Tijdens de interviews is meermaals die bedreiging geformuleerd, met de oproep om met de beschikbare expertise in Vlaanderen ook een antwoord te bieden aan de afhankelijkheid van Cybersecurity technologie van buiten Vlaanderen, mogelijkheden te exploreren om een verhoogde weerbaarheid te tonen of toch tenminste opties te onderzoeken en te experimenteren. Verhoogde weerbaarheid is een strategisch thema binnen Europa en de lidstaten, en draagt ook bij tot bestaande programma's (INFRA) en beleid (NIS; CIP). Niet beschikken over mogelijkheden zoals Cybersecurityexperten en teams in het geval een belangrijk incident zich zou voordoen in Vlaanderen, zou kunnen betekenen dat er uitzonderlijke economische en maatschappelijke schade geleden wordt.

- **Onvoldoende investeerders om core technologie vanuit onderzoek naar markt te financieren**

Hoewel recentelijk in België en Vlaanderen er een aantal nieuwe investeerders zijn die een oriëntatie naar Cybersecurity in een vroeg stadium overwegen (Investlink, Fortino, Seederfund, imec-istart, Startit@KBC, … het Business Angel Netwerk) blijft het moeilijk voor Vlaamse starters om de nodige fondsen in een vroeg stadium bij mekaar te sprokkelen. Maar ook na de startup fase is het moeilijk om de nodige fondsen van meer dan 1 miljoen EUR te vinden. Dit is een belemmering voor Vlaamse ondernemers en Cybersecurity experten die proberen op een onafhankelijke basis een eigen product en technologie te ontwikkelen en naar de markt te brengen en dus een bedreiging op lange termijn voor een voldoende groot Vlaams aandeel aan core cybersecurity ontwikkelingen. Cybersecurity-technologieën vanuit de onderzoekscentra vinden moeilijker hun weg naar de markt en zullen meer tijd nodig hebben om te worden opgepikt door andere internationale spelers. Ondernemers en Cybersecurity-experten zullen hun heil zoeken in het buitenland.

- **Israëlische, VS en UK-tech groepen die snel en direct kunnen aanpassen aan nieuwe omstandigheden.**

De internationale concurrentie is duidelijk, agressief en voornamelijk van buiten Europa. Hoewel Vlaanderen en Europa beschikken over expertise, innovatie en continue onderzoek en ontwikkeling op wereldschaal zijn het voornamelijk bedrijven uit Israël, VS, en het VK die marktleiders blijven in Cybersecurity-technologie. De technologiebedrijven kunnen zich onderscheiden door een grote thuismarkt voor evaluatie en ondersteuning en een grotere lokale thuismarkt door een hogere maturiteit van de bedrijven.

- **Krapte op de arbeidsmarkt - nood aan meer Cybersecurity-experten**

In de komende vijf jaar zal de Cybersecurity-expertise niet alleen een strategische meerwaarde voor Vlaanderen en Europa betekenen, maar ook een reële jobcreatie realiseren. Het gaat om Cybersecurity experten, die - deels via de opleidingscentra, deels via onlinetraining in combinatie met de hands-on inschakeling tijdens het werk - bijkomende training krijgen om hun expertise te vervolledigen en te vervolmaken. Een sterke toename van het aantal Cybersecurity-experten maakt een toekomstige versterking van cybersecurity-ontwikkelingen in producten, diensten en in strategische Vlaamse

sectoren mogelijk. Het zal echter een uitdaging worden voor ondernemingen om mensen met de juiste profielen aan te aantrekken. Tijdens de validatieworkshop werd aangegeven dat sommige ondernemingen genoodzaakt zijn om bepaalde activiteiten te outsourcen omdat ze niet in staat zijn om lokaal de mensen met de nodige expertise aan te trekken. Er werden hier wel al stappen in de goede richting gezet. Door toedoen van de Vlaamse Beleidsagenda Cybersecurity gaat er extra aandacht en middelen naar het opleiden van nieuwe Cybersecurity-experten.

8. Aanbevelingen IPCEI

1. Vlaanderen heeft potentieel om deel te nemen aan IPCEI maar niet als trekker

Tijdens de validatieworkshop wordt aangegeven dat het momenteel moeilijk is om het 'potentieel' te beoordelen van een actieve deelname van Vlaanderen en Vlaamse bedrijven aan een IPCEI cybersecurity. Dit omdat er nog geen duidelijke scope is van deze IPCEI. De scope van een IPCEI wordt bepaald door het trekker-land in samenspraak met geïnteresseerde landen, onder toezicht van de EC. Het hoeft echter niet te verbazen dat het trekker-land een belangrijke bijdrage levert tot het bepalen van de scope.

De afgelopen jaren is Vlaanderen erin geslaagd om te groeien op het vlak van cybersecurity. Met het opzetten van de beleidsagenda Cybersecurity werd er vanuit de overheid (in samenspraak met het ecosysteem) een duidelijke richting vooropgesteld. Duitsland blijft wel de richtlijn m.b.t. Cybersecuritybeleid. Het resultaat vandaag is dat Vlaanderen Europees gezien een goede middenpositie inneemt. Dit houdt wel in dat België/Vlaanderen (nog) niet in een positie is om een IPCEI cybersecurity te trekken.

2. Directe IPCEI-deelname van Vlaanderen hangt niet enkel af van pure Cybersecurity spelers

Er wordt opgemerkt dat we als Vlaanderen zeker kunnen aansluiten voor bepaalde cybersecurity-topics op niveau van Duitsland; we hebben veel potentieel. Een actieve deelname aan IPCEI - met notificatieproces bij de EC en steun buiten de staatssteunregeling - is natuurlijk afhankelijk van de concrete interesse van de bedrijven (die niet aanwezig waren bij de validatieworkshop).

Voor het bepalen van die interesse mag er niet eenzijdig gepolst worden bij bedrijven die zich uitsluitend op Cybersecurity richten. Dergelijke spelers zijn momenteel eerder beperkt aanwezig in Vlaanderen. Voor een mogelijke IPCEI-deelname moet ook ruimer gekeken worden. Als er bv. vijf grote bedrijven die cybersecurity als kernvereiste hebben in hun producten, interesse hebben om deel te nemen dan is dit een even belangrijke piste om te bekijken als de interesse van één grote Cybersecurity-speler.

3. Zelfs zonder directe deelname zijn er vruchten te plukken via indirecte IPCEI-deelname

Indien er op het tijdstip van het ontstaan van een cybersecurity-IPCEI geen bedrijven zijn die direct willen deelnemen is het voor Vlaanderen toch belangrijk om het IPCEI-initiatief op te volgen en indirecte deelname te stimuleren. Vlaanderen heeft heel veel Cybersecurity-expertise en experten bij bedrijven en kennisinstellingen die zeker kunnen aansluiten bij internationale initiatieven in het kader van IPCEI (maar zeker ook breder). Die bedrijven kunnen daarvoor in Vlaanderen steun krijgen via de reguliere kanalen.

Bijlage 1: Lijst geconsulteerde partijen LSEC

Tabel 5: Lijst geconsulteerde partijen experten rapport Cybersecurity LSEC

Organisatie	**Geïnterviewden**
Maarten Van Horenbeeck	CISO Zendesk (US), former chairman FIRST
Bart Preneel	Prof. Dr. departementshoofd COSIC, KU Leuven
Luc Dooms	Ondernemer, oprichter en voormalige CEO C-Cure
Freddy Dezeure	Board-member Arctic Security, Corelight, Oneclick, EIQ…
Wouter Joosen	Prof. Dr. Departementshoofd DISTRINET, KU Leuven
Stijn Bijnens	Voorzitter stuurgroep Cybersecurity – Vlaams Actieplan Cybersecurity, CEO Cegeka, voormalige CEO Ubizen en CEO LRM
Frank Staut	CTO & mede-oprichter SecureLink, partner Investlink
Matias Madou	Founder, COO Secure Code Warrior
Eric Lafortune	Voormalige CTO Guardsquare
Jan Valcke	Co-founder en voormalig COO Vasco Datasecurity (OnePass)
Jo De Boeck	COO, imec
Luigi Rebuffi	CEO ECSO
Danilo D'Elia	Cybervalleys project
Patrick Coomans	Agoria
Yves Schellekens	Agoria
Wim Sohier	Flanders Investment and Trade, attaché
Michel Hofman	Flanders Investment and Trade, attaché
Katie Stebbins	Chair Global EPIC (Global Cybersecurity Innovators), innovation specialist MIT
Barbara Van Den Haute	Administrateur-Generaal Vlaanderen Digitaal
Stefan Desmet	Afdelingshoofd ICT, Vlaanderen Digitaal
Kelly McKain	Informed Security Manager, Orasure
Jeroen Fiers	Adviseur Vlaams Agentschap Innoveren en Ondernemen
Miguel De Bruycker	Managing director CCB – CERT.be
Karl Driessens	VP Aviatrix (former VP EMEA Palo Alto, Elastica, Rubrik)
Lieven Danneels	CEO Televic
Bart Donné	General Manager Westpole
Walter Van Uytven	CEO Awingu

Bijlage 2: Deelnemers validatieworkshop Cybersecurity

Datum: 25 augustus 2022, MS Teams

Experten:

- Caroline Breure (Centrum voor Cybersecurity België)
- Ferdinand Casier (Agoria)
- Patrick Coomans (Agoria)
- Stefan De Smet (Digitaal Vlaanderen)
- Filip De Weerdt (FIT Agency)
- Jeroen Fiers (VLAIO)
- Patrick Hauspie (VLAIO)
- Michel Hofman (FIT Agency)
- Wouter Joosen (Professor KU Leuven en coördinator van enkele programma's in het Vlaamse Beleidsplan)
- Paul Roevens (Unizo)
- Paris Van Paesschen (Departement EWI)
- Simon Verschaeren (Departement EWI)

Schriftelijke feedback:

- Wim Codenie/Herman Derache (Sirris)
- Kurt Callewaert (Howest – proeftuin innovatieve cyberveiligheid en flankerend beleid van beleidsagenda)
- Wim Sohier (FIT Agency)

VARIO:

- Lieven Danneels
- Vanessa Vankerckhoven

VARIO-staf:

- Thomas Geernaert
- Danielle Raspoet
- Annelies Wastyn

Bijlage 3: Resultaten FRIS-analyse

Om beter zicht te krijgen op het onderzoek dat aan onze kennisinstellingen gebeurt, heeft VARIO een beroep gedaan op het FRIS-team van het departement EWI, om dit in kaart te helpen brengen[35]:

