Projectvoorstel Cybersecurity Noord-Nederland

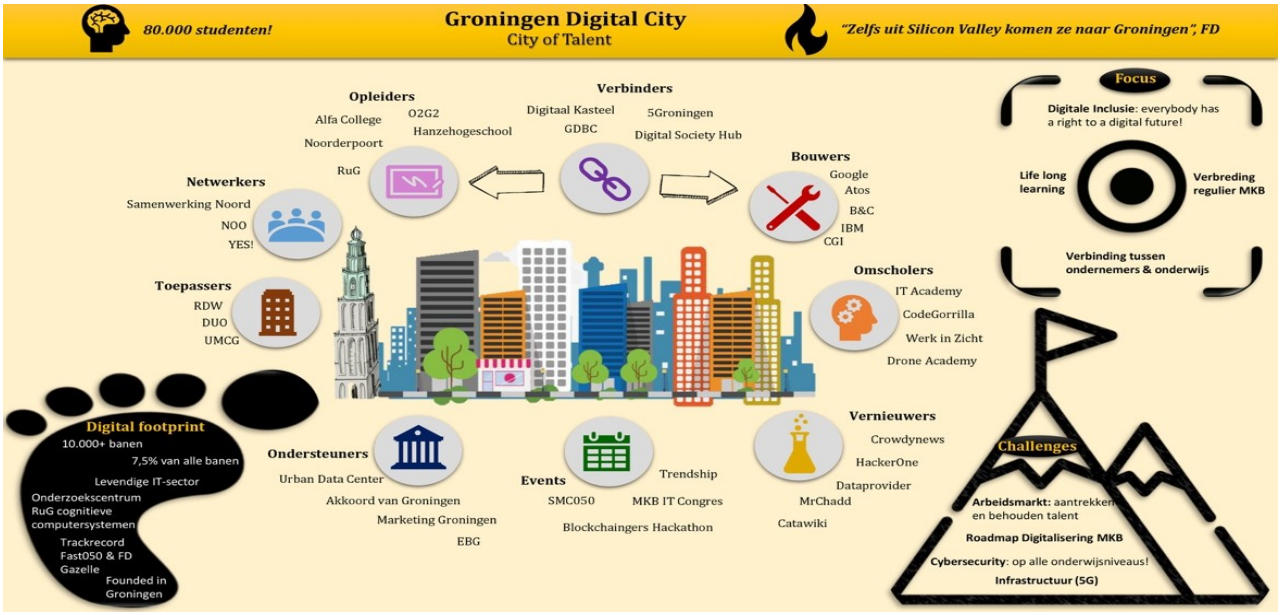
Versie 24/01/2019

Contents

1 Omschrijving programma

1.1 Aanleiding

Digitalisering speelt een belangrijke rol in onze samenleving en onze economie. Door toenemende digitalisering neemt dit belang alleen maar verder toe. Digitalisering stelt ons bijvoorbeeld in staat om onze industrie te verduurzamen, zorg bereikbaar en betaalbaar te houden en online meer producten te verkopen. Noord-Nederland kent een snelgroeiende digitalisering en heeft daarmee een sterke positie in de digitale economie in Nederland en daarbuiten verworven. Belangrijk is deze positie verder wordt verstevigd. Daarom wordt er door bedrijven, overheden en kennisinstellingen geïnvesteerd in: 1. Samenwerking tussen bedrijven en organisaties in het Noorden (o.a. de Noordelijke Online Ondernemers (NOO) en Samenwerking Noord) en 2. Het verhogen van het kennisniveau op specifieke thematische gebieden, zoals via het Groningen Digital Business Centre (GDBC) (digital business), de Digital Literacy Coalition (DLC) (digital literacy), het Mobility Innovation Center (MIC) (mobility), de Noorderlijke Smart Industry Hub, dHealth Lab). 3. Het inrichten van specifieke onderwijsprogramma's op het gebied van de digitale samenleving (zoals bijvoorbeeld ICT & Recht (Engels en Nederlandstalig programma) (RUG), Governance and Law in Digital Society (RUG – Campus Fryslân New Business & ICT (Hanzehogeschool), de werkplaats digitaal vakmanschap in het Nieuwe Kasteel (Noorderpoort), de IT-Academy etc. Dit alles leidt tot het ontstaan van een digitaal ecosysteem in Noord-Nederland (zie onderstaand figuur).



Figuur 1 Afbeelding Groningen Digital City

Om nadere samenwerking tussen de belangrijkste stakeholders op het gebied van digitalisering in de Provincie Groningen te bevorderen is in 2018 besloten tot de oprichting van de Coalitionboard. Hierin nemen vertegenwoordigers zitting vanuit onderwijs- en kennisinstellingen, de gemeente Groningen en provincie, met een staande uitnodiging voor participatie van het Ministerie van Economische Zaken en Klimaat (EZK). Het bedrijfsleven vraagt aandacht voor, en benadrukt het belang van, een doorlopende leerlijn van basisschool tot wetenschappelijk onderwijs om de kennis van digitale veiligheid te

