Vlaamse Regering

DE VLAAMSE MINISTER VAN ECONOMIE, INNOVATIE, WERK, SOCIALE ECONOMIE EN LANDBOUW

BISNOTA AAN DE VLAAMSE REGERING

Betreft: Vlaams Beleidsplan Cybersecurity 2024-2028

- **Onderzoeksprogramma Cybersecurity - Werkjaar 5 (2024)**
- **Flankerend beleid - Werkjaar 3 (2024)**

Samenvatting

Het Vlaamse Beleidsplan Cybersecurity, bestaande uit een onderzoeksprogramma, een implementatieluik en een flankerend beleid, werd opgestart in maart 2019.

In 2023 werd een eerste externe evaluatie afgerond die het beleidsplan doorlichtte. De evaluatie betrof in de eerste plaats het onderzoeksprogramma van het beleidsplan, maar onderzocht ook de interactie tussen het onderzoeksprogramma en de andere twee luiken. Op deze manier was het mogelijk om ook een algemene beoordeling van het volledige beleidsplan op te stellen.

De externe consultant die de evaluatie heeft uitgevoerd, concludeerde in zijn rapport dat het onderzoeksprogramma hoogwaardige resultaten heeft opgeleverd. Het panel van internationale experten dat in het kader van deze evaluatie werd ingezet, beoordeelde de resultaten als van 'uitstekende kwaliteit'. Ook oordeelde de externe consultant dat het beleidsplan goed is ingedeeld. De externe consultant gaf de aanbeveling om het Vlaamse Beleidsplan Cybersecurity voort te zetten. Finaal formuleerde hij enkele nuttige aanbevelingen die de impact en resultaten potentieel nog zouden kunnen vergroten. Met deze nota zet Vlaanderen het Vlaamse Beleidsplan Cybersecurity bijgestuurd verder en blijft een budgettaire inspanning leveren om een volgende cyclus van vijf jaar te ondersteunen.

Deze nota bouwt voort op de nota VR 2019 2203 DOC.0317/1 QUATER om de focuspunten en bijkomende accenten voor de tweede cyclus van het Vlaamse Beleidsplan Cybersecurity weer te geven. De essentie van de eerste cyclus wordt, gezien de positieve evaluatie en de sterke resultaten, grotendeels behouden.

Met deze nota zetten we de lijnen uit voor de volgende vijf jaar, mede gebaseerd op de resultaten van de externe evaluatie. We voorzien met deze nota ook in de financiering van werkjaar 5 van het onderzoeksprogramma cybersecurity en werkjaar 3 van het flankerend beleid.

1. SITUERING

A. BELEIDSVELD/BELEIDSDOELSTELLING

Het Vlaamse Beleidsplan Cybersecurity, het onderzoeksprogramma, het implementatieluik en het flankerende beleid passen in het beleidsdomein Werk, Economie, Wetenschap, Innovatie, Landbouw en Sociale economie:

- Beleidsveld wetenschappelijk onderzoek;
- Beleidsveld innovatie.

De subsidiëring draagt bij tot de algemene uitvoering en doelstellingen van het Vlaamse Beleidsplan Cybersecurity.

B. VORIGE BESLISSINGEN EN ADVIEZEN

Vlaams Beleidsplan Cybersecurity

Op 22 maart 2019 keurde de Vlaamse Regering het Vlaamse Beleidsplan Cybersecurity goed (VR 2019 2203 DOC.0317/1QUATER). Dit beleidsplan bestaat uit drie complementaire pijlers.

Luik 1: **onderzoeksprogramma**
Het doel van het onderzoeksluik is om top strategisch basisonderzoek uit te voeren om nieuwe kennis, wetenschappelijke doorbraken en talent op wereldniveau te ontwikkelen op domeinen waar Vlaanderen reeds excellent presteert én waar synergie kan bekomen worden met de vraaggedreven implementatie-agenda van het Vlaamse bedrijfsleven.

Luik 2: **implementatieluik**
De centrale focus van het tweede luik is de implementatie van cybersecurity-toepassingen in het bedrijfsleven. Een vraaggedreven agenda vanuit het bedrijfsleven moet via open, goed georganiseerde kanalen en netwerken gebracht worden tot bestaande overheidsinstrumenten van VLAIO (Vlaams Agentschap Innoveren en Ondernemen) en relevante instellingen.

Luik 3: **flankerend beleid**
Het flankerende beleid voorziet dat er wordt gewerkt aan de significante opleidingsnoden gericht op de arbeidsmarkt. Verder ligt er een focus op een correcte doch ambitieuze “outreach” zodat vernieuwende cybersecurity-kennis, inzichten en technologieën worden gedeeld, waardoor zo veel mogelijk Vlaamse actoren actief kunnen participeren.

In uitvoering van dit beleidsplan duidde de Vlaamse Regering op 7 juni 2019 de leden van de stuurgroep van het beleidsplan aan (VR 2019 0706 DOC.0866/1BIS).

Onderzoeksprogramma Cybersecurity

Op 4 en 5 juli 2019 heeft de Internationale Wetenschappelijke Adviesraad (ISAB - International Scientific Advisory Board) het voorgestelde onderzoeksprogramma positief beoordeeld. Daarnaast heeft de ISAB ook de uitvoering en de wetenschappelijke relevantie van het vierde werkjaar (01/01/2023 – 31/12/2023) positief beoordeeld. Zij velden dit oordeel tijdens de jaarlijks georganiseerde bijeenkomst die op 11 en 12 december 2023 plaatsvond (zie bijlage 4).

Voor de uitvoering van het onderzoeksluik voorzag het Vlaamse Beleidsplan Cybersecurity een recurrent budget van 8 miljoen euro op jaarbasis. Het onderzoeksprogramma cybersecurity werd reeds viermaal goedgekeurd door de Vlaamse Regering:

- Beslissing van de Vlaamse Regering voor het eerste werkjaar van het Onderzoeksprogramma Cybersecurity Vlaanderen (VR 2019 1312 DOC.1235/1-10);
- Beslissing van de Vlaamse Regering voor het tweede werkjaar van het Onderzoeksprogramma Cybersecurity Vlaanderen (VR 2020 1812 DOC.1469/1-8);
- Beslissing van de Vlaamse Regering voor het derde werkjaar van het Onderzoeksprogramma Cybersecurity Vlaanderen (VR 2021 1712 DOC.1482/1-8);
- Beslissing van de Vlaamse Regering voor het vierde werkjaar van het Onderzoeksprogramma Cybersecurity Vlaanderen (VR 2023 2403 DOC.0285/1-7).

Het onderzoeksprogramma is opgebouwd rond vier onderzoekslijnen:

- *Research Track 1: Application and Software Security;*
- *Research Track 2: Strategic Security Services;*
- *Research Track 3: System and Infrastructure Security;*
- *Research Track 4: Technology Building Blocks: Secure Hardware, Cryptography and Secure Implementations.*

Flankerend beleid

Voor het onderdeel 'flankerend beleid' in beheer van het Departement EWI werden twee subprogramma's ontwikkeld, namelijk het opleidingsprogramma en het outreach- en communicatieprogramma. Vanaf werkjaar 2 werden deze samengebald voor efficiëntiewinsten. De eerdere goedkeuringen rond het flankerend beleid zijn de volgende:

- Beslissing van de Vlaamse Regering voor het Vlaams Cybersecurity Opleidingsprogramma werkjaar 1 (VR 2020 2711 DOC.1304/1-8);
- Beslissing van de Vlaamse Regering voor het Vlaams Outreach en Communicatieprogramma Cybersecurity werkjaar 1 (VR 2020 2711 DOC.1303/1-6);
- Beslissing van de Vlaamse Regering voor het Flankerend beleid werkjaar 2 (VR 2022 1011 DOC.1216/1-6).

2. INHOUD

A. VLAAMS BELEIDSPAN CYBERSECURITY

Externe evaluatie

In 2023 werd het Vlaamse Beleidsplan Cybersecurity over de periode 2019–2023 geëvalueerd, met een focus op het onderzoeksprogramma. Het doel van de evaluatie was om terug te kijken naar de werking, activiteiten en effecten van het beleidsplan (ex post), maar ook om te kijken naar de toekomstige trends en behoeften voor het toekomstige cybersecuritybeleid (ex ante). Tijdens de evaluatie was er ook aandacht voor het implementatieluik en het flankerende beleid, alsook voor de interactie tussen de drie luiken.

De evaluatie werd gecoördineerd door de evaluatiecel van het Departement Economie, Wetenschap en Innovatie. Voor de eigenlijke uitvoering ervan werd via een aanbestedingsprocedure een externe consultant aangesteld. In de evaluatie werd ook een panel van internationale experten betrokken. De evaluatie is te vinden in bijlage 5.

Op basis van de evaluatie door Technopolis en het internationale expertenpanel wordt het beleidsplan bijgestuurd, zoals verder in deze nota wordt toegelicht. Tot slot volgt een voorstel voor de invulling van werkjaar 5 (2024) van het onderzoeksprogramma cybersecurity en voor werkjaar 3 (2024) van het flankerende beleid.

Het onderzoeksprogramma cybersecurity gaf de afgelopen jaren een financiële impuls aan top strategisch basisonderzoek in cybersecurity in Vlaanderen, waarbij er dankzij het beleidsplan een stabiel langetermijnperspectief geboden wordt aan de consortiumpartners. Volgens de externe

consultant leverde het onderzoeksprogramma 'hoogwaardige resultaten' op. Het onafhankelijke internationale panel van experten dat het opzet en de resultaten van het onderzoeksprogramma heeft onderzocht, beoordeelde de resultaten als 'van uitstekende kwaliteit'.