- Welke onderzoekgroepen betrokken zijn bij onderzoek m.b.t. cybersecurity
- Om welke specialisatie(sub)domeinen het gaat;

Deze informatie werd verkregen op basis van de gegevens voor projecten en publicaties m.b.t. het onderzoek aan de universiteiten in de periode 2015-2021, aanwezig in FRIS op 18 februari 2021. Hoewel deze oefening een 'eerste, ruw' overzicht biedt, is dit niet exhaustief en moeten we enkele kanttekeningen maken bij de resultaten:

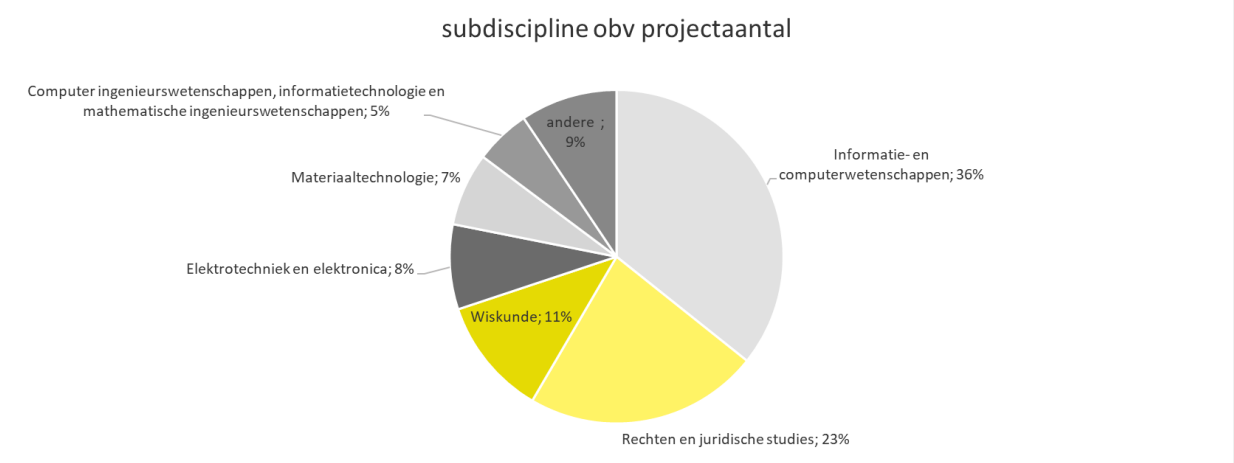
- Deze selectie kan ruis bevatten d.w.z. onderzoek dat wel de betreffende zoektermen bevat, maar eigenlijk geen betrekking heeft op onderzoek betreffende het thema
- Bepaalde stakeholders die relevant kunnen zijn m.b.t. dit onderzoek ontbreken in FRIS (bv. imec, VITO, de industrie…)
- Spelers zoals de hogescholen leveren aan FRIS enkel die projecten aan die worden gefinancierd door VLAIO. De rest van hun onderzoeksportfolio ontbreekt in FRIS.

De zoekopdracht leverde rechtstreekse zoekhits op bij de volgende objecten:

- 12 onderzoeksgroepen bij de universiteiten (10) en LSEC (2)
- 181 projecten bij de universiteiten (178), LSEC (2) en hogescholen (1)
- 555 publicaties bij de universiteiten (551), ITG (2), ILVO (1) en Plantentuin (1)

Cybersecurity onderzoek in Vlaanderen situeert zich in hoofdzaak in de subdomeinen van Informatie- en computerwetenschappen (36%), Rechten en juridische studies (23%) en Wiskunde (11%) (Figuur 5).

Figuur 5: Wetenschapssubdisciplines bij Cybersecurity onderzoek (o.b.v. 181 projecten)



Bron: FRIS-databank. Analyse uitgevoerd door het departement EWI

[35] Er werd daarbij gebruik gemaakt van de volgende zoektermen: "cybersecurity, cyber security, cyberveiligheid, computer security, computerbeveiliging, data security, data beveiliging, digital security, data integrity, data protection, cryptogra"

Onderzoek over Cybersecurity in Vlaanderen

Analyse op basis van FRIS (2015 – 2021)
18/02/2021
Pascale Dengis, team FRIS, EWI

Situering

- VARIO wil graag voor de IPCEI waardeketens in kaart brengen welke onderzoeksgroepen in Vlaanderen betrokken zijn en in welke wetenschapsdisciplines die expertise vooral zit
- Het FRIS-team doet hiervoor een opzoeking in FRIS aan de hand van een aantal zoektermen.

methodologie

- **Data zoals beschikbaar in FRIS op 18/02/2021**
- **Gezocht met volgende zoektermen:** “cybersecurity, cyber security, cyberveiligheid, computer security, computerbeveiliging, data security, databeveiliging, digital security, data integrity, data protection, cryptogra"

- **Bij Onderzoeksgroepen:**

  Gezocht in naam, onderzoeksactiviteit, keywords en disciplines
- **Bij Projecten:**

  Gezocht in titels, abstracts, acronyms, keywords en disciplines.

  Startjaar: 2015-2021
- **Bij Publicaties:**

  Gezocht in titels, abstracts, keywords en disciplines.

  Publicatiejaar: 2015-2021

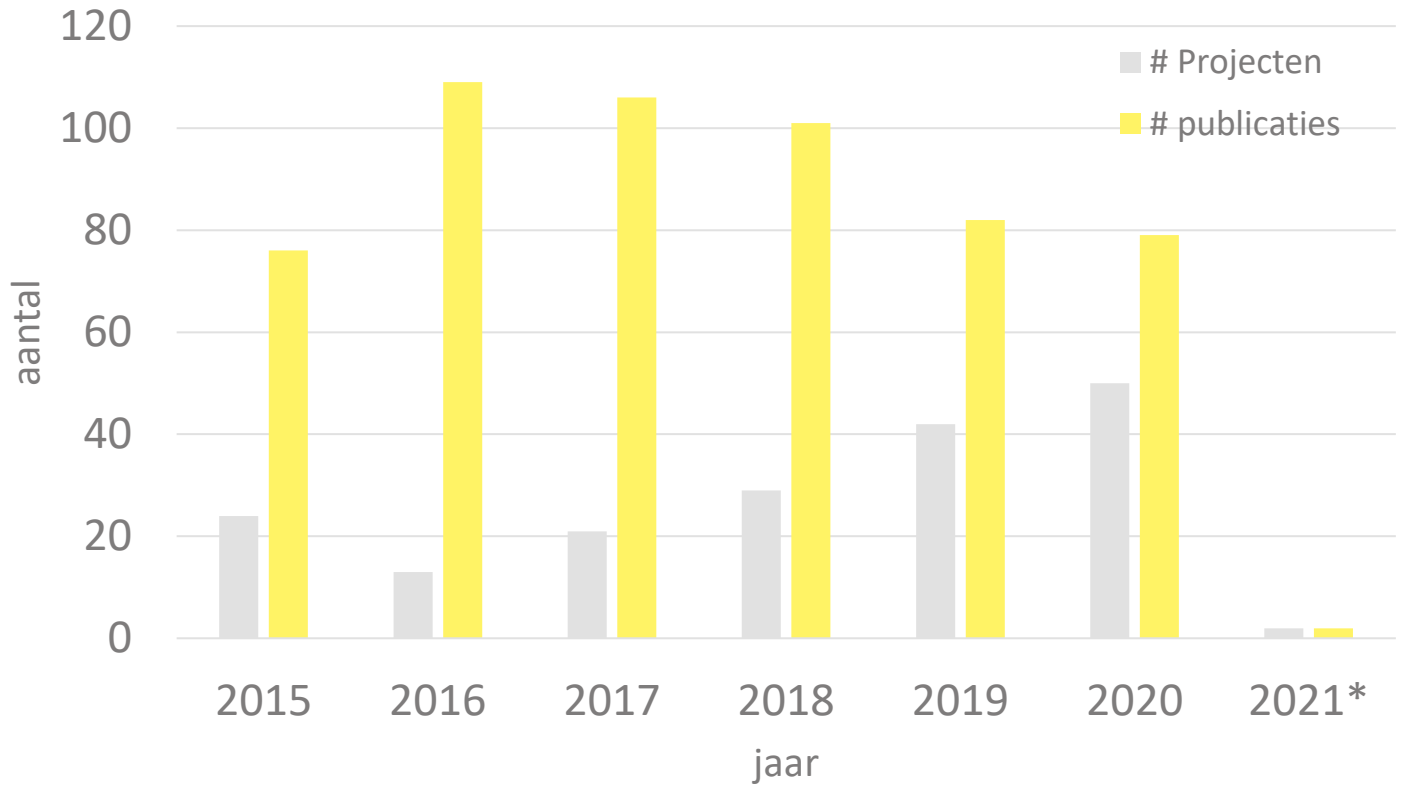
methodologie

De zoekopdracht leverde rechtstreekse zoekhits op bij de volgende objecten:

- **12 onderzoeksgroepen** bij de universiteiten (10) en LSEC (2)
- **181 projecten** bij de universiteiten (178), LSEC (2) en hogescholen (1)
- **555 publicaties** bij de universiteiten (551), ITG (2), ILVO (1) en Plantentuin (1)

- Deze selectie kan ruis bevatten dwz onderzoek dat wel de betreffende zoektermen bevat, maar eigenlijk geen betrekking heeft op onderzoek betreffende het thema
- Bepaalde stakeholders die relevant kunnen zijn mbt dit onderzoek ontbreken in FRIS (bv. IMEC, de industrie…)
- Spelers zoals de hogescholen leveren aan FRIS enkel die projecten aan die worden gefinancierd door VLAIO. De rest van hun onderzoeksportfolio ontbreekt in FRIS.

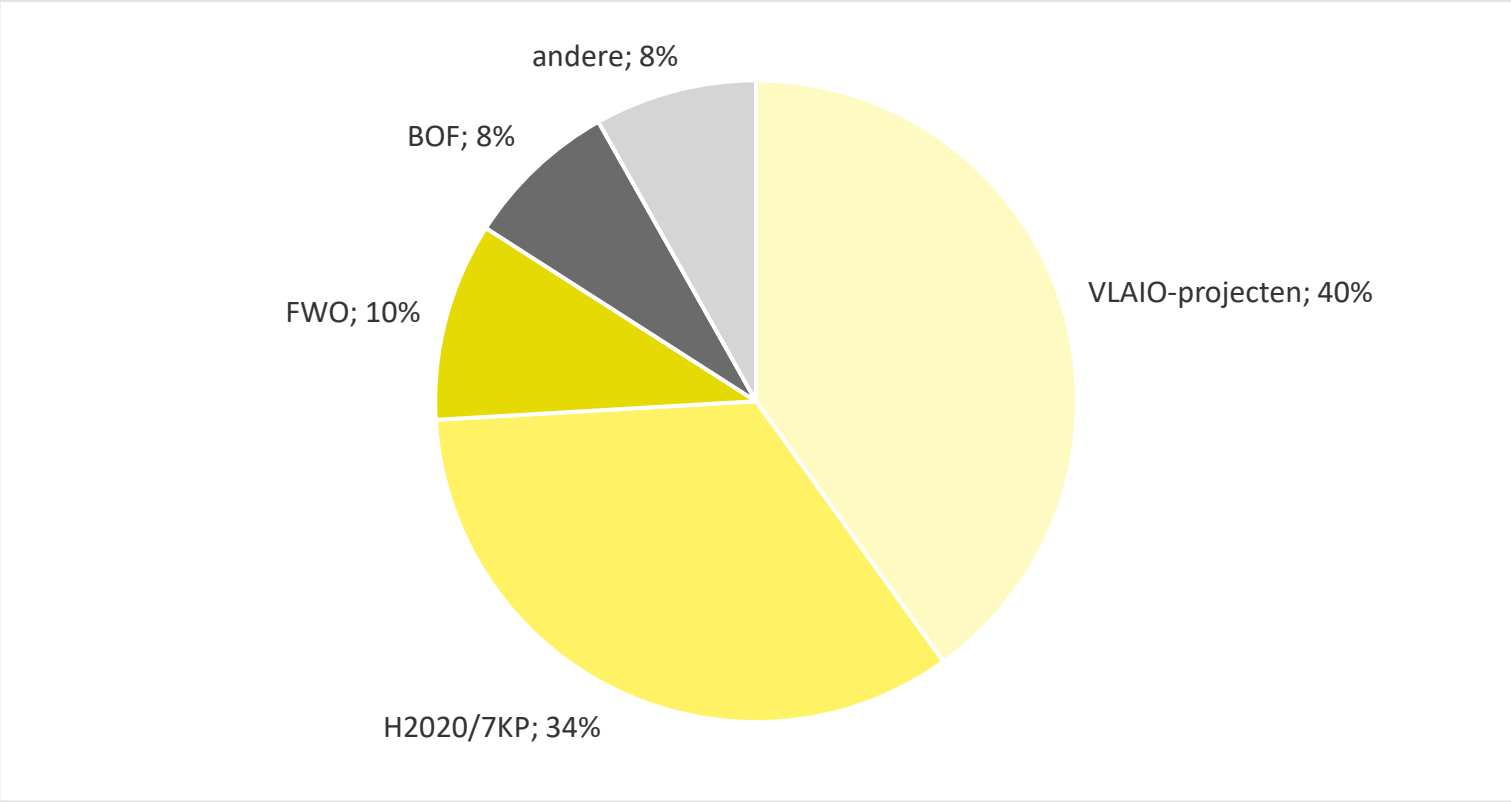
Cybersecurity onderzoek



**: 2021: voorlopig cijfers zoals in FRIS aanwezig op 18/02/2021*

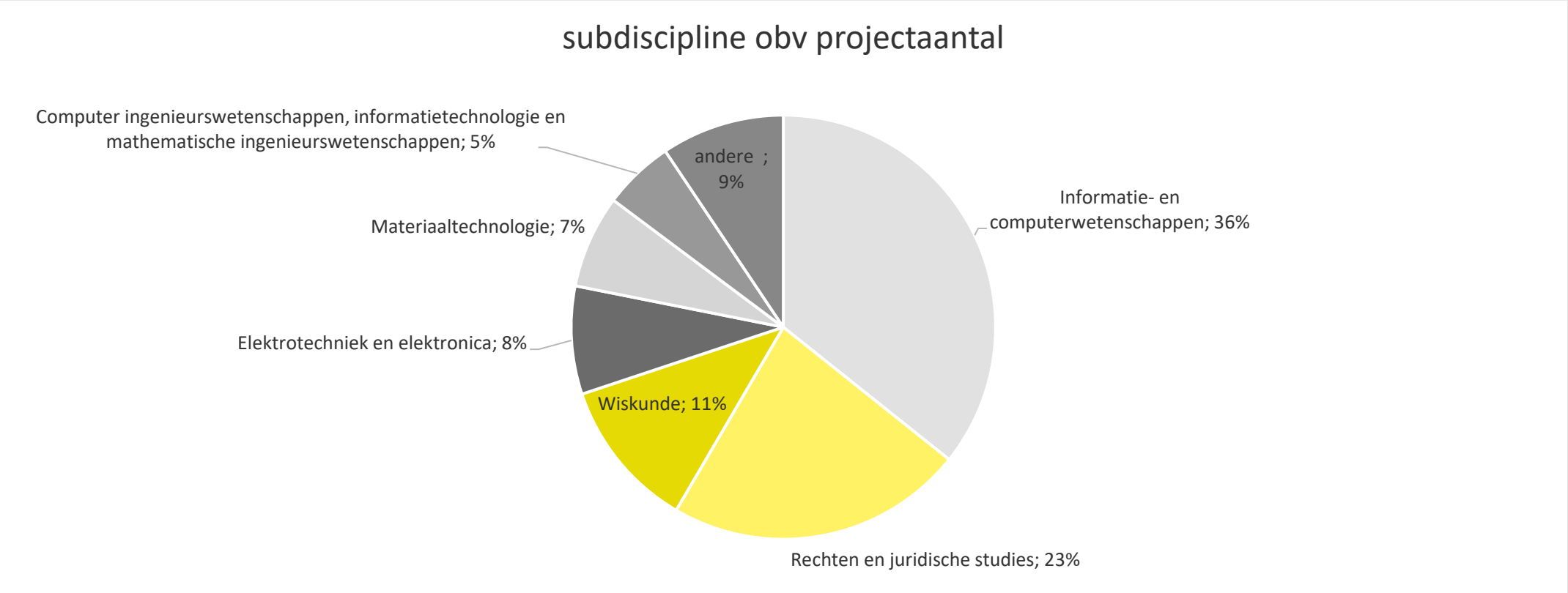
Cybersecurity-onderzoek in Vlaanderen, zoals gevonden in FRIS, lijkt de laatste jaren toe te nemen wanneer men kijkt naar projecten. Die stijgende trend wordt niet bevestigd bij de publicaties.

Budgetverdeling volgens financieringsbron (o.b.v. 181 projecten)



Cybersecurity-onderzoek in Vlaanderen, aanwezig in FRIS, is in hoofdzaak gefinancierd vanuit VLAIO (40%) en H2020/7KP (34%).

Wetenschapssubdisciplines bij Cybersecurity onderzoek (o.b.v. 181 projecten)



Cybersecurity onderzoek in Vlaanderen situeert zich in hoofdzaak in de subdomeinen van Informatie- en computerwetenschappen (36%), Rechten en juridische studies (23%) en Wiskunde (11%).

Onderzoeksgroepen in detail

- **In wat volgt worden een aantal onderzoeksgroepen meer in detail bekeken. Hierbij werden niet alle gevonden onderzoeksgroepen bekeken maar werden de meest relevante geselecteerd volgens een aantal criteria:**
  - → Onderzoeksgroepen met een zoekhit in de informatie van de onderzoeksgroep zelf
  - → Onderzoeksgroepen met een zoekhit in de informatie van de projecten
  - → Onderzoeksgroepen met een zoekhit in de informatie van de publicaties
- **De onderzoeksgroepen werden samengebracht, en dat leverde 161 unieke onderzoeksgroepen op**
  - → Hierna worden een aantal onderzoeksgroepen getoond met een hoog aantal zoekhits (de zoekhits in organisatie, projecten en publicaties werden samengeteld)
  - → De VUB-groepen Metajuridica, Faculteit Recht en Criminologie, en Recht Wetenschap Technologie en Samenleving hebben voor een groot gedeelte dezelfde gekoppelde projecten en publicaties. De eerste is het departement ingebed in de Faculteit Recht en Criminologie, de tweede de faculteit, en de derde is een onderzoeksgroep. Enkel voor deze derde is er een detailfiche uitgewerkt.

Onderzoekgroepen met meeste zoekhits op Cybersecurity

Onderzoeksgroep	Instelling	Verantwoordelijke	Hit in Organisatie	Hit in Project	Hit in Publicatie	Totaal
Computerbeveiliging en Industriële Cryptografie (COSIC)	KU Leuven	Bart Preneel	1	78	133	211
Metajuridica[1]	VUBrussel		0	12	163	175
Recht Wetenschap Technologie en Samenleving[1]	VUBrussel	Serge Gutwirth	1	7	136	144
Onderzoekseenheid KU Leuven Centrum voor IT & IE Recht	KU Leuven	Maria-Christina Janssens	0	39	46	85
Faculteit Recht en Criminologie[1]	VUBrussel		0	5	76	81
Fundamentele rechten centrum	VUBrussel	Paul De Hert	0	2	66	68
Europees Criminologisch Recht	VUBrussel		0	0	53	53
Gedistribueerde en Veilige Software (DistriNet)	KU Leuven	Wouter Joosen	0	11	32	43
Digitale Wiskunde	VUBrussel		1	1	24	26
Industriële Wetenschappen & Technologie	VUBrussel		0	1	24	25
Vakgroep Metajuridica, Privaat- en Ondernemingsrecht	UGent	Georges Martyn, Gerd Verschelden, Michel Tison, Piet Taelman	0	2	22	24
Afdeling Informatica	KU Leuven		0	11	9	20
Industriële Ingenieurswetenschappen	VUBrussel	Joannes Schoukens	0	1	18	19
Vakgroep Criminologie, Strafrecht en Sociaal Recht	UGent	Gert Vermeulen	0	2	17	19

1: Deze groepen zijn samen betrokken bij een aantal van de gevonden projecten en publicaties.