De opzet en inrichting van het implementatieluik (aansluiting bij het bestaande VLAIO-instrumentarium) en van het flankerende beleid (dat voor het beleidsplan is opgezet) heeft zoals beoogd plaatsgevonden en is gegroeid tijdens de looptijd van het programma. Er wordt vastgesteld dat er een impliciete spreidstand is tussen de doelstellingen van het implementatieluik. Enerzijds is het de bedoeling om 'koplopers' binnen het Vlaamse bedrijfsleven te bereiken en resultaten van excellent onderzoek verder te valoriseren. Idealiter is er daarvoor een doorstroom van resultaten vanuit het onderzoeksprogramma naar het implementatieluik, met name in enkele projecten waaraan consortiumpartners en bedrijven gezamenlijk deelnemen. We stellen vast dat er meer moet worden ondernomen om via het implementatieluik de impact van het onderzoeksprogramma te verhogen en valorisatie te verbeteren. Anderzijds is er ook een grote behoefte aan een toenemende cybersecuritymaturiteit in het brede bedrijfsleven, bij kmo's en innovatievolgers. Daarvoor moet bekeken worden of de bredere insteek van digitalisering effectiever is dan een nauwere insteek die zich enkel beperkt tot cybersecurity.

Volgens de analyse van de externe consultant levert het beleidsplan een positieve bijdrage aan het Vlaamse wetenschaps- en innovatiesysteem. Het beleidsplan heeft het cybersecurity-onderzoek in Vlaanderen bestendigd. De economische en maatschappelijke impact is positief, maar nog bescheiden, voornamelijk ten gevolge van externe factoren zoals schaarste omtrent cybersecurity-experts en een beperkte interesse en investeringsbereidheid in cybersecurity onder bedrijven. Deze factoren spelen niet enkel in Vlaanderen, maar internationaal in het cybersecurityveld.

Op basis van deze globale beschouwing en de teweeggebrachte resultaten van het beleidsplan adviseert de externe consultant om het beleidsplan verder te zetten. Daardoor worden de stabiele langetermijnobjectieven verzekerd, net zoals de daarbij horende financiering.

Over het beleidsplan als geheel en de indeling ervan in drie luiken is de externe consultant positief: deze indeling dekt de breedte van thematiek af en past bij de sterktes van de verschillende betrokken spelers. Het beleidsplan zou volgens de evaluatie efficiënt zijn ingericht.

De externe consultant geeft ook enkele aandachtspunten en mogelijk optimalisaties mee. Hij beveelt aan om te werken aan een sterkere interactie tussen de drie luiken: *"Het Vlaamse Beleidsplan Cybersecurity vormt een logisch kader, maar de activiteiten in elk van de luiken staan te los van elkaar om goed op elkaar aan te sluiten."*

Volgens het rapport van de externe consultant kunnen de impact en resultaten van het onderzoeksprogramma verhoogd en de valorisatie verbeterd worden. Ook het inzichtelijk maken van de resultaten en impact is een aanbeveling die gemaakt wordt door de externe consultant en door het internationale expertenpanel.

Structurele aanpassingen

De verschillende betrokkenen bij het beleidsplan zijn de voorbije maanden aan de slag gegaan om de suggesties en aandachtspunten die geformuleerd werden in het rapport van de externe consultant en van het internationale expertenpanel, beleidsmatig te vertalen. Deze 'vertaling' wordt toegelicht in de volgende secties en toegepast op het onderzoeksprogramma cybersecurity, werkjaar 5 (01/01/2024 – 31/12/2024), en op het flankerende beleid, werkjaar 3 (01/01/2024 – 31/12/2024). Om het overzicht te bewaren worden enkele ingrijpende structurele veranderingen in het beleidsplan en de programma's hier kort samengevat. In de volgende secties worden deze diepgaander toegelicht.

Het beleidsplan wordt in grote lijnen voortgezet zoals gedefinieerd tijdens de eerste cyclus In 2019 werd voor het beleidsplan CS een bedrag van 20 miljoen euro voorzien [VR 2019 2203

DOC.0317/1QUATER]. Hiervan ging 8 miljoen euro naar het onderzoeksluik bij het departement EWI, 9 miljoen euro naar het implementatieluik bij VLAIO, en 3 miljoen euro naar het flankerende beleid (1,5 miljoen naar respectievelijk EWI en VLAIO). De middelen voor het flankerende beleid kunnen efficiënter benut worden: de middelen voor open oproepen (521.000 euro) en niet- of onderbenutte middelen (449.200) worden verschoven richting het onderzoeksprogramma. Hiervoor wordt 75.000 euro herverdeeld vanuit het flankerende beleid bij VLAIO richting het departement EWI (zie bijlage 1). Deze laatste herverdeling dient bij Begrotingsaanpassing te gebeuren, zodat de middelen tijdelijk intern binnen EWI herschikt worden. Het budget voor CS-onderzoek komt zo op 8,97 miljoen euro, dat voor het flankerende beleid bij EWI op 604.800 euro.

Daarnaast wordt ingezet op onderstaande punten.

- Er wordt ingezet op een sterkere interactie tussen de drie luiken.
    - Het resterende flankerende beleid bij EWI wordt ingekanteld in het onderzoeksprogramma.
    - Het implementatieluik wordt bijgestuurd: er worden geoormerkte middelen voorzien voor het onderzoeksconsortium in functie van de doorstroom van onderzoeksresultaten naar de Vlaamse bedrijven (via het reguliere VLAIO-instrumentarium).
- In het onderzoeksluik wordt ingezet op:
    - meer valorisatiepotentieel, o.a. door het aanwerven van een halftijdse valorisatiemanager;
    - communiceren over impact onderzoeksresultaten, o.m. via nieuwsbrieven en persberichten ;
    - het verder versterken van het onderzoeksconsortium door het aanwerven van een bijkomende consortiumpartner
- Op vlak van implementatie wordt het verhogen van de cybersecuritymaturiteit bij een grote groep van Vlaamse ondernemingen (kmo's en innovatievolgers) de focus van een afzonderlijk actieplan ter bevordering van de digitale transformatie, met inbegrip van AI en CS.
- Er gebeuren ook enkele bestuurlijke en organisatorische aanpassingen.

Jaarlijks worden er in lijn met de strategische doelstellingen, noden en kansen specifieke accenten gelegd.

Luik 1: het versterken van top strategisch basisonderzoek in Vlaanderen

Consortiumuitbreiding

Een deel van het budget van het flankerende beleid wordt overgeheveld naar het onderzoeksprogramma. zoals later wordt toegelicht). Zoals later wordt toegelicht, genereerde het open oproepenmechanisme niet de gewenste engagementen. Deze middelen kunnen efficiënter en effectiever benut worden. Ze worden beschikbaar gesteld om het consortium uit te breiden met een onderzoeksgroep en zo verder te werken aan de bestendiging van het onderzoeksprogramma.

Vanaf 2024 wordt het onderzoeksprogramma uitgebreid met een team onder leiding van prof. An Braeken (VUB). De kandidatuur van prof. An Braeken werd eind 2022, samen met die van andere kandidaat-consortiumpartners, door de ISAB geëvalueerd. Haar kandidatuur kwam als beste uit de bus. Haar wetenschappelijke output is de laatste jaren sterk gegroeid; haar onderzoeksprofiel is complementair met dat van het huidige consortium en vormt een logische verbreding en verdieping binnen de onderzoekslijnen van het onderzoeksprogramma. Daarnaast is haar onderzoek gericht op samenwerking met industriële partners en valorisatie, wat een focuspunt vorm in de tweede cyclus.

Valorisatie

Een belangrijk aandachtspunt dat werd geformuleerd in het rapport van de externe consultant, betrof valorisatie. Ook het internationale expertenpanel gaf aan dat de impact van de resultaten van het onderzoeksprogramma het zeker waard was om extra belicht en gecommuniceerd te worden.
Dit punt wordt ter harte genomen en er wordt op verschillende manieren aan gewerkt. Daarom wordt valorisatie een belangrijk element dat verder versterkt wordt. Er zal gefocust worden op twee werkvelden.

(1) De benutting van de geoormerkte middelen die in het implementatieluik worden voorzien voor het onderzoeksconsortium wordt versterkt ingezet op de genese, definitie en indiening van projecten die bijdragen aan de doorstroom van de resultaten (toolboxes, usecases, …) uit het onderzoeksprogramma naar de Vlaamse ondernemingen (zie onder). De nadruk ligt op COOCK-, ICON- en TETRA-projecten.

(2) Bijkomend wordt er ingezet op valorisatietrajecten waar ondernemerschap (start-ups, spin-offs) centraal staan. Dit wordt verderop toegelicht.

Ter versterking van het valorisatiepotentieel worden maar liefst 5 verschillende maatregelen getroffen.

- Ten eerste wordt er nauw samengewerkt met de TTO-actoren van de verschillende onderzoekspartners (zoals bv. de IOF-mandaathouders).
- Ten tweede wordt er een halftijdse valorisatiemanager aangeworven. Hij/zij zal de volgende drie maatregelen mee overzien, uitvoeren en coördineren.
- Ten derde worden een aantal onderzoeksresultaten sneller geanalyseerd in termen van marktpotentieel en mogelijkheden tot een versneld valorisatietraject. Bovendien worden onderzoekers met interesse voor valorisatieprojecten gestimuleerd om valorisatietrajecten te starten. Dit gegeven wordt opgezet aan de hand van een programma dat (1) ervaringen deelt (succes en mislukking), dat (2) proactief prospecteert en sterke tussenresultaten toetst aan de mogelijkheden en opportuniteiten in de cybersecurity-markt, en dat (3) potentiële initiatiefnemers met elkaar in contact brengt en verder connecteert met het ecosysteem in Vlaanderen en daarbuiten.