Vlaamse overheid

Detailfiches

Enkele groepen uit de overzichtslijst

Computerbeveiliging en Industriële Cryptografie (COSIC)

Bart Preneel

# objecten met zoekhit:	
Onderzoeksgroep	**1**
Projecten	**78**
Publicaties	**133**

Hoofddisciplines: Ingenieurswetenschappen en technologie
Disciplines: Algebra, Andere informatie- en computerwetenschappen, Communicatie, Communicatietechnologie, Computerarchitectuur en -netwerken, Distributed computing, Informatiesystemen, Informatiewetenschappen, Modellering, Multimediaverwerking, Programmeertalen, Scientific computing, Theoretische informatica, Toegepaste wiskunde, Visual computing
Trefwoorden: authentication, cryptografie, cyberbeveiliging, hardware beveiliging, netwerkbeveiliging, privacy, software beveiliging, systeembeveiliging

Onderzoeksgroep Computerbeveiliging en Industriële CryptografieDe COSIC onderzoeksgroep heeft een ruime expertise in digitale veiligheid. Op basis van deze expertise ontwikkelt COSIC innovatieve beveiligingsoplossingen die rekening houden met privacy en gebruiksvriendelijkheid.Het onderzoek in COSIC richt zich op het ontwerp, de evaluatie en de implementatie van cryptografische algoritmen en protocollen, de ontwikkeling van beveiligingsarchitecturen voor informatie- en communicatiesystemen, het creëren van hardware en software beveiligingsmechanismen voor ingebedde systemen en het ontwikkelen van privacy-vriendelijke oplossingen. Specifieke technologieën die bestudeerd worden zijn post-quantum cryptografie, Volledige Homomorfe Encryptie, Multi-Party Computation (MPC), block chain, drempel oplossingen tegen fysische aanvallen, whitebox cryptografie, PUFs (Physical Unclonable Functions), veilige processoren en mixnets.Ons onderzoek vindt zijn toepassing in omgevingen van cloud tot het Internet der Dingen (IoT); de applicaties omvatten elektronische betalingen en cryptomunten, mobiele authenticatie, digitaal stemmen, biometrie, medische implantaten, slimme wagens en slimme steden.

Projecten met zoekhit:

Flipchip machine voor het afbinden van chips met veel in- en uitgangen (1/01/2021 - 31/12/2022)
Cryptografie beveiligd tegen fysieke aanvallen (4/12/2020 - 4/12/2024)
Toepassingen van MPC (8/10/2020 - 8/10/2024)
Symmetrische cryptografische primitieven met een lage complexiteit (1/10/2020 - 30/09/2023)
MOZAIK: Schaalbaar en veilig delen van data (1/10/2020 - 30/09/2024)
Onderzoek naar fysieke aanval met behulp van elektromagnetische golven tegen op ringoscillatoren gebaseerde generator voor echte willekeurige getallen (28/09/2020 - 28/09/2024)
Verbeteren van roostergebaseerde cryptografische constructies voor een veilige en digitale wereld (28/09/2020 - 28/09/2024)
Praktisch toepasbare privacy verbeterende technieken (9/09/2020 - 9/09/2024)
Wiskundige aspecten van veilige computaties (20/08/2020 - 20/08/2024)
Black-box-beveiliging van White-box-cijfers (15/07/2020 - 15/07/2024)
Consensus bereiken in blockchains (10/07/2020 - 10/07/2024)
Veilige Berekening en Smart Grids (22/06/2020 - 22/06/2024)
Mobile Web Privacy en beveiliging (6/04/2020 - 6/04/2024)
Efficiëntere veilige MPC-protocollen (12/02/2020 - 12/02/2024)
Ontwerp en implementatie van veilige distance bounding protocollen (12/02/2020 - 12/02/2024)
Ontwerp van algoritmische tegenmaatregelen ter bescherming van implementaties tegen fysieke aanvallen (7/02/2020 - 3/02/2021)
Naar de Volgende Generatie Anonieme Communicatiesystemen: Verbetering van het Bestuur, de Veerkracht en de Schaalbaarheid (10/01/2020 - 10/01/2024)

Computerbeveiliging en Industriële Cryptografie (COSIC) - vervolg

Bart Preneel

Projecten met zoekhit - vervolg:

Gedistribueerde consensusprotocollen en blockchain (8/01/2020 - 8/01/2024)
Privacyvriendelijke handel in stroomflexibiliteit (1/01/2020 - 30/06/2022)
Post-Kwantumcryptografische Protocollen (1/01/2020 - 25/11/2023)
Nieuwe vertrouwde computerarchitecturen die bestand zijn tegen zijkanaal- en foutaanvallen (14/10/2019 - 14/10/2023)
Ontwerp en analyse van anonieme communicatie netwerken (3/10/2019 - 3/10/2023)
Gevorderde Methoden in Cryptoanalyse (1/10/2019 - 30/09/2022)
Analyse van privacyvriendelijke patroonvergelijking met behulp van homomorfe encryptie (1/10/2019 - 30/09/2022)
Implementatie uitdagingen van cryptografie gebaseerd op roosters. (1/10/2019 - 17/07/2023)
Cybersecurity (1/09/2019 - 31/08/2029)
Geünificeerde grondbeginselen voor de lineaire en differentiële cryptanalyse van permutatie-gebaseerde cryptografie (27/08/2019 - 27/08/2023)
Verona (3/06/2019 - 2/06/2020)
Beveiligingsoplossingen voor het Internet der Dingen, gebaseerd op blockchain technologie. (27/05/2019 - 27/05/2023)
MPC-protocollen en applicaties (21/03/2019 - 21/03/2023)
Evaluatie van trade-offs tussen performantie en veiligheid in hardware en systeem software (1/01/2019 - 31/12/2022)
Locatie-beveiligde cryptografische oplossingen gebaseerd op akoestische signalen voor slimme geconnecteerde systemen en passieve toestellen (1/01/2019 - 31/12/2022)
Toolkit voor gegevensbescherming om risicos in ziekenhuizen en zorgcentra te verminderen (1/01/2019 - 31/12/2022)
Post-kwantum cryptografie. (23/10/2018 - 23/10/2022)
Quantum Random Number Generators: goedkoper, sneller en veiliger (1/10/2018 - 30/09/2021)
Nieuwe Blokcijferstructuren (1/10/2018 - 30/09/2024)
Cryptanalyse van post-quantum cryptografie (1/10/2018 - 30/09/2022)
Veilige microarchitecturen voor betrouwbare uitvoeringseenheden (1/10/2018 - 9/08/2022)
Module-lattice-gebaseerde cryptografie in volgende generatie platforms (1/10/2018 - 9/03/2020)
Generische methodiek om werkelijke willekeur te genereren in geïntegreerde schakelingen. (17/09/2018 - 31/12/2022)
Wiskundige aanpak voor de evaluatie van de veiligheid van blokcijfers tegen lineaire en differentiële cryptanalyse (27/04/2018 - 31/12/2022)
Functionele coderingstechnologieën. (1/01/2018 - 31/12/2020)
Lichtgewicht cryptoanalyse met blockcipher (21/11/2017 - 21/11/2021)
Publieke en private willekeur in cryptografie (9/11/2017 - 9/11/2021)
Post-kwantum cryptografie voor het internet der dingen (11/10/2017 - 30/09/2019)
Nieuwe Methoden in White-Box Cryptografie (29/09/2017 - 30/09/2022)
Algorithmische Tegenmaatregelen Tegen Passieve en Actieve Fysieke Aanvallen (27/09/2017 - 31/12/2022)
Praktijkgerichte beveiligingsmodellen en granulaire ontwerpen voor toekomstbestendige geauthenticeerde versleuteling (1/09/2017 - 31/08/2019)
Cybersecurity en privacy-dialoog tussen Europa en Japan (1/06/2017 - 31/05/2019)
Cijferkunst en computerarchitectuur voor post-quantum cryptografie (16/01/2017 - 16/01/2021)
Veilige en efficiënte berekeningen op privé-gegevens (13/01/2017 - 13/01/2021)
Delende cryptanalyse van symmetrische cijfers (9/11/2016 - 27/05/2019)
Ontwerpmethodologieën en beveiligingsevaluaties voor echte willekeurige getallen generatoren (6/10/2016 - 6/10/2020)
Cryptanalyse van ARC cijfers (1/10/2016 - 31/12/2020)

Computerbeveiliging en Industriële Cryptografie (COSIC) – vervolg 2

Bart Preneel

Projecten met zoekhit - vervolg:

Post-Snowden circuits en ontwerpmethoden voor beveiliging (1/09/2016 - 31/08/2021)
Praktische fout-injectie in cryptografische processoren (18/05/2016 - 18/05/2020)
CRYPTOGRAPHY: Cryptography secured against side-channel attacks and fault attacks by means of treshold implementations (1/04/2016 - 31/12/2019)
Ontwerp en verificatie van maatregelen tegen aanvallen gebaseerd op nevenkanalen en geïnduceerde fouten (3/03/2016 - 29/05/2020)
Veiligheid van cryptografische implementaties (14/01/2016 - 14/01/2020)
Een beveiligingsarchitectuur voor het Internet of Things (1/01/2016 - 31/12/2019)
Privacy-vriendelijke protocollen voor cloud beveiliging (15/12/2015 - 1/07/2017)
Lichtgewicht cryptografische cijfers ter bescherming tegen nevenkanaal- en foutaanvallen (14/12/2015 - 14/12/2019)
Zeer betrouwbare fysisch onkloonbare functies: Ontwerp, karakterisatie en veiligheidsanalyse (11/12/2015 - 11/02/2020)
Lineaire cryptanalyse van ARX-gebaseerde blokcijfers (13/11/2015 - 13/11/2019)
Evaluatie van nevenkanaal aanvalbestendige cryptografische implementaties tijdens de ontwerpfase (4/11/2015 - 28/10/2020)
Een brug te ver? Privacy by design in het tijdperk van cybersecurity. (1/10/2015 - 30/04/2019)
Volledig homomorfe vercijfering en multilineaire afbeeldingen (1/10/2015 - 30/09/2020)
Beveiliging en privacy voor cyber-fysische systemen en het Internet van de Dingen (1/10/2015 - 30/09/2021)
Theorie Ontmoet Praktijk voor Veilige Embedded Systemen. (1/10/2015 - 28/04/2019)
. (8/09/2015 - 13/02/2020)
Privacy en verantwoordelijkheid in netwerken via geoptimaliseerde gerandomiseerde Mix-nets (1/09/2015 - 31/08/2018)
Optimalisaties van volledig homomorfe encryptie (12/08/2015 - 27/05/2019)
Europees geïntegreerd onderzoeksopleidingsnetwerk voor geavanceerde cryptografische technologieën voor het internet der dingen en de cloud. (1/03/2015 - 28/02/2019)
Europese coördinatie- en ondersteuningsactie in cryptologie (1/03/2015 - 30/09/2019)
Hardware Enabled Crypto en willekeurigheid. (1/03/2015 - 28/02/2018)
Post-quantum cryptografie voor langetermijnbeveiliging (1/03/2015 - 28/02/2018)
Homomorfe coderingstoepassingen en -technologie. (1/01/2015 - 31/12/2017)
Versterking van privacy en veiligheid in niet-vertrouwde omgevingen (1/01/2015 - 31/12/2017)