  Deze drie elementen komen binnen het onderzoeksprogramma periodiek aan bod aan de hand van workshops en informatiesessies. Het aansporen en uitnodigen tot deze initiatieven moet leiden tot extra mobilisatie bij alle deelnemers aan het onderzoeksprogramma.
- Ten vierde worden een aantal assets (sterke prototypes met een hoog TRL-level) expliciet onderwerp van een marktanalyse die leidt tot het ontwerp van een businesscase. Ook hier spelen de extra middelen die worden vrijgemaakt voor valorisatie een rol als katalysator, uiteraard aangevuld met de domeinexpertise van de cybersecurity-specialisten van de prototypes in kwestie. Dit leidt potentieel tot een aantal exploratieprojecten.
- Tot slot wordt de expertise van het onderzoeksconsortium proactief aangeboden en aangewend om onder meer in functie van de in het implementatieluik voorziene geoormerkte middelen de valorisatie in het Vlaamse ecosysteem op het vlak van cybersecurity te ondersteunen en meer specifiek in functie van de doorstroom van onderzoeksresultaten naar de Vlaamse ondernemingen.

Communicatie- en disseminatie-initiatieven

Zoals de externe consultant aangaf, kan de impact van de onderzoeksresultaten verhoogd worden. Deze impact is een logisch gevolg van twee factoren: enerzijds communicatie en disseminatie van de onderzoeksresultaten, en anderzijds de valorisatie ervan. Hieronder wordt dieper ingegaan op de communicatie-aspecten.

Verschillende stappen worden ondernomen om het communicatiepotentieel van het onderzoeksprogramma te versterken. Zo zal het aangestelde communicatiebureau in de loop van 2024 de nodige communicatiemiddelen aanleveren om op een coherente, efficiënte en effectieve manier te communiceren. Zo wordt er een statische website opgeleverd in het Nederlands en in het Engels waar steeds naar teruggegrepen kan worden om de doelen van het beleidsplan en de programma's overzichtelijk en helder te communiceren. Deze wordt zo opgesteld dat elke doelgroep van het beleidsplan op de site zijn vragen beantwoord ziet of in contact kan treden met zij die een antwoord kunnen bieden. Daarbij denken we uiteraard aan (internationale) onderzoekers, bedrijven, waaronder kmo's, en beleidsmakers. Een van de hoofddoelen is dat er linken kunnen worden gelegd met de doelgroepen en dat relevant samenwerkingsopportuniteiten gevonden kunnen worden.

Uiteraard wordt er ook verder gewerkt met de website 'https://cybersecurity-bites.be/', die dynamisch van aard is en tracht om actuele informatie en kennis uit het onderzoeksprogramma te delen met de industrie en andere geïnteresseerden. In de toelichting betreffende flankerende beleid, werkjaar 3, verder in deze nota, wordt dieper ingegaan op de doelstellingen van de site in 2024. Het zwaartepunt van de communicatie gericht op de Vlaamse ondernemingen blijft liggen bij de website www.vlaio.be/cybersecurity, die door VLAIO werd opgezet met als doel de Vlaamse ondernemingen te informeren en te activeren rond het thema cyberveiligheid. Op de VLAIO-webpagina wordt ook actief doorverwezen naar andere webpagina's waar ondernemingen relevante informatie kunnen vinden met betrekking tot cyberveiligheid.

Bijkomend zal er door de programmamanager en -directie voor gezorgd worden dat de relevante en betrokken partijen geïnformeerd worden over de onderzoeksresultaten. Drie keer per jaar worden nieuwsbrieven verspreid via sociale media en via mail (op basis van een mailinglijst) met een update over de vooruitgang van het Vlaamse Beleidsplan Cybersecurity. Daarnaast zullen er ook persberichten geschreven worden om spraakmakende resultaten in de kijker te zetten. Dit laat toe om de kwaliteit die behaald wordt met het onderzoeksprogramma te belichten. Tevens zullen in de jaarlijkse rapporten op begrijpelijke manier de resultaten inzichtelijk gemaakt worden zodat deze vertaald kunnen worden naar bijkomende communicatie-opportuniteiten. Het beter inzichtelijk maken van de impact van het onderzoeksprogramma is een aanbeveling van het internationaal expertenpanel.

Tot slot zal er op kwartaalbasis ook overlegd worden met betrokken actoren zoals relevante sectororganisaties om prioriteiten te noteren rond (content)noden die de cybersecuritymaturiteit bij stakeholders te vergroten.

Samenwerking

Nu de sterke basis is uitgebouwd, wordt er verder ingezet op samenwerkingen. Er zal verder verkend worden welke samenwerkingen mogelijk zijn op Vlaams niveau (zoals met Digitaal Vlaanderen voor o.a. datasets), met de federale overheid (zoals het Cybersecurity Centre Belgium – CCB) en met Europese initiatieven. Zo wordt een blijvende aansluiting bij Europese en nationale beleidsontwikkelingen verzekerd. Het laat ook toe bedrijven bijkomend voor te bereiden of te informeren over nieuwe EU-regelgeving, via de instrumenten van het flankerend beleid.

Begrotingsaanpassingen

Tijdens de eerste cyclus werd een jaarlijks recurrent bedrag van 8 miljoen euro voorzien voor het onderzoeksprogramma Cybersecurity.

De externe consultant geeft aan dat de onderzoeksbudgetten geschikt zijn voor de geformuleerde doelstellingen van het onderzoeksprogramma, maar maakt de kanttekening dat er rekening gehouden moet worden met indexatie en gestegen personeelskosten. Het internationale expertenpanel geeft ook aan dat een deel van hun aanbevelingen niet doorgevoerd kunnen worden zonder extra financiële middelen.

Daartoe wordt er bijkomend voor gekozen om de eenmalige indexatie die in 2022 werd gegeven voor jaar 2022 en jaar 2023 op een structurele manier te verankeren. Daartoe worden niet bestede middelen en het budget van de open oproepen verschoven naar het onderzoeksprogramma om tegemoet te komen aan de indexering en het consortium te kunnen uitbreiden. Ook het aanstellen van een halftijdse valorisatiemanager vereist middelen. De jaarlijks recurrente subsidie zal daarom worden opgetrokken tot bijna 9 miljoen euro (later meer informatie).

Voor de tweede cyclus bedraagt de jaarlijks recurrente subsidie 9 miljoen euro. In deze nieuwe cyclus wordt dit bedrag o.a. voorzien voor de indexatie, de uitbreiding van het consortium en voor de valorisatiemanager.

Luik 2: implementatie in het Vlaamse bedrijfsleven

A) Valorisatieprojecten: doorstroom van resultaten uit het onderzoeksprogramma richting de Vlaamse ondernemingen

Voor de consortiumpartners van het Vlaamse onderzoeksprogramma CS wordt jaarlijks bij VLAIO een geoormerkt bedrag voorzien op begrotingsartikel ECH-1EFG5NA-WT (basisallocatie ECH 1EF3BV) t.b.v. 4 miljoen euro. Zij kunnen deze middelen aanwenden voor projecten die aantoonbaar bijdragen aan de doorstroming naar en valorisatie door het bedrijfsleven van resultaten uit het onderzoeksprogramma. Er zijn drie voorwaarden om deze middelen te benutten.

1. Het project heeft een duidelijk aantoonbare link met resultaten uit het onderzoeksprogramma;
2. Het project bevat een significant luik kennisopbouw bij ondernemingen of collectieve kennisverspreiding naar ondernemingen.
3. Minstens één consortiumpartner is betrokken als projectpartner bij het project. Samenwerking met onderzoeksorganisaties die geen consortiumpartner van het onderzoeksprogramma zijn, is mogelijk.

In navolging van de aanbevelingen uit de evaluatie, zal VLAIO via het implementatieluik een extra stimulans geven aan de doorstroom van de resultaten (toolboxes, usecases…) uit het onderzoeksprogramma naar de Vlaamse ondernemingen via het VLAIO-instrumentarium. De focus ligt hierbij in het bijzonder op de innovatieleiders onder de technologiegebruikers en technologie-aanbieders. Om dit te realiseren worden voor het onderzoeksconsortium geoormerkte middelen voorzien bij VLAIO, waarop het consortium via reguliere VLAIO-instrumenten beroep kan doen voor specifieke projecten die aantoonbaar bijdragen aan deze doelstelling.

De hiervoor inzetbare VLAIO-instrumenten zijn ICON, COOCK, en TETRA. Losstaande SBO-projecten komen niet in aanmerking aangezien deze niet voldoen aan de voorwaarde inzake kennisopbouw bij ondernemingen of collectieve kennisverspreiding. Waar relevant en op voorwaarde dat er een sterkte betrokkenheid is van Vlaamse bedrijven kan het Beslissingscomité bij het Fonds voor Innoveren en Ondernemen (FIO) ook andere projecttypes of projecten die voldoen aan bovenstaande voorwaarden in aanmerking nemen.

Het is de verantwoordelijkheid van de programmamanager om, samen met het onderzoeksconsortium, rond de projectgeneratie of -funnel, en dus de benutting van deze middelen, de nodige ondersteuning te voorzien (zie hoger *“valorisatietoeleiding”),* met het oog op de projectindiening die verloopt in onderling overleg met VLAIO. De governance en werkwijze daarvoor worden ter validatie voorgelegd aan de CS-stuurgroep. Het FIO-beslissingscomité staat in voor de finale evaluatie van de projectvoorstellen.