Publicaties met zoekhit:

On Detecting Relay Attacks on RFID Systems Using Qubits (2020)
Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography (2020)
Highly Reliable Physically Unclonable Functions: Design, Characterization and Security Analysis (2020)
A framework for cryptographic problems from linear algebra (2020)
Design Time Evaluation for Side-Channel Attack Resistant Cryptographic Implementations (2020)
Dismantling DST80-based Immobiliser Systems (2020)
New Methods for Symmetric Cryptography (2020)
Cryptography in the Presence of Physical Attacks: Design, Implementation and Analysis (2020)
Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols (2020)
Systematic Analysis of Randomization-based Protected Cache Architectures (2020)
Collaborative Authentication Using Threshold Cryptography (2020)
Design and Verification of Side-Channel and Fault Attacks Countermeasures (2020)
Forkcipher: A New Primitive for Authenticated Encryption of Very Short Messages (2019)
Efficient and Privacy-Preserving Cryptographic Key Derivation From Continuous Sources (2019)

Computerbeveiliging en Industriële Cryptografie (COSIC) – vervolg 3

Bart Preneel

Publicaties met zoekhit - vervolg:

Improved Interpolation Attacks on Cryptographic Primitives of Low Algebraic Degree (2019)
Arithmetic Considerations for Isogeny Based Cryptography (2019)
Security on Plastics: Fake or Real? (2019)
Security of Cryptographic Implementations (2019)
Problems and solutions from the fourth International Students Olympiad in Cryptography (NSUCRYPTO) (2019)
On the Difficulty of Using Patients Physiological Signals in Cryptographic Protocols (2019)
Compact and Flexible FPGA Implementation of Ed25519 and X25519 (2019)
The Fifth International Students? Olympiad in cryptography?NSUCRYPTO: Problems and their solutions (2019)
Classification of Balanced Quadratic Functions (2019)
Optimisations of Fully Homomorphic Encryption (2019)
Arithmetic of tau-adic expansions for lightweight Koblitz curve cryptography (2018)
Editorial: Special issue on recent trends in cryptography (2018)
From Keys to Databases-Real-World Applications of Secure Multi-Party Computation (2018)
On-chip jitter measurement for true random number generators (2018)
Constant-time Discrete Gaussian Sampling (2018)
PUF Constructions with Limited Information Leakage (2018)
Privacy-Preserving Biometric Authentication Model for e-Finance Applications (2018)
Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM (2018)
Collateral damage of Facebook third-party applications: a comprehensive study (2018)
Digital Signatures and Signcryption Schemes on Embedded Devices: a Trade-off between Computation and Storage (2018)
Cryptography Secured Against Side-Channel Attacks (2018)
Computational problems in supersingular elliptic curve isogenies (2018)
True Random Number Generators for FPGAs (2018)
Towards Inter-Vendor Compatibility of True Random Number Generators for FPGAs (2018)
Towards Efficient and Automated Side Channel Evaluations at Design Time (2018)
Sound hashing modes of arbitrary functions, permutations, and block ciphers (2018)
Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography (2018)
Impact analysis of SBAS authentication (2018)
Detection of IEMI Fault Injection Using Voltage Monitor Constructed with Fully Digital Circuit (2018)
Immunological algorithms paradigm for construction of Boolean functions with good cryptographic properties (2017)
Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things (2017)
Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory (2017)
Does Coupling Affect the Security of Masked Implementations? (2017)
Directivity Assessment of MEMS Microphones in Microphone Array Applications (2017)
Towards Quantum Distance Bounding Protocols (2017)
A Practical Multivariate Blind Signature Scheme (2017)
On the Construction of Side-Channel Attack Resilient S-boxes (2017)
On the Evolution of Bent (n, m) Functions (2017)
Security Analysis of PUF-based Key Generation and Entity Authentication (2017)
Design of S-boxes Defined with Cellular Automata Rules (2017)
Public Key Cryptography on Hardware Platforms: Design and Analysis of Elliptic Curve and Lattice-based Cryptoprocessors (2017)
Cryptanalysis of Symmetric-key Primitives (2017)
Single-Trace Side-Channel Attacks on Scalar Multiplications with Precomputations (2017)
Template attack versus Bayes classifier (2017)
Short Solutions to Nonlinear Systems of Equations (2017)
Side-channel analysis and machine learning: A practical perspective (2017)
SOFIA: Software and Control Flow Integrity Architecture (2017)
Trapdoor Computational Fuzzy Extractors and Stateless Cryptographically-Secure Physical Unclonable Functions (2017)
Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy? (2017)
Efficient methods to generate cryptographically significant binary diffusion layers (2017)
Sancus 2.0: A low-cost security architecture for IoT devices (2017)
Security Adds an Extra Dimension to IC Design (2017)
Area-optimized montgomery multiplication on IGLOO 2 FPGAs (2017)
High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers (2017)
Finding short and implementation-friendly addition chains with evolutionary algorithms (2017)

Computerbeveiliging en Industriële Cryptografie (COSIC) – vervolg 4

Bart Preneel

Publicaties met zoekhit - vervolg:

An Easy-to-Use Tool for Rotational-XOR Cryptanalysis of ARX Block Ciphers (2017)
Hypersurfaces in Weighted Projective Spaces Over Finite Fields with Applications to Coding Theory (2017)
Dude, is my code constant time? (2017)
Cherry-Picking Reliable PUF Bits with Differential Sequence Coding (2016)
Upper Bounds on The Min-Entropy of RO Sum, Arbiter, Feed-Forward Arbiter, and S-ArbRO PUFs (2016)
Efficient Finite field multiplication for isogeny based post quantum cryptography. (2016)
Evolving Cryptographic Pseudorandom Number Generators (2016)
Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications (2016)
On the Feasibility of Cryptography for a Wireless Insulin Pump System (2016)
Hardware Acceleration of a Software-based VPN (2016)
A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography using Lambda Coordinates (2016)
Masking AES with d+1 Shares in Hardware (2016)
Maximal Nonlinearity in Balanced Boolean Functions with Even Number of Inputs, Revisited (2016)
Ring-LWE: Applications to cryptography and their efficient realization (2016)
Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties (2016)
Cryptographic Boolean functions: One output, many design criteria (2016)
A Tiny Coprocessor for Elliptic Curve Cryptography over the 256-bit NIST Prime Field (2016)
Exploring the Use of Shift Register Lookup Tables for Keccak Implementations on Xilinx FPGAs (2016)
Analysis and Design of Masking Schemes for Secure Cryptographic Implementations (2016)
Improved impossible differential attack on reduced version of Camellia with FL/FL-1 functions (2016)
Insynd: Improved Privacy-Preserving Transparency Logging (2016)
Provably Weak Instances of Ring-LWE Revisited (2016)
Improving the Sphinx Mix Network (2016)
Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm (2016)
On the choice of the appropriate AES data encryption method for ZigBee nodes (2016)
Practically Efficient Secure Single-Commodity Multi-Market Auctions (2016)
Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography (2016)
A 5.1µJ per point-multiplication elliptic curve cryptographic processor (2016)
Evolving Algebraic Constructions for Designing Bent Boolean Functions (2016)
Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography (2016)
A New Cost Function for Evolution of S-boxes (2016)
A MAC Mode for Lightweight Block Ciphers (2016)
DES S-box generator (2016)
Recipient Privacy in Online Social Networks (2016)
On Error Distributions in Ring-based LWE (2016)
Theory of implementation security workshop (TLS 2016) (2016)
Evolutionary Algorithms for Finding Short Addition Chains: Going the Distance (2016)
Evolutionary Computation and Cryptology (2016)
Binary decision diagram to design balanced secure logic styles (2016)
Leaky Birds: Exploiting Mobile Application Traffic for Surveillance (2016)
Security of Keyed Sponge Constructions Using a Modular Proof Approach (2015)
Circuit challenges from cryptography (2015)
A New Classification of 4-bit Optimal S-boxes and its Application to PRESENT, RECTANGLE and SPONGENT (2015)
Provoking Security: Spoofing attacks against crypto-biometrics (2015)
Galileo Open Service Authentication: A Complete Service Design and Provision Analysis (2015)
Efficient Ring-LWE Encryption on 8-bit AVR Processors (2015)
Evolutionary Approach for Finding Correlation Immune Boolean Functions of Order t with Minimal Hamming Weight. (2015)
Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis (2015)
A masked ring-LWE implementation (2015)
Highly Efficient Entropy Extraction for True Random Number Generators on FPGAs (2015)
Trade-offs for Threshold Implementations Illustrated on AES (2015)
Compact Implementations of Multi-Sbox Designs (2015)
Open Problems in Hash Function Security (2015)
Efficient Software Implementation of Ring-LWE Encryption (2015)

Computerbeveiliging en Industriële Cryptografie (COSIC) – vervolg 5

Bart Preneel

Publicaties met zoekhit - vervolg:

Mathematicians discuss the Snowden revelations: Cryptographic standards, mass surveillance, and the NSA (2015)
Lightweight PUF-based Key and Random Number Generation (2015)
Practical identity-based private sharing for online social networks (2015)
Challenges in designing trustworthy cryptographic co-processors (2015)
Lightweight Coprocessor for Koblitz Curves: 283-bit ECC Including Scalar Conversion with only 4300 Gates (2015)
Purchase details leaked to PayPal (2015)
A bimodal verification cryptosystem as a framework against spoofing attacks (2015)
PROBLEMS, SOLUTIONS AND EXPERIENCE OF THE FIRST INTERNATIONAL STUDENTS OLYMPIAD IN CRYPTOGRAPHY (2015)
Cryptography and Information Security in the Post-Snowden Era (2015)
Inner Product Masking Revisited (2015)

Recht Wetenschap Technologie en Samenleving (LSTS)

Serge Gutwirth

# objecten met zoekhit:	
Onderzoeksgroep	1
Projecten	7
Publicaties	136

Hoofddiscipline: Sociale wetenschappen
Disciplines: Algemene pedagogische en onderwijswetenschappen, Rechten, Toegepaste sociologie
Trefwoorden: Legal aspects of science and technology studies

De interdisciplinaire onderzoeksgroep LSTS, opgericht in 2003 aan de Vrije Universiteit Brussel (VUB) is gewijd aan analytisch, theoretisch en prospectief onderzoek naar de relaties tussen recht, wetenschap, technologie en samenleving. De kerndeskundigheid van LSTS is het recht, maar we hebben ook een sterke reputatie in de juridische theorie, de wetenschapsfilosofie en de bioethiek, en we doen ook criminologische (surveillance & security) en STS-onderzoek.