Het benutten van deze middelen zal vanaf werkjaar 6 (=2025) als prestatie-indicator voor het onderzoeksprogramma gelden (de concrete invulling ervan wordt aan de CS-stuurgroep overgelaten

(zie verder). Onbenutte middelen en eventuele saldi van het begrotingsartikel ECH-1EFG5NA-WT (basisallocatie ECH 1EF3BV) kunnen steeds door VLAIO aangewend worden voor relevante CS- en/of digitaliseringsprojecten ten behoeve van Vlaamse ondernemingen. Op basis van de rapportage over de jaarlijkse benutting van voorziene middelen kan door VLAIO aan het FIO-beslissingscomité jaarlijks een advies voorgelegd worden om voor het volgende werkjaar de opgelegde voorwaarden of projecttypes bij te sturen en/of het voorziene budget te wijzigen.

Uiteraard blijft het zowel voor onderzoeksorganisaties binnen en buiten het onderzoeksconsortium, als voor andere intermediaire actoren, mogelijk om aanvullend verder gebruik te maken van de reguliere VLAIO-kanalen om bijkomende projecten te initiëren in functie van een brede AI-adoptie en/of verspreiding van onderzoeksresultaten. Ook zal VLAIO via de reguliere O&O-bedrijfssteun CS-projecten van individuele bedrijven of samenwerkingsverbanden van bedrijven die voldoen aan de door VLAIO gestelde voorwaarden blijven ondersteunen. Het bevorderen van het ondernemerschap en van start-ups en scale-ups die "CS-oplossingen" aanbieden zal hierbij ook de nodige aandacht blijven krijgen. Verder zal VLAIO via de reguliere bedrijfssteun afdwingen dat ondernemingen die digitale producten, diensten of processen ontwikkelen al vroeg in het ontwikkelproces aspecten van cyberveiligheid meenemen.

B) Programma ter bevordering van de digitale informatie bij Vlaamse ondernemingen

Succesvolle digitale transformatie en de adoptie van nieuwe digitale technologieën (inclusief cyberveiligheid) is enkel mogelijk als een onderneming voldoet aan de juiste randvoorwaarden of fundamenten. Ondernemingen dienen hierbij te beschikken over een digitale strategie en een geschikte aanpak rond data. Ook moet er een voldoende niveau van digitale basiscompetenties bereikt zijn alvorens zinvol over specifieke toepassing van andere digitale technologieën zoals AI kan gepraat worden. Bovendien dient het gebruik van (nieuwe) digitale technologieën ook op een cyberveilige, duurzame en inclusieve manier te gebeuren. Vandaag ontbreekt het in nog veel Vlaamse ondernemingen aan deze fundamenten om die volgende stap richting digitale transformatie te zetten. Het werken aan de digitale maturiteit van ondernemingen vereist dan ook een aanpak die losstaat van het laten doorstromen van de resultaten van het onderzoeksprogramma richting de ondernemingen.

Aanvullend op het implementatieluik van de AI-beleidsagenda en de CS-beleidsagenda zal VLAIO een nieuw, afzonderlijk actieplan opzetten ter bevordering van de digitale transformatie bij Vlaamse ondernemingen, met een focus op kmo's en innovatievolgers. Het doel van dit nieuwe plan is om meer Vlaamse ondernemingen te laten groeien inzake digitale maturiteit zodat ook zij toekomstbestendig zijn in een sterk gedigitaliseerde economie en maatschappij. Deze ambitie is in lijn met de doelstellingen van het European Digital Decade en de Vlaamse digitale strategie die in ontwikkeling is onder coördinatie van Digitaal Vlaanderen.

De doelgroep van het programma ter bevordering van de digitale transformatie bij Vlaamse ondernemingen zijn de kmo's, innovatievolgers en/of ondernemingen die nog belangrijke stappen moeten maken in digitale maturiteit en veelal nog aan de start van de digitale transformatie staan.

Voor de uitrol van dit programma worden geen extra middelen gevraagd. In eerste fase zal VLAIO het programma financieren op bestaande eigen middelen door het heroriënteren of reserveren van aan VLAIO toegewezen middelen uit de implementatieluiken en flankerend beleid van de beleidsplannen AI en CS en van de transitieoproepen rond industrie 4.0. Specifiek vanuit het beleidsplan CS reserveren we 5,825 miljoen euro (jaarlijks), met name:

- Onder de strategische doelstelling 'ondernemerschap': 1,425 miljoen euro (jaarlijks) via de lijn 'initiatieven ter bevordering van ondernemerschap' (ECH 1EC361) en de lijn 'AI/CS' (1EC3AU);

- Onder de strategische doelstelling ‘ Innovatie’ 4,4 miljoen euro van de basisallocatie ‘beleidsagenda AI’ (ECH 1EF3BU) die op dit ogenblik al aangewend wordt voor o.a. de cybersecurity-verbetertrajecten.

Verder kunnen ook middelen uit reguliere VLAIO-programma’s en/of meer generieke VLAIO-acties (Blikopener, TETRA, COOCK, ondernemerschapsbevordering…) aangewend worden voor het realiseren van de doelstellingen van het programma ter bevordering van de digitale transformatie bij Vlaamse ondernemingen. Waar relevant staat VLAIO ook open voor samenwerking over de beleidsdomeinen heen.

De gedetailleerde uitwerking van het programma met duidelijke doestellingen en aanpak wordt op een later tijdstip onder de vorm van een conceptnota aan de Vlaamse Regering voorgelegd.

Luik 3: flankerend beleid

Inkanteling in het onderzoeksprogramma

In het rapport van de externe consultant werd aangegeven dat de opzet van de drie luiken goed bevonden wordt, maar dat er door een versterkte interactie betere resultaten en valorisatie gerealiseerd kunnen worden. Op basis daarvan zal de geest van het beleidsplan, en dus ook het flankerend beleid, in grote mate behouden blijven. Om de interactie echter te versterken, zal het flankerend beleid vanaf nu in de praktijk beschouwd worden als een vijfde horizontale track in het onderzoeksprogramma. Deze beweging brengt tal van voordelen met zich mee, zoals een beter en meer gericht opleidings- en communicatie-aanbod, maar ook operationele efficiëntie. Het is efficiënter om de werking van het flankerend beleid te organiseren in harmonie met het onderzoeksprogramma. Behalve een harmonieuzere aanpak heeft deze aanpassing voornamelijk een positieve administratieve impact.

Stopzetting open oproepen

Binnen het flankerend begeleide, dat bestaat uit een opleidingsprogramma en een communicatieprogramma, werden elk jaar enkele ‘open oproepen’ georganiseerd. Vlaamse kennisinstellingen buiten het onderzoeksconsortium konden projectvoorstellen indienen die door een beoordelingscommissie werden beoordeeld. Het ging daarbij vooral om artikels die bedrijven trachten te sensibiliseren over actuele cybergevaren of tips gaven om de cybermaturiteit en -security te verhogen. Via de opleidingsmodule werd getracht om meer geavanceerde gebruikers, zoals ICT-verantwoordelijken, bij te scholen over nieuwe cyberrisico’s en hoe deze te vermijden. We stellen echter vast dat de open oproepen geen groot succes en de voorstellen van de kennisinstellingen buiten het consortium zeer gering zijn in aantal. Het blijkt moeilijk om occasionele participanten, bijvoorbeeld hogescholen, te laten deelnemen aan deze open werkwijze, wellicht omwille van beperkt beschikbare tijd of omwille van een beperkte capaciteit op het thema cybersecurity.

Daarom worden de open oproepen vanaf 2024 stopgezet. De deelname van kennisinstellingen buiten het onderzoeksconsortium wordt mogelijk via de geoormerkte middelen in het implementatieluik en of de reguliere oproepen voor COOCK en TETRA bij VLAIO.

De middelen voor de open oproepen worden geheroriënteerd (521.000 euro) naar het onderzoeksprogramma, zoals eerder toegelicht.

Verschuiving richting Programma Digitale Transformatie

Binnen het flankerende beleid CS bij VLAIO werd 0,6 mio. EUR voorzien voor projecten i.s.m. het beleidsdomein Onderwijs. Deze middelen werden samengevoegd met 1 mio. EUR binnen het flankerende beleid van het beleidsplan AI voor enerzijds samenwerkingen met de structurele partners Vlajo en Unizo en anderzijds oproepen die ad hoc werden uitgewerkt. Deze middelen blijven

behouden. Met deze enveloppe voorzien we, naast een voortzetting van de samenwerking met de structurele partners (zo'n 280.000 tot max. 300.000 EUR), ook:

- een trekkingsrecht met voorbehouden middelen voor het beleidsdomein Onderwijs binnen PIO (Project Innovatieve Overheidsopdrachten) waarop rechtstreeks beroep gedaan kan worden voor AI- en CS-projecten;
- ondersteuning van initiatieven en begeleiding van onderwijsspelers en bedrijven om EdTech-oplossingen in de klas te krijgen en drempels weg te werken;
- oproepen of initiatieven die inzetten op het aanpakken van een maatschappelijke uitdaging op een digitale en/of slimme ('smart') manier (met aandacht voor cybersecurity) door een consortium van minimaal enkele scholen en maximaal een quadruple-helixsamenwerking. De geselecteerde aanpak zet daarbij expliciet in op het gebruiken en versterken van de computationele vaardigheden van de leerlingen.

De middelen uit deze enveloppe worden ingezet in overleg met de minister bevoegd voor Onderwijs.