Projecten met zoekhit:
SRP-Onderzoekszwaartepunt: Articulating Law, Technology, Ethics and Politics: Issues of Enforcement and Jurisdiction of EU Data Protection Law under and beyond the General Data Protection Regulation (ALTEP-DP) (1/03/2019 - 29/02/2024)
Europese data onderworpen aan (privacy)recht in grensoverschrijdende data stromen (1/10/2018 - 30/09/2022)
STAR II (1/06/2018 - 31/12/2020)
STAR: Ondersteunende trainingsactiviteiten voor de databeschermingshervorming (1/11/2017 - 31/10/2019)
Cybersecurity-accelerator voor vertrouwde IT-ecosystemen in het MKB (FORTIKA) (1/06/2017 - 31/05/2020)
Forensisch bewijs verzamelen autonome sensor (FORENSOR) (1/09/2015 - 28/02/2019)
Een risico voor een recht? Verkenning van een nieuw begrip binnen het recht op bescherming van persoonsgegevens (1/01/2015 - 31/12/2018)

Publicaties met zoekhit:
The Achilles Heel of EU data protection in a law enforcement context: international transfers under appropriate safeguards in the law enforcement directive (2020)
Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection (2020)
The Proposed ePrivacy Regulation: The Commissions and the Parliaments Draft s at a Crossroads? (2020)
Handbook on Data Protection in Humanitarian Action - Second Edition (2020)
A reflection of current oversight measures of the use of surveillance technology by the local police in Belgium (2020)
Een reflectie over het huidig toezicht van het gebruik van surveillancetechnologie door de lokale politie in België (2020)
Article 40 Commentary (2020)
Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms? (2020)
Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR (2020)
Commentaries on Articles 9, 44, 45, 46, 47, 48, 49, and 50 (2020)
Shortcomings of the Passenger Namer Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union (2020)
Vulnerable Data Subjects (2020)
The concept of fairness in the GDPR: a linguistic and contextual interpretation (2020)
The EU General Data Protection Regulation: A Commentary (2020)
Comparing LED and GDPR adequacy (2020)
Biometric Data in the EU (Reformed) Data Protection Framework and Border Management: A Step Forward or an Unsatisfactory Move? (2020)
Article 41 Commentary (2020)
Big data analytics in electronic communications (2020)

Recht Wetenschap Technologie en Samenleving (LSTS) - vervolg

Serge Gutwirth

Publicaties met zoekhit - vervolg:

Composting and computing: On digital security compositions (2019)
The Internet and the Global Reach of EU Law (2019)
Responsibility for Data Protection in a Networked World (2019)
El Comité Europeo de Protección de Datos (CEPD): Territorio Desconocido (2019)
The European Data Protection Board (EDPB): Unknown territory (2019)
Data Protection by Design for Cybersecurity Systems in a Smart Home Environment (2019)
Data protection policies in EU justice and home affairs (2019)
International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law (2019)
Data Protection and the EPPO (2019)
Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles (2019)
Digital Security and Human Rights: A Plea for Counter-Infringement Measures (2019)
Cyber-Trust: The Shield for IoT Cyber-Attacks (2019)
The new EU cybersecurity framework (2019)
Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective (2019)
What is Equivalent? A Probe into GDPR Adequacy based on EU Fundamental Rights (2019)
The right to data portability in the GDPR: Towards user-centric interoperability of digital services (2018)
Practical challenges to the right to data portability in the collaborative economy (2018)
Data As Counter-Performance: A New Way Forward Or A Step Back For The Fundamental Right Of Data Protection? (2018)
Data Protection by Design and by Default (2018)
Door-to-door preaching by Jehovahs Witnesses community falls under data protection law (2018)
Léternel retour de la propriété des données : de linsistance dun mot dordre (2018)
Data Protection Certification in the EU (2018)
Transparency as translation in data protection (2018)
Right engineering? The redesign of privacy and personal data protection (2018)
Privacy and Data Protection Seals (2018)
Data Protection and Privacy: The Internet of Bodies (2018)
The role of the data protection authorities in supervising police and criminal justice authorities processing personal data (2018)
International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15 (EU-Canada PNR) (2018)
The price is (not) right: data protection and discrimination in the age of pricing algorithms (2018)
The Right of Access Under the Police Directive: Small Steps Forward (2018)
Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research (2018)
Understanding the notion of risk in the General Data Protection Regulation (2018)
Data protection by design: promises and, perils in crossing the Rubicon between law and engineering (2018)
Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data (2017)
The legal significance of individual choices about privacy and personal data protection (2017)
Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy (2017)
European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards Good Enough Judicial Oversight (2017)
Data Protection and Privacy: The Age of Intelligent Machines, (2017)
The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment (2017)
A Security Union In Full Respect Of Fundamental Rights (2017)
Landscape with the Rise of Data Privacy Protection (2017)
Handbook on Data Protection in Humanitarian Action (2017)
Mapping the legal and administrative frameworks of informational rights in Europe. A cross-European comparative analysis (2017)
On Risk, Balancing, and Data Protection: A Response to van der Sloot (2017)
The Anonymisation of Research Data — A Pyric Victory for Privacy that Should Not Be PushednToo Hard by the EU Data Protection Framework? (2017)
A behavioural alternative to the protection of privacy (2017)
A European perspective on data protection and the right of access (2017)
Co-regulation in EU personal data protection: the case of technical standards and the Privacy by Design standardisation 'mandate' (2017)
Preface: Yet Another Book about Snowden and Safe Harbor? (2017)
Trans-Atlantic Data Privacy Relations as a Challenge for Democracy (2017)

Recht Wetenschap Technologie en Samenleving (LSTS) – vervolg 2

Serge Gutwirth

Publicaties met zoekhit - vervolg:

Why the GDPR risk-based approach is about compliance risk, and why its not a bad thing (2017)
Cloud computing and data processing: sorting out legal requirements (2017)
Reality and Illusion in EU Data Transfer Regulation Post Schrems (2017)
The rich UK contribution to the field of EU data protection: Lets not go for “third country” status after Brexit (2017)
Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (2017)
Data Protection’s Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer (2017)
Genetic Classes and Genetic Categories: Protecting Genetic Groups through Data Protection Law (2017)
Data Protection Law and International Dispute Resolution (2017)
Courts, privacy and data protection in Spain: Experiencing data protection’s dominance (2017)
Exercising access rights in Belgium (2017)
Data Protection and Privacy: (In)visibilities and Infrastructures (2017)
Courts, Privacy and Data protection in Belgium: Fundamental rights that might as well be struck from the Constitution (2017)
The Unaccountable State of Surveillance. Exercising Access Rights in Europe (2017)
The new General Data Protection Regulation: Still a sound system for the protection of individuals? (2016)
Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research (2016)
The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR (2016)
Data protection authority perspectives on the impact of data protection reform on cooperation in the EU (2016)
Towards Harmonised Duties of Care and Diligence in Cybersecurity (2016)
Enforcing Privacy. Regulatory, Legal and Technological Approaches (2016)
The co-existence of administrative and criminal law approaches to data protection wrongs (2016)
EU Data Protection and Future Payment Services (2016)
IoT standardization. The approach in the field of data protection as a model for ensuring compliance of IoT applications? (2016)
Behavioural Profiling in the Post-constitutionalisation Data Protection Regime (2016)
Nothing is as it seems. The exercise of access rights in Italy and Belgium: dispelling fallacies in the legal reasoning from the ‘law in theory’ to the ‘law in practice’ (2016)
Data Protection and Privacy. European Data Protection Reform (2016)
EU Criminal Law and Fundamental Rights (2016)
Visions of Technology (2016)
The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection (2016)
Európai Kézikönyv a Magánszféra - és a Személyes Adatok Védelméről Iskolák Számára (2016)
The European Handbook for Teaching Privacy and Data Protection at Schools (2016)
Data Protection on the Move (2016)
Introduction to Enforcing Privacy (2016)
Un-mapping Personal Data Transfers (2016)
Redefining the smart grids’ smartness. Or why it is impossible to adequately address their risks to privacy and data protection if their environmental dimension is overlooked (2016)
Predictive Profiling and its Legal Limits: Effectiveness Gone Forever? (2016)
We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection (2016)
Wearables, Health and Privacy: A European Perspective (2016)
Europejski podręcznik: Nauczanie o ochronie danych i prywatności w szkołach (2016)
Evropski priročnik za poučevanje zasebnosti in varstva osebnih podatkov v šolah (2016)
A risk to a right? Beyond data protection risk assessments (2016)
Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context (2016)
The New Police And Criminal Justice Data Protection Directive. A First Analysis (2016)
Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters? (2015)
The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet (2015)
The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges (2015)
Assessing the European approach to privacy and data protection in smart grids. Lessons for emerging technologies (2015)
Google Spain: Addressing Critiques and Misunderstandings One Year Later (2015)
EU’s One-Stop-Shop Mechanism: Thinking Transnational (2015)
Extraterritoriality and regulation of international data transfers in EU data protection law (2015)

Recht Wetenschap Technologie en Samenleving (LSTS) – vervolg 3

Serge Gutwirth

Publicaties met zoekhit - vervolg:

The proceduralisation of data protection remedies under EU data protection law: towards a more effective and data subject-oriented remedial system? (2015)
Preface to Reforming European Data Protection (2015)
Data protection: the EU institutions' battle over data processing vs individual rights (2015)
Cooperation between the private sector and law enforcement agencies: an area in between legal regulations (2015)
The accountability culture in its european union dress. Sticks but no carrots to make the proposed data protection regulation work (2015)
Smart Grid Security (2015)
Enforcing privacy: lessons from current implementations and perspectives for the future (2015)
Towards efficient cooperation between supervisory authorities in the area of data privacy law (2015)
Google Spain in the EU and international context (2015)
Reforming European Data Protection (2015)
Curtailing a Right in Flux (2015)
Introduction to Enforcing privacy (2015)
Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative (2015)
Developing and testing a surveillance impact assessment methodology (2015)
Drones. Current challenges and standardisation solutions in the field of privacy and data protection (2015)
The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents? (2015)
Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling (2015)
Smart Technologies and the End(s) of Law (2015)
Understanding data protection as risk regulation (2015)

Onderzoekseenheid KU Leuven Centrum voor IT & IE Recht

Maria-Christina Janssens

# objecten met zoekhit:	
Onderzoeksgroep	0
Projecten	39
Publicaties	47

Hoofddisciplines: Sociale wetenschappen
Disciplines: Andere rechten en juridische studies, Rechten
Trefwoorden: Law

De Onderzoekseenheid KU Leuven Centrum voor IT & IE Recht heeft een solide track record als een recht en ethiek partner van grote internationale en interdisciplinaire onderzoeksprojecten. Het is internationaal bekend om zijn expertise op het gebied van data privacy en informatiebeveiligingsrecht, nieuwe media en communicatie wetgeving, Information Rights Management, intellectuele eigendomsrecht en juridische aspecten van ehealth.Onze onderzoekers richten zich op de fundamentele heroverweging van het huidige wettelijke kader, dat is noodzakelijk geworden door de snelle evolutie van de technologie op verschillende gebieden, zoals overheid, media, gezondheidszorg, informatica, onderzoek en ontwikkelingen in de digitale economie, het bankwezen, transport, cultuur, enz.

Projecten met zoekhit:

Gegevensintegriteit en elektronisch bewijs in het licht van grensoverschrijdende e-commerce (6/02/2021 - 6/02/2025)
ESR 13 Conceptueel kader voor het gebruik en de regulering van nieuwe biometrische gegevens (TreSPasS) (1/10/2020 - 1/10/2024)
Privacy- en gegevensbeschermingskwesties van biometrische blockchain-identiteiten (1/10/2020 - 1/10/2024)
MOZAIK: Schaalbaar en veilig delen van data (1/10/2020 - 30/09/2024)
Sparkle (Studie over de aanpak van veiligheids-, Privacy- en Autonomie-Risicos door middel van Legal Engineering). (1/10/2020 - 30/09/2025)
Privacy en biometrie bij het volgen van gezondheid en activiteiten (1/09/2020 - 1/09/2024)
Sabbatperiode Peggy Valcke: SPARKLE+ (1/09/2020 - 31/08/2021)
Close-up: uw ID is uw gezicht (1/09/2020 - 31/08/2023)
Catalogus van risicos van het gebruik van biometrische gegevens en beoordeling van technische beschermingsmaatregelen (1/09/2020 - 1/09/2024)
Gegevensbescherming en aspecten van de bescherming van het privéleven bij het implementeren van NFV en SDN technologieën in 5G netwerken (13/05/2020 - 13/05/2026)
AVG en big health data. Fundamentele uitdagingen voor het EU-kader voor de bescherming van persoonsgegevens (26/02/2020 - 26/02/2026)
Training in veilige en privacy-conserverende biometrische gegevens (1/01/2020 - 31/12/2023)
Vertrouwde veilige ruimte voor het delen van gegevens (1/01/2020 - 31/12/2022)
Privacy is belangrijk (1/01/2020 - 31/12/2023)
Veilige collaboratieve intelligente industriële activa (1/12/2019 - 31/05/2022)
Bewakingsrisicos in het internet van de dingen toegepast op Smart Cities (7/11/2019 - 7/11/2025)
Het verzekeren van gegevensbescherming in de smart city: de verantwoordingsplicht in de data-intensieve, multi-actor smart city omgeving (21/10/2019 - 21/10/2025)
Massa-overdracht van persoonsgegevens van de private naar de publieke sector : een gevalstudie van predictive policing (9/09/2019 - 9/09/2023)

Onderzoekseenheid KU Leuven Centrum voor IT & IE Recht - vervolg

Maria-Christina Janssens

Projecten met zoekhit - vervolg:

Cyber Security Incident handling, waarschuwing en responssysteem voor de Europese kritieke infrastructuur (1/09/2019 - 31/08/2022)
Cybersecurity (1/09/2019 - 31/08/2029)
5e generatie beveiliging voor telecomdiensten (1/09/2019 - 31/08/2023)
Makelaardij en marktplatform voor persoonlijke gegevens (1/01/2019 - 30/11/2022)
Machinaal leren om gedeelde kennis te vergroten in gefedereerde privacybeschermende scenarios (1/12/2018 - 30/11/2021)
Veilige gegevens maakten economische ontwikkeling mogelijk (1/12/2018 - 30/11/2021)
Mechanismen die gegevens beveiligen: het beste manier om een evenwicht te vinden tussen de juridische data minimisatie en big data? (1/10/2018 - 23/04/2019)
VEILIGHEID VAN Kritieke gezondheidsinfrastructuur (1/09/2018 - 31/08/2021)
Van smartwatches tot autonome auto's : de rechten en belangen van consumenten veiligstellen in het tijdperk van slimme technologie en het Internet of Things (1/09/2018 - 1/09/2022)
Methoden en hulpmiddelen voor naleving van GDPR door middel van privacy- en gegevensbeschermingstechnieken (1/05/2018 - 31/01/2021)
GDPR Compliance Cloud Platform voor micro-ondernemingen. (1/05/2018 - 31/10/2020)
Smart city Privacy: Engageren tot Collaboratieve Transparantie in het Regelgevende Ecosysteem. (1/01/2018 - 31/12/2021)
Algoritmische transparantie en verantwoording in de praktijk (1/01/2018 - 31/12/2020)
Functionele coderingstechnologieën. (1/01/2018 - 31/12/2020)
Eerlijke of Oneerlijke Differentiatie ? Een heroverweging van de concepten gelijkheid en gegevensbescherming ter regulering van algoritmisch geïnformeerde besluitvorming (20/12/2017 - 20/12/2021)
Opstellen van een regelgevingskader voor de behandeling van softwaretekorten door nationale beveiligingsagentschappen (1/11/2017 - 1/11/2021)
Privacy-by-design Regulering in Software Engineering (PRiSE) (1/10/2017 - 30/09/2021)
Cybersecurity en privacy-dialoog tussen Europa en Japan (1/06/2017 - 31/05/2019)
Competitieve methoden om lokaal openbaar bestuur te beschermen tegen cyberbeveiliging bedreigingen (1/05/2017 - 31/10/2019)
Strafrechtelijk beslag: digiproof en (multi)functioneel ? (1/09/2015 - 29/01/2020)
Juridische grenzen aan de monitoring en exploitatie van online emoties (24/04/2015 - 30/09/2019)

Publicaties met zoekhit:

An Overview of Belgian Legislation Applicable to Biobank Research and Its Interplay with Data Protection Rules (2021)
The patient's right to privacy and autonomy against a changing healthcare model (2020)
DPMF: A Modeling Framework for Data Protection by Design (2020)
Strafrechtelijk beslag: digiproof en (multi)functioneel ? (2020)
Getting Data Subject Rights RightA submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance (2020)
Does EU Medical Devices Directive Apply to Contact Proximity Tracing Apps? (2020)
From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives (2020)
Open Source Hardware and Healthcare Collaborative Platforms: Common Legal Challenges (2020)
Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems: AG Discusses the Validity of Standard Contractual Clauses and Raises Concerns Over Privacy Shield (C-311/18 Schrems II, Opinion of AG Saugmandsgaard Øe) (2020)
The Bigger Picture: Approaches to Inter-Organizational Data Protection Impact Assessment (2020)
A data protection perspective on training in the m-health sector (2019)
A Comparison of System Description Models for Data Protection by Design (2019)

Onderzoekseenheid KU Leuven Centrum voor IT & IE Recht – vervolg 2

Maria-Christina Janssens

Publicaties met zoekhit - vervolg:

Korean data protection law: Moving towards a Korean adequacy decision? (2019)
The cybersecurity requirements for operators of essential services under the NIS directive – An analysis of potential liability issues from an EU, German and UK perspective (2019)
The by Design Turn in EU Cybersecurity Law: Emergence, Challenges and Ways Forward (2019)
The European cross-border health data exchange roadmap: Case study in the Italian setting (2019)
The legal limits to the monetisation of online emotions (2019)
Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security (2019)
An Architectural View for Data Protection by Design (2019)
Pre-Formulated Declarations Of Data Subject Consent – Citizen-Consumer Empowerment and The Alignment Of Data, Consumer and Competition Law Protections (2019)
Data protection and the role of fairness (2018)
Fairness and Enforcement: Bridging Competition, Data Protection, and Consumer Law (2018)
Gap analysis for information security in interoperable solutions at a systemic level: The KONFIDO approach (2018)
Key Ethical Challenges in the European Medical Information Framework (2018)
Comprehensive user requirements engineering methodology for secure and interoperable health data exchange (2018)
Why data protection and transparency are not enough when facing social problems of machine learning in a big data context (2018)
When data protection by design and data subject rights clash (2018)
Shattering one-way mirrors – data subject access rights in practice (2018)
How Machine Learning Generates Unfair Inequalities and How Data Protection Instruments May Help in Mitigating Them (2018)
Platforms and commercial communications aimed at children: a playground under legislative reform? (2018)
The Europol Regulation and purpose limitation: from the “silo-based approach to… what exactly? (2017)
On the Road to Privacy- and Data Protection-Friendly Security Technologies in the Workplace – A Case-Study of the MUSES Risk and Trust Analysis Engine (2017)
Looking for needles in a haystack: Key issues affecting childrens rights in the General Data Protection Regulation (2017)
Accountability for the Use of Algorithms in a Big Data Environment (2017)
Book Review: Ctrl+Z: The Right to be Forgotten. By Meg Leta Jones (2017)
Reconciling the (extra)territorial reach of the GDPR with public international law (2017)
The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework (2017)
Why Research May No Longer Be the Same: About the Territorial Scope of the New Data Protection Regulation (2016)
Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity (2016)
Online dispute resolution: Settling data protection disputes in a digital world of customers (2016)
Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation (2016)
From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain (2016)
Cyberveiligheid wordt pijler van Defensie (2015)
Oktober was de Europese Cybersecurity maand (2015)
The EU, children under 13 years and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet (2015)
Privacy by Design – The Case of Automated Border Control (2015)

Fundamentele rechten centrum (FRC)

Paul De Hert

# objecten met zoekhit:	
Onderzoeksgroep	0
Projecten	2
Publicaties	66

Hoofddiscipline: Sociale wetenschappen
Disciplines: Rechten
Trefwoorden: Human Rights

De onderzoeksgroep Mensenrechten coordineert en centraliseert de vele aan mensenrechten gekoppelde onderzoeksprojecten in de Rechtsfaculteit. Zowel de theorie van de mensenrechten, de nationale wetgeving inzake mensenrechten (grondwettelijk recht, strafrecht, civiel recht, ...) en Internationaal humanitair recht worden samen gebracht met als doel het ontstaan en het stimuleren van geintegreerde mensenrechten onderzoeksprojecten.