De overige aan VLAIO toegekend middelen in het kader van het flankerend beleid zullen verschoven worden richting het programma Digitale Transformatie waar ook expliciet aandacht zal geschonken worden aan de digitale basiscompetenties (incl. rond cyberveiligheid) die nodig zijn voor (toekomstige) werknemers). Goed opgeleide werknemers zijn immers een belangrijke randvoorwaarde voor een succesvolle digitale transformatie. Bovendien wordt 75.000 euro van het flankerend beleid bij VLAIO verschoven richting de onderzoeksprogramma's van het AI- en het CS-beleidsplan.

Organisatie en governance

Op basis van de evaluatieresultaten en -aanbevelingen de nodige voorstellen en aanpassingen gedaan aan de organisatie van het Vlaamse Beleidsplan Cybersecurity. Er wordt toegelicht welke constellaties verder worden gezet en welke optimalisaties en aanpassingen worden doorgevoerd.

Operationeel management

In de nota aan de Vlaamse Regering van 22 maart 2019 (VR 2019 2203 DOC.0317/1QUATER) werd de coördinatie van het onderzoeksprogramma cybersecurity bij de KU Leuven gelegd. Deze coördinatie wordt gerealiseerd onder leiding van prof. Bart Preneel en prof. Wouter Joosen. Deze verantwoordelijkheid houdt het organiseren en opleveren van de rapportering van het programma in, het opzetten van de programmareviews, het organiseren van alle programma-activiteiten (actualiseren van de *roadmap* en de vernieuwing van programma-activiteiten door een oproep voor nieuwe ideeën). De rol van de programmamanager bestaat uit het management en de operationele coördinatie van het onderzoeksprogramma (VR 2019 1312 DOC.1235/1). De programmamanager werd in 2023 aangeworven zodra het programma op kruissnelheid waas gekomen. De rol van programmamanager werd in de evaluatie als positief ervaren en wordt verdergezet. Bijkomend zal de programmamanager (en -directie) toezien op de naleving van de nieuwe structurele aanpassingen, zoals de focus op de communicatie-initiatieven.

Daarnaast werkt het programmamanagement nauw samen met de *'Track Leaders'*. Dit zijn telkens experten uit de corresponderende onderzoekslijnen:

1. Software- en Applicatiebeveiliging o.l.v. prof. Bart Jacobs;
2. Beveiligingsdiensten o.l.v. prof. Tom Van Cutsem;
3. Systeem- en Infrastructuurbeveiliging o.l.v. prof. Frank Piessens;
4. Technologiebouwstenen zoals veilige hardware en cryptografie o.l.v. prof. Ingrid Verbauwhede.

De evaluatie gaf eveneens aan dat de lage administratieve lasten en de flexibiliteit voor onderzoekers in de keuze voor onderwerpen en de inzet van middelen een positieve impact heeft op de efficiëntie en relevantie van het beleidsplan. Wel suggereert de evaluatie om de duidelijkheid van de rapportering te verbeteren. Dit moet niet-deskundigen in staat stellen om de informatie te begrijpen, te evalueren en op een doordachte manier beslissingen te nemen op basis van deze rapporten. We

besteden hier dit jaar aandacht aan via de nieuwsbrief als toegankelijke, tussentijdse en niet-formele rapportering van de vooruitgang van het beleidsplan.

Daarnaast wordt vanaf dit jaar ook een valorisatiemanager aangesteld, wiens rol eerder werd toegelicht in de sectie 'Valorisatie'.

Stuurgroep

De nota aan de Vlaamse Regering van 22 maart 2019 (VR 2019 2203 DOC.0317/1QUATER) bepaalde de oprichting van een stuurgroep voor het globale CS-programma (voor de drie luiken samen):

"Het globale programma wordt opgevolgd door een stuurgroep die opgezet wordt onder leiding van het Departement EWI en VLAIO met een vertegenwoordiging van de relevante stakeholders uit het bedrijfsleven en het onderzoeksveld. Om deze stuurgroep slagkrachtig te laten beslissen, telt zij maximaal 12 leden, waarbij de verschillende stakeholders werken via het principe van vertegenwoordiging uit hun bestaande overlegstructuren."

Op 7 juni 2019 duidde de Vlaamse Regering de leden aan van de stuurgroep van het Vlaamse Beleidsplan Cybersecurity (VR 2019 0706 DOC.0866/1BIS).

Het evaluatierapport stelt dat het beleidsplan *"een nieuwe, tweede fase in[gaat], die een andere vorm van governance vraagt, met meer sturing op tactische en operationele samenhang en minder op strategie."* De stuurgroep wordt daarom deels opnieuw samengesteld. Naast de kennisinstellingen en vertegenwoordigers van de overheid, worden vertegenwoordigers uit de industrie (met voldoende O&O-kennis) als essentieel ervaren. VLAIO en het departement EWI zullen een lijst van geschikte bedrijven opmaken en in overleg met deze bedrijven een geschikte vertegenwoordiger zoeken. De vernieuwde samenstelling van de stuurgroep wordt in de loop van het tweede kwartaal van 2024 aan de regering meegedeeld, en is opgebouwd als volgt:

Kennisinstellingen

- Rotatie VUB, UAntwerpen en UHasselt
- Rotatie VITO en Flanders Make
- Imec
- Vertegenwoordiger van de hogescholen
- UGent
- KU Leuven
- Onderzoeker uit een Nederlandse kennisinstelling

Industrie

- Zeven voldoende diverse industriële spelers

Overheid

- Kabinet beleidsdomein Werk, Economie, Wetenschap, Innovatie, Landbouw en Sociale economie
- Departement Economie, Wetenschap en Innovatie
- VLAIO
- Digitaal Vlaanderen (adviserend: leveren technische expertise aan en wijzen op opportuniteiten)
- National Competence Centre/ Cybersecurity Centre Belgium (waarnemend: leveren technische expertise aan en wijzen op opportuniteiten)

De wijzigingen in de vertegenwoordiging van de Stuurgroep worden toegelicht.

- Het behouden van imec zorgt voor sterke opportuniteiten met het AI- onderzoeksprogramma op technisch niveau, aangezien imec de programmadirectie afvaardigt van het Vlaamse Beleidsplan Artificiële Intelligentie.

//

- Er wordt een (Nederlandstalige) onderzoeker uit een Nederlandse universiteit gezocht. Hiermee kunnen we een expert vinden die buiten het consortium staat en kan een vergelijkend interlandelijke perspectief worden geboden en ook het bredere beleidsplan kan volgen, in interactie met de andere leden. Voor de ISAB is dit moeilijker omwille van de taalbarrière en omdat dit in se niet tot hun takenpakket behoort (enkel focus op onderzoeksprogramma).
- Digitaal Vlaanderen wordt structureel betrokken als adviserende partner in de stuurgroep. Voorts wordt een adviserende rol toegevoegd voor Cybersecurity Centre Belgium (CCB). Beide zullen technische expertise aanleveren, wijzen op verschillende opportuniteiten, en waar opportuun raakpunten zoeken met hun eigen cybersecurity-beleid.
- De andere rollen worden behouden, maar de bij de selectie wordt meer belang gehecht met een sterke ervaring of voeling met de technische noden. Hierdoor is de Stuurgroep in staat de techniciteit van de voorstellen en resultaten te capteren.

De Stuurgroep wordt weliswaar groter, maar dit laat toe om meer dynamische discussies te voeren of waar nodig op te splitsen om '*deep dives'* te houden over bepaalde thema's.

ISAB

Aan de huidige leden van de ISAB wordt gevraagd wie zijn/haar mandaat wenst te verlengen na het aflopen van de eerste cyclus. In de loop van 2024 zal het Departement EWI in samenwerking met het Fonds Wetenschappelijk Onderzoek – Vlaanderen (FWO) eventuele vervangers/opvolgers aanzoeken. De ISAB zal, in zijn vernieuwde samenstelling, opnieuw bijeenkomen in het vierde kwartaal van 2024 om zich te buigen over de prestaties van het onderzoeksprogramma in werkjaar 5.

Flankerend beleid

Gezien de inkanteling van het opleidingsprogramma en het communicatieprogramma binnen flankerend beleid in het onderzoeksprogramma (incl. het stopzetten van de open oproepen), zal KU Leuven de overgebleven activiteiten die onder het flankerend beleid vallen coördineren. De rol van Howest tijdens de afgelopen twee werkjaren als link voor de communicatie met de hogescholen voor de open oproepen valt weg.

Als gevolg van het stopzetten van de open oproepen wordt de Beoordelingscommissie opgeheven. Deze had als taak om de inzendingen van de open oproepen te beoordelen en zo de minister te adviseren bij de toekenning van de middelen van de open oproepen (VR 2020 2711 DOC.1303/1).
De acties van VLAIO met het oog op de competentieopbouw rond cyberveiligheid bij (toekomstige) werknemers worden ondergebracht binnen het hierboven vermelde programma digitale transformatie.

Evaluatie tweede cyclus

Het beleidsplan zal opnieuw geëvalueerd worden richting het einde van de tweede cyclus. Daartoe worden reeds onderstaande bepalingen opgenomen die de scope van de volgende evaluatie capteren:

§1. De algemene werking van het Vlaamse Beleidsplan Cybersecurity voor de periode 2024-2028 wordt geëvalueerd aan de hand van de Strategische Doelstellingen (SD's) en Kritieke Prestatie-Indicatoren (KPI's) die in het Vlaamse Beleidsplan Cybersecurity 2024-2028 en zijn jaarlijkse inhoudelijke programma's (onderzoeksprogramma, Implementatieluik en Flankerend beleid) vooropgesteld zijn.

§2. De evaluatie zal in principe rekening houden met:
- het Vlaamse Beleidsplan Cybersecurity 2024-2028 en het behalen van de SD's en de KPI's zoals geformuleerd in dit beleidsplan en in zijn jaarlijkse inhoudelijke programma's;
  - Geen evaluatie van de reguliere VLAIO-maatregelen voor het Implementatieluik, maar wel een evaluatie van hoe de ingezette instrumenten bijdragen aan de doelstellingen van het Implementatieluik en van het beleidsplan;

- De werking van de governancestructuren van het beleidsplan en zijn onderdelen, alsook de invulling van de verschillende rollen;
- de jaarverslagen die de programma-uitvoerders tijdens de duur van dit beleidsplan hebben bezorgd voor het onderzoeksprogramma en het flankerend beleid van het beleidsplan;
- de gezamenlijke zelfevaluatie voor het onderzoeksprogramma en het Flankerend beleid die de programma-uitvoerders hebben opgesteld;
- het beleidsplan Wetenschapscommunicatie;
- de correcte aanlevering van data aan FRIS;
- een bibliometrische (en technometrische) analyse voor het onderzoeksprogramma;
- het oordeel van een internationaal panel van experten over het onderzoeksprogramma dat voor deze beoordeling onder andere een bezoek ter plaatse brengt;
- een benchmark met andere vergelijkbare beleidsplannen;
- een analyse van de impact van de activiteiten van het beleidsplan op het Vlaamse maatschappelijke en economische weefsel m.b.t. wetenschap, technologie en innovatie;
- de resultaten van de vorige evaluatie;
- andere relevante evaluaties die uitgevoerd werden in de periode waarop het beleidsplan betrekking heeft.

Verder besteedt de evaluatie indien relevant aandacht aan:

1° de relatie van het beleidsplan met en de plaats van het beleidsplan ten opzichte van andere middelen/instrumenten/actoren voor onderzoek en innovatie en wat betreft wetenschapscommunicatie;
2° de rol en positie van het beleidsplan in het bredere Vlaamse onderzoeks- en innovatiesysteem;
3° transversale beleidsthema's of andere aspecten die raken aan het beleidsplan.

§3. Nadere bepalingen over de inhoud van de evaluatie en de reikwijdte zullen uiterlijk in het voorlaatste jaar (2027) van de periode waarop het beleidsplan betrekking heeft, worden opgesteld door het Departement EWI en toegelicht aan de programma-uitvoerders.

§4. De kosten van de evaluatie worden door het Departement EWI gedragen.

§5. De evaluatie wordt door het Departement EWI georganiseerd in de eerste helft van 2028 en moet afgerond zijn op 30 juni 2028.

§6. Het Departement EWI zal voor de evaluatie de gepaste evaluatieorganen aanstellen die over de expertise beschikken om de activiteiten, de resultaten en het potentieel van de uitvoering van het beleidsplan en zijn inhoudelijke programma's vakkundig te beoordelen. Daarbij zullen de algemene en specifieke procedures gevolgd worden die het Departement uitgewerkt heeft. Meer informatie over de evaluatieprocedures is opgenomen in het evaluatiekader van het Departement EWI.

§7. De zelfevaluatie bestaat uit zowel een ex-post- als een ex-antegedeelte en wordt door de programma-uitvoerders opgesteld op basis van een leidraad/richtlijnen die het Departement EWI aanreikt. Het ex-antegedeelte van de zelfevaluatie behelst het opstellen van een ontwerp van strategisch plan voor de periode die volgt op de looptijd van dit beleidsplan. Dat ontwerp van strategisch plan zal mee beoordeeld worden in het kader van de evaluatie van het lopende beleidsplan 2024-2028 en zijn inhoudelijke programma's. De volledige zelfevaluatie wordt beschouwd als een werkdocument dat input levert voor de evaluatie. Na de evaluatie kan de zelfevaluatie, voornamelijk het ex-antegedeelte, verder evolueren tot een definitief strategisch plan.

B. ONDERZOEKSPROGRAMMA CYBERSECURITY: SUBSIDIE VIJFDE WERKJAAR

Doelstellingen Werkjaar 5

Het programma voor 2024 is gebaseerd op de positieve evaluatie van de internationale experten in 2023. Het ex-anteluik van de zelfevaluatie, dat werd opgesteld door de programmadirectie van het onderzoeksprogramma, werd positief onthaald en als leidraad gebruikt bij het formuleren van de algemene inhoudelijke doelstellingen voor 2024.

De basisstrategie van het onderzoeksprogramma loopt uiteraard in lijn met de voorgestelde planning van het ex-anterapport (2023). Er wordt gewerkt volgens vier onderzoekslijnen ('tracks') die elkaar versterken en op elkaar inspelen, en die elk een ander potentieel brengen voor het Vlaamse Beleidsplan Cybersecurity.

1. *Track* 1: Software- en Applicatiebeveiliging. Het onderzoeksprogramma zet verder in op diverse aspecten van de ontwikkeling van veilige software, met veel aandacht voor de ontwerpfase ("Cybersecurity-by-Design"). Bovendien worden nieuwe oplossingen ontwikkeld op het vlak van verificatie en cybersecurity-testing, wat zeer belangrijk is voor het verhogen van cybersecuritykwaliteit en -garanties. Er wordt ook ingezet op het versterken van programmeertalen. Strategisch basisonderzoek staat hierbij aan de wieg van nieuwe beveiligingsomgevingen, het creëren en het verifiëren van beveiligingsbewijzen voor de uitvoeringsomgeving van een nieuwe generatie computerprogramma's en voor het ondersteunen van policy-talen.
2. *Track* 2: Security-services. De basisgedachte in deze track is dat beveiligingsbouwblokken worden ontwikkeld en verbeterd. Dit zijn bouwblokken die op termijn kunnen en moeten helpen om sneller beveiligingsoplossingen te maken en te integreren in applicatieraamwerken en -platformen.
3. *Track* 3: Systeem- en infrastructuurbeveiliging. De beveiligingsgaranties van ICT-toepassingen en diensten zijn in belangrijke mate afhankelijk van de beveiliging die geleverd wordt door de onderliggende infrastructuur en systemen waarop deze diensten en toepassingen worden uitgerold. *Track* 3 richt zich helemaal op het infrastructuurgegeven. Een eerste thema kijkt naar individuele systemen (*single nodes*), een tweede thema adresseert het netwerk, en een derde thema richt zich op het monitoren van de beveiligingsproblematiek, met aandacht voor het uitrollen van verbeteringen.
4. *Track* 4: Basisbouwblokken voor cyberbeveiliging. *Track* 4 concentreert zich op onderzoek en innovatie in het domein van cryptografie en op het vlak van hardwarebeveiliging en veilige implementaties. Op het vlak van cryptografie staat het consortium – met COSIC (KU Leuven) – aan de top in de wereld. Het consortium bouwt hier verder op een extreem solide track record.

Ten opzichte van de vorige jaren worden verschillende nieuwe accenten gelegd of verkend die de impact van het onderzoeksprogramma op middellange termijn zullen verhogen:

1. Een groeiend gedeelte van de onderzoeksinspanningen wordt gericht op **defensieve aspecten van cybersecurity**. Deze keuze werd initieel gemaakt in 2023 en wordt verder doorgetrokken.
2. De verdere validatie van sterke resultaten wordt doorgetrokken in het ontwikkelen, testen en valideren van betrouwbare **prototypes**. Voor 2024 zal het onderzoeksconsortium ten minste 3 prototypes verder in de verf zetten.
   Zowel de inzet op defensieve aspecten als op prototypes kan de impact van het onderzoeksprogramma verhogen.
3. Verhoogde samenwerking binnen het **Europees kader**. Het onderzoeksconsortium zal een aantal speerpunten van het Vlaamse onderzoek bundelen met andere partners in Europa en een aantal deelthema's verder uitwerken binnen het Europees kader.

Het budget dat vrijkomt door de herverdeling vanuit het flankerende beleid, wordt gebruikt om het consortium uit te breiden met de onderzoeksgroep onder leiding van prof. An Braeken (VUB - ETRO-ECLIPS). In dit eerste opstartjaar is er nog geen volledige benutting van het beschikbare budget voorzien. Daarom zal dit niet-benutte budget in 2024 eenmalig worden aangewend voor minstens twee projecten, namelijk een referentieplatform voor IoT-beveiliging onder leiding van COSIC en een project rond de gecombineerde aanpak van cybersecurity-, resilience- en safety-vereisten in digitaliseringsvereisten onder leiding van DistriNet (KU Leuven). Dit zijn kortlopende projecten die een aantal onderzoeksactiviteiten en resultaten versneld dichter bij industriële toepasbaarheid brengen. De ambitie is om in 2025 de industriële samenwerking rond deze twee elementen te versterken. De meeste consortiumpartners dragen bij aan deze projecten.
Naast voorgaande strategisch-kwalitatieve doelstellingen worden ook verschillende kwantitatieve KPI's geformuleerd.
Enkele belangrijke beschouwingen bij de vooropgestelde cijfers.

- De inflatie en loonindexering vormen een uitdaging voor de realisatie van resultaten bij gelijkblijvend budget;
- Het sterke engagement gericht op defensieve cybersecurity-oplossingen en op een groeiend aantal sterk uitgebouwde prototypes zorgt voor een hogere VTE-kost per publicatie, aanzienlijk hoger dan voor ander onderzoek.

De KPI's worden weergegeven in onderstaande tabel.