Projecten met zoekhit:
STAR II (1/06/2018 - 31/12/2020)
Een risico voor een recht? Verkenning van een nieuw begrip binnen het recht op bescherming van persoonsgegevens (1/01/2015 - 31/12/2018)

Publicaties met zoekhit:
Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection (2020)
The Proposed ePrivacy Regulation: The Commissions and the Parliaments Draft s at a Crossroads? (2020)
Handbook on Data Protection in Humanitarian Action - Second Edition (2020)
Data protection policies in EU justice and home affairs (2019)
Data Protection and the EPPO (2019)
Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles (2019)
Digital Security and Human Rights: A Plea for Counter-Infringement Measures (2019)
The new EU cybersecurity framework (2019)
Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective (2019)
Police, privacy and data protection from a comparative legal perspective (2018)
The right to data portability in the GDPR: Towards user-centric interoperability of digital services (2018)
Léternel retour de la propriété des données : de linsistance dun mot dordre (2018)
Data Protection Certification in the EU (2018)
Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach (2018)
Making the most of new laws: reconciling big data innovation and personal data protection within and beyond the GDPR (2018)
Data Protection and Privacy: The Internet of Bodies (2018)
The role of the data protection authorities in supervising police and criminal justice authorities processing personal data (2018)
The Right of Access Under the Police Directive: Small Steps Forward (2018)
Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research (2018)
The legal significance of individual choices about privacy and personal data protection (2017)
Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy (2017)
European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards Good Enough Judicial Oversight (2017)
Data Protection and Privacy: The Age of Intelligent Machines, (2017)
Mapping the legal and administrative frameworks of informational rights in Europe. A cross-European comparative analysis (2017)
A European perspective on data protection and the right of access (2017)

Fundamentele rechten centrum (FRC) - vervolg

Paul De Hert

Publicaties met zoekhit - vervolg:

The rich UK contribution to the field of EU data protection: Lets not go for “third country” status after Brexit (2017)
Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (2017)
Data Protection’s Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer (2017)
Genetic Classes and Genetic Categories: Protecting Genetic Groups through Data Protection Law (2017)
Exercising access rights in Belgium (2017)
Data Protection and Privacy: (In)visibilities and Infrastructures (2017)
Courts, Privacy and Data protection in Belgium: Fundamental rights that might as well be struck from the Constitution (2017)
The Unaccountable State of Surveillance. Exercising Access Rights in Europe (2017)
The new General Data Protection Regulation: Still a sound system for the protection of individuals? (2016)
Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research (2016)
The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR (2016)
Data protection authority perspectives on the impact of data protection reform on cooperation in the EU (2016)
Towards Harmonised Duties of Care and Diligence in Cybersecurity (2016)
Enforcing Privacy. Regulatory, Legal and Technological Approaches (2016)
The co-existence of administrative and criminal law approaches to data protection wrongs (2016)
Data Protection and Privacy. European Data Protection Reform (2016)
EU Criminal Law and Fundamental Rights (2016)
Visions of Technology (2016)
The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection (2016)
Data Protection on the Move (2016)
Introduction to Enforcing Privacy (2016)
Predictive Profiling and its Legal Limits: Effectiveness Gone Forever? (2016)
Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context (2016)
The New Police And Criminal Justice Data Protection Directive. A First Analysis (2016)
Dealing with overlapping jurisdictions and requests for mutual legal assistance, while respecting individual rights. What can data protection law learn from cooperation in criminal justice matters? (2015)
The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet (2015)
Assessing the European approach to privacy and data protection in smart grids. Lessons for emerging technologies (2015)
Google Spain: Addressing Critiques and Misunderstandings One Year Later (2015)
EU’s One-Stop-Shop Mechanism: Thinking Transnational (2015)
The proceduralisation of data protection remedies under EU data protection law: towards a more effective and data subject-oriented remedial system? (2015)
Preface to Reforming European Data Protection (2015)
Data protection: the EU institutions’ battle over data processing vs individual rights (2015)
Cooperation between the private sector and law enforcement agencies: an area in between legal regulations (2015)
The accountability culture in its european union dress. Sticks but no carrots to make the proposed data protection regulation work (2015)
The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns (2015)
Enforcing privacy: lessons from current implementations and perspectives for the future (2015)
Reforming European Data Protection (2015)
Introduction to Enforcing privacy (2015)
The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents? (2015)
Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer’s Duty to Regulate Profiling (2015)
Smart Technologies and the End(s) of Law (2015)

Gedistribueerde en Veilige Software (DistriNet)

Wouter Joosen

# objecten met zoekhit:	
Onderzoeksgroep	**0**
Projecten	**11**
Publicaties	**32**

Hoofddisciplines: Ingenieurswetenschappen
Disciplines: Distributed computing
Trefwoorden: software

Gedistribueerde en Veilige Software (DistriNet)

Projecten met zoekhit:
De volgende generatie software ondersteuning voor het anonimiseren van datasets (16/12/2020 - 16/12/2024)
Het in praktijk brengen van dataset anonimisatie (16/12/2020 - 16/12/2024)
Integriteitsborging voor meercomponentendiensten in 5G-netwerken (3/11/2020 - 3/11/2024)
Gecertificeerde semi-automatische modulaire formele programma verificatie (23/10/2020 - 20/05/2024)
Ontwerp, ontwikkeling en onderhoud van veilige ingebedde apparaten. (1/10/2020 - 30/09/2022)
Softwaregebaseerde nevenkanaal aanvallen en tegenmaatregelen (10/09/2020 - 10/09/2024)
Veiligheid en privacy in een Internet-of-Things omgeving (26/02/2020 - 26/02/2024)
Cybersecurity (1/09/2019 - 31/08/2029)
5e generatie beveiliging voor telecomdiensten (1/09/2019 - 31/08/2023)
Cyberbeveiligingsnetwerk van competentiecentra voor Europa (1/02/2019 - 1/07/2022)
Beveiliging en betrouwbaarheid voor opkomende IoT-netwerken (13/10/2016 - 10/02/2021)

Publicaties met zoekhit:
Mis-shapes, Mistakes, Misfits: An Analysis of Domain Classification Services (2020)
CRAM: Robust Medium Access Control for LPWAN using Cryptographic Frequency Hopping (2020)
DPMF: A Modeling Framework for Data Protection by Design (2020)
Operationalization of privacy and security requirements for eHealth IoT applications in the context of GDPR and CSL (2020)
Distributed Security Framework for Reliable Threat Intelligence Sharing (2020)
DNS Abuse and Active Authentication: Applications of Machine Learning in Cyber Security (2020)
The Bigger Picture: Approaches to Inter-Organizational Data Protection Impact Assessment (2020)
A Comparison of System Description Models for Data Protection by Design (2019)
Middleware for Data Management in Multi-Cloud (2019)
A data utility-driven benchmark for de-identification methods (2019)
DataBlinder: A distributed data protection middlewaresupporting search and computation on encrypted data (2019)
An Architectural View for Data Protection by Design (2019)

Gedistribueerde en Veilige Software (DistriNet) - vervolg

Wouter Joosen

Publicaties met zoekhit - vervolg:

slimIoT: Scalable lightweight attestation protocol for the Internet of Things (2018)
Parametricity Versus the Universal Type (2018)
Symbolic Execution of Security Protocol Implementations: Handling Cryptographic Primitives. (2018)
Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study (2018)
Towards a roadmap for privacy technologies and the general data protection regulation: A transatlantic initiative (2018)
The Relationship Between the Cost of Cybercrime and Web Security Posture: A Case Study on Belgian Companies (2017)
Telling your secrets without page faults: Stealthy page table-based attacks on enclaved execution (2017)
DLoc: Distributed Auditing for Data Location Compliance in Cloud (2017)
Towards an adaptive middleware for efficient multi-cloud data storage (2017)
Sancus 2.0: A low-cost security architecture for IoT devices (2017)
Key reinstallation attacks: Forcing nonce reuse in WPA2 (2017)
Security and privacy controls for streaming data in extended intelligent environments (2016)
Optimizing resource and data security in shared sensor networks (2016)
Ethical aspects in eHealth – design of a privacy-friendly system (2016)
Data protection compliance regulations and implications for smart factories of the future (2016)
PROTECTOR: Privacy-preserving information lookup in content-centric networks (2016)
uCentive: An efficient, anonymous and unlinkable incentives scheme (2015)
Formal Reasoning about Privacy and Trust in Loyalty Systems (2015)
Verifying protocol implementations by augmenting existing cryptographic libraries with specifications (2015)
Lightweight and flexible trust assessment modules for the Internet of Things (2015)

Meer informatie

info@fris.vlaanderen.be

Tel. 02/553 59 80

https://researchportal.be/nl/contact

FRIS-programma manager: Ils De Bal

Data-analyse: Pascale Dengis

Brochure:

https://www.ewi-vlaanderen.be/sites/default/files/bestanden/fris_het_vlaamse_onderzoeksportaal.pdf

Vlaanderen
is economie, wetenschap & innovatie