KPI's Basisonderzoek Cybersecurity		Prognose werkjaar 5
Onderzoeksresultaten		
KPI O1.1	Aantal peer-reviewed publicaties met steun van het CS-programma, d.w.z. waarvan minstens 1 van de auteurs financiering van het CS-onderzoeksprogramma heeft ontvangen	**105**
KPI O1.2	Aantal peer-reviewed cybersecurity-publicaties waarvan minstens één van de auteurs geaffilieerd is met één van de onderzoeksgroepen van het CS-programma	**200**
Menselijk kapitaal vanuit het onderzoek		
KPI O2.1	Aantal doctorandi met een (co)promotor uit de groep Hoofdonderzoekers (`PI's – Principal Investigators')	**160**
KPI O2.2	Aantal afgelegde doctoraten met een (co)promotor uit de groep Hoofdonderzoekers	**24**
Samenwerking met bedrijven zonder overheidssteun		
KPI R1.1	Bedrag (voor de onderzoekspartners) uit samenwerkingen met actoren (zowel Vlaamse als niet-Vlaamse actoren) (excl. overheidssubsidies)	**500 000**
KPI R1.2	Aantal samenwerkingen met de actoren (excl. overheidssubsidies)	**24**
Samenwerking met bedrijven met overheidssteun		

KPI R2.1	Bedrag (voor de onderzoekspartners) uit samenwerkingen[1] met actoren met subsidie van de Vlaamse overheid (o.a. via VLAIO)	**1.800.000**
KPI R2.2	Aantal samenwerkingen met actoren met subsidie van de Vlaamse overheid (o.a. via VLAIO)	**126**
Internationale onderzoeksfinanciering		
	Bedrag verkregen uit de internationale programma's of andere internationale organisaties of stichtingen. De financiering is toegekend aan een team waarvan één van de leden geaffilieerd is met één van de onderzoeksgroepen van het CS-programma.	

Begrotingsvoorstel

Voor de consortiumuitbreiding met de VUB-onderzoeksgroep o.l.v. prof. An Braeken wordt in 2024 een budget van 240.000 euro voorzien dat vanaf 2025 – i.e. na opstart – kan toenemen tot 360.000 euro. Deze toename (vanaf 2025) wordt al binnen de huidige budget kader (9 miljoen euro) voorzien. De financiering voor de eenmalige projecten wordt pas vrijgegeven na een indiening van het opzet van deze projecten en goedkeuring door het Departement EWI. De subsidie-aanvraag bevat het opzet, de te behalen doelstellingen en de budgettaire vraag (met een maximum van 222.193 euro voor alle projecten samen).

De tabel hieronder bevat een samenvatting van het begrotingsvoorstel voor werkjaar 5 per onderzoekslijn en per kennisinstelling. Het budget voor werkjaar 5 bedraagt in totaal 8.970.200 euro. Deze middelen worden uitbetaald zoals bepaald in het Besluit van de Vlaamse Regering.

	KU Leuven			VUB	UGent	imec	VUB	Totaal
Basis-onderzoek 2024	**COSIC**	**DistriNet**	**CiTiP**	**SOFT**	**CSL**	**DRE**	**Team An Braeken**	
Begroting (Euro)	**3.181.934**	**3.415.124**	**459.902**	**613.461**	**459.200**	**590.579**	**250.000**	**8.970.200**
TRACK 1		885.868		593.461				1.479.329
TRACK 2	590.579	590.579	444.902				240.000	1.866.060
TRACK 3	590.579	1.624.390			444.200			2.659.169
TRACK 4	1.919.679					590.579		2.510.258
Coördinatie		158.191						158.191
Valorisatie		75.000						75.000
Eenmalige projecten 2024	81.097	81.097	15.000	20.000	15.000		10.000	222.193

Het inhoudelijke en budgettair voorstel voor het onderzoeksprogramma cybersecurity werkjaar 5 gaat in bijlage 3.
Deze middelen zullen uitbetaald worden door middel van een subsidiebesluit (zie bijlage 2).

[1] Samenwerkingen zijn projecten die voldoen aan de voorwaarden inzake kennisopbouw bij ondernemingen of collectieve kennisverspreiding. Typische voorbeelden zijn ICON, TETRA en COOCK.

Open science en FRIS – FLANDERS RESEARCH INFORMATION SPACE

Het onderzoek verricht in het kader van het CS-onderzoeksprogramma dient te worden opgenomen in Flanders Research Information Space (FRIS)[2] om de informatie beter te ontsluiten en zichtbaarder te maken (in het kader van open-sciencebeleid). De nodige criteria daartoe worden doorgesproken met de programmamanager.

De consortiumpartners onderschrijven het Vlaamse open-sciencebeleid en de principes van Open Science volgens het principe "zo open als het kan, zo gesloten als nodig". Dit geldt zowel voor de toegang tot publicaties als voor de toegang tot de achterliggende onderzoeksdata.

C. FLANKEREND BELEID: SUBSIDIE DERDE WERKJAAR

Doelstellingen Werkjaar 3

Het doel van het flankerende beleid is de Vlaamse vooruitgang in onderzoeksresultaten en kennis maximaal te laten doorstromen naar een groep van stakeholders die met versterkte kennis en inzicht aan de slag kunnen gaan om binnen hun eigen context vooruitgang te boeken op het vlak van cyberveiligheid.

De voorbije drie kalenderjaren resulteerde het flankerend beleid in een geslaagde, geleidelijke opbouw van heel wat resultaten zowel content – toegankelijke artikels rond cybersecurity – voor communicatie naar diverse doelgroepen, als cursusmateriaal voor diverse stakeholders. Een heel groot deel van deze resultaten werd gerealiseerd door leden van het onderzoeksconsortium en een beperkte hoeveelheid bijdragen werd door (voor het onderzoeksconsortium) 'externe' partners aangeleverd na een kandidaatstelling bij open oproepen. Zoals eerder toegelicht worden de open oproepen stopgezet wegens de geringe participatie. Het is echter belangrijk om blijvend te communiceren over belangrijke cybersecuritytrends en te sensibiliseren over cybersecuritydreigingen en -oplossingen.

Daarom wordt er in deze tweede cyclus gespecialiseerd materiaal geleverd door het onderzoeksconsortium. Op die manier wordt er bijgedragen aan de strategische doelstellingen uit het Vlaamse Beleidsplan Cybersecurity en blijft de Nederlandstalige website https://cybersecurity-bites.be/ in gebruik als platform voor de verspreiding van deze gespecialiseerde content. Het uitgangspunt is dat deze content aansluit bij de actuele evoluties en trends in cybersecurity.

Daarnaast worden er ook belangrijke events georganiseerd om de doelstelling waar te maken.

Deze strategische doelstellingen leiden in 2024 tot onderstaande KPI's.

Opleidingen	
Summer Schools, Experten-bijeenkomsten	
Summer Schools	2
Expertenbijeenkomsten	6
Geavanceerde opleidingen (productie en uitrol)	3

Outreach & Communicatie	
Industrie-event	1
Participatie in partner-events	2

[2] FRIS is het platform dat wordt beheerd door het Departement EWI en biedt informatie over publiek gefinancierd onderzoek in Vlaanderen.

Content – artikels	45
Kompas-bijdragen	3
Nieuwsbrieven	3
Persberichten	3

Opleidingen

De nadruk ligt op de ontwikkeling van geavanceerd cursusmateriaal, op de organisatie van ten minste twee PhD-schools, en op de organisatie van ten minste zes expertenbijeenkomsten.

Cursusmateriaal

Op het vlak van geavanceerd cursusmateriaal worden in lijn met de bestaande strategie ingezet op de uitwerking van drie nieuwe opleidingen/cursussen:

1. *'Fuzzing for Security Testing and Security Evaluation'*
2. *'A Development Roadmap for Compliance'*
3. *'Advanced Data Protection for security and privacy in Machine Learning and federated ML'*

Deze opleidingen vangen een hiaat in het aanbod op, spelen in op concrete noden van het bedrijfsleven en sluiten nauw aan bij de competenties van het onderzoeksconsortium.

Training Events:

Er komen jaarlijks 2 'Summer Schools' voor onderzoekers:

- Thema Summer School 1: '*Cybersecurity and Machine Learning*' (3de Editie – September 2024);
- Thema Summer School 2: meerdere opties, finaal vast te leggen in Q1 ('*Testing and Verification 4 Cybersecurity*' is de eerste optie).

Verder worden er regelmatig expertenbijeenkomsten georganiseerd, waarvan minstens drie in het voorjaar en drie in het najaar (net als in 2023).

De Summer Schools bestaan uit een intensief programma over meerdere dagen waarin een nieuw onderwerp bij experten en onderzoekers grondig wordt geïntroduceerd. Expertenbijeenkomsten zijn kortere events van een of twee halve dagen waar een innovatief concept wordt voorgesteld en de focus vaak ligt op concrete applicaties en gevalstudies.

Outreach & communicatie

Er wordt verder geïnvesteerd in proactieve communicatie rond het beleidsplan als geheel. Zo worden er dit jaar twee nieuwe zaken gelanceerd, namelijk elke vier maanden een nieuwsbrief en de productie van persberichten. Deze bevat een vooruitblik en blikt ook deels terug op events en resultaten, zowel in onderzoek als praktijk, gericht op een breed spectrum van stakeholders in overheid, industrie en onderzoek. Hierbij komt hoofdzakelijk het beleidsplan aan bod, zonder daarbij onze blik op de wereld te verliezen.

Naast deze periodieke update (wellicht maart – juni – oktober) willen we vanuit het flankerende beleid ook regelmatig inzoomen op actuele hoogtepunten, bv. de aandacht vestigen op spraakmakende onderzoeksresultaten.

Naast de creatie en distributie van online content omvat het flankerende beleid ook het (intussen gevestigde) jaarlijkse industrie-event.

Dit alles draagt bij tot een verhoogde visibiliteit, sensibilisering en valorisatiekans.

Industrie-Events

Het jaarlijks flagship-event wordt georganiseerd vanuit het beleidsplan en vormt het belangrijkste ontmoetingspunt met het oog op interactie, samenwerking en synergie tussen onderzoek en industriële innovatie. De ondernemingsdoelgroep van dit event zijn eerder de innovatieleiders en technologie-aanbieders dan de grote groep van innovatievolgers.

Bijkomend worden er samenwerkingen opgezet om een aantal events (ten minste twee) te organiseren ter ondersteuning van derden. Hierbij wordt de visibiliteit van het beleidsplan maximaal bewaakt en worden de contacten met de industrie verder bevorderd.

Geavanceerde content online

De "*Bites*" https://cybersecurity-bites.be/ worden verder uitgebreid met

- 45 artikels, waaronder ongeveer 30 geavanceerde artikels en 15 ter ondersteuning van een ruimere kennisverspreiding;
- Drie kompasbijdragen, nl.
    i. een bijdrage rond het bedreigingslandschap (*Threat Landscape*);
    ii. een gerichte bijdrage rond de ondersteuning van ontwikkelaars van software, systemen en diensten;
    iii. een bijdrage die inzoomt op een belangrijke intersectie tussen cybersecurity en dominante trends in ICT (zoals bv AI/ML, 5G/6G);
- Wegwijs, bits & bytes: het verder afwerken en onderhouden van vakjargon (o.a. naar een "top" 100 van cybersecuritytermen).

Het cybersecurity-kompas tracht op een toegankelijke manier analyses en studies over het cybersecuritylandschap weer te geven op basis van markt-neutrale topexpertise. De nadruk binnen het kompas ligt op actuele prioriteiten waarrond een dringende nood aan toegankelijke kennis bestaat.

De onderzoekssite van het onderzoeksprogramma (https://cybersecurity-research.be/) wordt uitgebreid met de Engelstalige versie van de meer geavanceerde artikels, die dan ook dichter aanleunen bij het onderzoeksprogramma.

Begrotingsvoorstel

Het budget voor het flankerende beleid in 2024 bedraagt in totaal 604.800 euro en is als volgt samengesteld, in lijn met de uitgaven van het vorige werkjaar. Het budget voor de open oproepen (overgedragen naar het onderzoeksprogramma) is hierbij geschrapt.

Opleidingen	321.800 €
Summer Schools, Expert Gatherings	149.000 €
Geavanceerde opleidingen	172.800 €
Contentproductie en -distributie	
Outreach & communicatie	283.000 €
Events	62.500 €
Content	131.000 €
Web & media	89.500 €
Totaal budget Flankerend beleid	**604.800 €**

Het inhoudelijke en budgettaire voorstel voor het flankerende beleid in werkjaar 3 gaat in bijlage 3. Deze middelen worden uitbetaald overeenkomstig het besluit van de Vlaamse Regering (bijlage 2).

3. BESTUURLIJKE IMPACT

D. BUDGETTAIRE IMPACT VOOR DE VLAAMSE OVERHEID

Voor het vijfde werkjaar van het onderzoeksprogramma Cybersecurity (01/01/2024 – 31/12/2024) wordt een subsidie toegekend van maximaal 8.970.200 euro. De begunstigden zijn de universiteiten KU Leuven, UGent, VUB en het strategisch onderzoekscentrum imec. Deze subsidie wordt aangerekend op de Lissabonlijn van het departement EWI, zijnde begrotingsartikel EB0-1EEB2JY-IS voor de universiteiten en op begrotingsartikel EB0-1EEB2JA-WT voor imec van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2024.

Voor het derde werkjaar van het Flankerend beleid (01/01/2024 – 31/12/2024) wordt een subsidie toegekend van maximaal 604.800 euro. De begunstigde is de KU Leuven. Deze subsidie wordt aangerekend op de Lissabonlijn, zijnde begrotingsartikel EB0-1EEB2JY-IS van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2024.

Voorts wordt 75.000 EUR herverdeeld binnen EWI. Bij Begrotingsaanpassing kan dit bedrag vanuit de VLAIO-lijnen, begrotingsartikel EC0-1ECB5DY-IS, herverdeeld worden. De herverdeling gebeurt naar artikel EB0-1EEB2JY-IS en is bestemd voor het onderzoeksluik.

Het gunstig advies van de Inspectie van Financiën werd verleend op 13/02/2024 voor beide subsidies.

Het begrotingsakkoord werd aangevraagd op 18/03/2024 voor beide subsidies.

E. ESR-TOETS

Aangezien de beschikbare middelen binnen het budget van het begrotingsjaar 2024 voorzien zijn, is een ESR-toets niet van toepassing.

F. IMPACT OP HET PERSONEEL VAN DE VLAAMSE OVERHEID

Het voorstel heeft geen weerslag op het personeelsbestand en op het personeelsbudget, zodat het akkoord van de Vlaamse minister, bevoegd voor het algemeen beleid inzake personeel en organisatieontwikkeling, niet vereist is.

G. IMPACT OP DE LOKALE EN PROVINCIALE BESTUREN

Het voorstel van beslissing heeft geen weerslag op de werking van de lokale besturen.

4. VERDER TRAJECT

De samenstelling van de CS-stuurgroep wordt in overleg met de vertegenwoordigde organisaties en zoals voorzien in deze nota aangepast en zal aan in het tweede kwartaal van 2024 aan de Vlaamse Regering meegedeeld worden.

In de eerste helft van 2024 volgt de uitbetaling van het saldo voor het onderzoeksprogramma en flankerend beleid (onder EWI-beheer) voor het kalenderjaar 2023 op basis van de verslaggeving voor dat jaar en bij goedkeuring door het Departement EWI.

Deze nota betreft de financiering van het vijfde werkjaar van het onderzoeksprogramma cybersecurity en het derde werkjaar voor het flankerend beleid. De uitbetaling gebeurt volgens de bijgevoegde besluiten van de Vlaamse Regering.

De financiering van de eenmalige projecten in het onderzoeksprogramma cybersecurity, werkjaar 5, worden uitbetaald na indiening van een subsidieaanvraag en goedkeuring door het Departement EWI.

De gedetailleerde uitwerking en aanpak van het programma ter bevordering van de digitale transformatie bij kmo's en innovatievolgers zal op een later tijdstip onder de vorm van een conceptnota aan de Vlaamse Regering worden voorgelegd.

Het zesde werkjaar van het onderzoeksprogramma Cybersecurity en het vierde werkjaar van het Flankerend beleid lopen naar verwachting van 01/01/2025 – 31/12/2025.

In de loop van 2027 wordt een externe evaluatie van het volledige beleidsplan Cybersecurity voorbereid en opgestart, waarbij zowel de onderdelen op zichzelf als hun samenhang met de andere onderdelen, als hun bijdrage tot en hun plaats in het geheel van het Vlaamse Beleidsplan CS, geëvalueerd zullen worden, conform de bepalingen zoals opgenomen in deze nota.

5. VOORSTEL VAN BESLISSING

De Vlaamse Regering beslist:

1° haar goedkeuring te hechten aan het voortzetten van het Vlaamse Beleidsplan Cybersecurity voor een volgende vijfjarencyclus met de aanpassingen zoals voorgesteld in deze nota;

2° haar goedkeuring te hechten aan het ontwerpbesluit van de Vlaamse Regering tot herverdeling van begrotingsartikelen van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2024 in het kader van de 2de cyclus van het Vlaamse Beleidsplan Cybersecurity;

3° haar goedkeuring te hechten aan het ontwerpbesluit van de Vlaamse Regering betreffende de toekenning van een subsidie aan het onderzoeksprogramma Cybersecurity (vijfde werkjaar) en de subsidie voor het luik Flankerend beleid (derde werkjaar) voor de periode 01/01/2024 tot en met 31/12/2024;

4° de Vlaamse minister, bevoegd voor het wetenschapsbeleid en het technologisch innovatiebeleid, te belasten met de uitvoering van deze beslissing.

De Vlaamse minister van Economie, Innovatie, Werk, Sociale Economie en Landbouw

Jo BROUNS

Bijlagen:

B1 – Besluit van de Vlaamse Regering tot herverdeling van begrotingsartikelen van de algemene uitgavenbegroting van de Vlaamse Gemeenschap voor het begrotingsjaar 2024 in het kader van de 2de cyclus van het Vlaamse Beleidsplan Cybersecurity.

B2 – Ontwerpbesluit van de Vlaamse Regering betreffende het Vlaamse Beleidsplan Cybersecurity (tweede cyclus) en een subsidie voor het onderzoeksprogramma Cybersecurity (vijfde Werkjaar) en een subsidie voor het Flankerend beleid (Werkjaar 3)

B3 – Vlaams cybersecurity programma - strategisch basisonderzoek en flankerend beleid 2024

B4 – *International Scientific Advisory Board Cybersecurity Initiative Flanders - Assessment of the Strategic Research Program*

B5 – De evaluatie van het Vlaamse Beleidsplan Cybersecurity: eindrapportage (opgesteld door Technopolis, september 2023) (vertrouwelijk)

B6 – Advies Inspectie van Financiën

B7 - Begrotingsakkoord d.d. 18 maart 2024.