verbeteren. Daarom heeft de Provincie Groningen het initiatief ingebracht om een dergelijke doorlopende leerlijn te implementeren. De Coalitionboard heeft het belang van een dergelijk initiatief onderschreven. Op basis daarvan zijn de kennisinstellingen met de Provincie Groningen en de input vanuit het bedrijfsleven aan de slag gegaan om een programma te ontwikkelen dat gericht is op kennisontwikkeling en product- en procesinnovaties, de vertaling van deze kennis naar onderwijsprogramma's en product/diensten-ontwikkelingen en concrete ondersteuning aan bedrijven/MKB.
Met de groeiende digitalisering neemt ook het aantal cyberaanvallen toe en worden de technieken die cybercriminelen gebruiken om in te breken in netwerken van de overheid en bedrijven geavanceerder en slimmer. Cybersecurity[1] wordt daarmee een belangrijk onderdeel van het digitale ecosysteem en een onderzoeksgebied waarvan de noodzaak steeds duidelijker wordt. Voor de groei van de digitale economie is het daarom essentieel om aandacht te geven aan de veiligheid en weerbaarheid van de samenleving en de bescherming van burgers en bedrijven. Maar de beschikbare expertise is schaars. Daarom moeten meer mensen worden opgeleid tot *cybersecurity* -experts en moeten de huidige professionals optimaal worden ingezet. Verder moet het onderzoek op dit gebied worden uitgebreid, van mbo tot universiteit en onderzoeksinstituten moet de hiermee opgedane kennis worden gebruikt om nieuwe producten en diensten te ontwikkelen, en zo onze (digitale) economie verder te stimuleren.
Niet alleen de bescherming van de digitale economie is belangrijk. Ook de bescherming van onze maatschappij, onze samenleving, is cruciaal. Dit betekent dat we ons ook moeten richten op onze burgers. Zij moeten zich zoveel mogelijk bewust worden van de gevaren van cybercriminaliteit. (Nieuwe digitale) producten, waar onze burgers gebruik van maken, moeten veilig zijn en hackers niet de gelegenheid geven hierop in te breken. En bij cybercriminaliteit moeten Justitie en Politie over de juiste kennis en middelen beschikken de criminelen snel op te sporen en te vervolgen. Kortom onze (digitale) economie en onze samenleving moet zoveel mogelijke cybersafe zijn.

1.2 Noodzaak en ambitie

De groeiende digitalisering biedt burgers en bedrijven kansen op welvaart, gemak, groei en ontwikkeling. Burgers adopteren nieuwe technologie om gemakkelijker te kunnen communiceren, te kunnen bankieren, op afstand hun thermostaat te bedienen of hun huis te beveiligen. Gevestigde en nieuwe bedrijven spelen in op de groeiende digitalisering. Er ontstaan veel jonge ICT en ICT gerelateerde bedrijven en “klassieke” bedrijven in belangrijke sectoren zoals *energie, logistiek en gezondheidszorg* transformeren onder invloed van digitalisering hun businessmodellen en bedrijfsprocessen, zodat ze concurrerend blijven. Het ministerie van EZK onderkent in de publicatie Nederland Digitaal[2] de economische kansen en het belang van digitalisering.
Zoals hierboven beschreven biedt digitalisering uitdagingen op het gebied van veiligheid. Een organisatie die haar IT-veiligheid niet op orde heeft kan in grote problemen komen. Criminele activiteiten spelen zich meer en meer af in het ‘cyber-domein’ en vormen een toenemende dreiging voor burgers en organisaties (bijlage 1 bevat een aantal voorbeelden).

[1] We gebruiken in dit document de term cybersecurity. We zien cybersecurity als middel om het uiteindelijke doel cybersafety te realiseren. De resultaten die het programma oplevert dragen uiteindelijk bij aan het ultieme doel, komen tot een cybersafe samenleving.
[2] Nederlandse digitaliseringsstrategie: Nederland Digitaal. Hier kan het. Hier gebeurt het. Ministerie van Economische Zaken en Klimaat (juni, 2018).

Veel systemen en apparaten zijn vaak niet of slecht beveiligd. In 2016 zorgde een DDoS-aanval[3] ervoor dat een groot deel van het Amerikaanse internet aan de oostkust platlag. Ook dringen steeds meer hackers "ons huis binnen". Ze gebruiken je IP-telefoon om te bellen of zetten je harde schijf met persoonlijke foto's en video's online. Naast toenemende aandacht voor software beveiligingen dringen zich ook vragen op als: wie kunt je bij schade aanspreken wanneer de dader een onbekende is of wanneer de aanval het gevolg is van een gecoördineerde 'cyber war'?

De digitale transformatie stelt de maatschappij voor veel (cybersecurity) vragen waar vaak nog geen antwoord op gevonden is. Het voorgestelde programma biedt dan ook oplossingen voor levende vragen vanuit de samenleving en het bedrijfsleven op het gebied van digitale veiligheid. De benodigde kennis is er nog niet of is niet toegankelijk voor de partijen die deze kennis nodig hebben. Veel bedrijven, met name in het MKB, hebben behoefte aan deze kennis en ondersteuning van cybersecurity professionals. Maar het aantal experts is beperkt en ook het aantal studenten met kennis van cybersecurity is op dit moment onvoldoende (zie ook bijlage 2). Daarnaast ontstaat er een grote vraag naar cybersecuritycursussen en –trainingen door de toenemende aandacht voor cybersecurity in bestaande functies. De sterke toename van het aantal producten dat via het internet met elkaar verbonden is heeft gevolgen voor de digitale veiligheid van onze inwoners, organisaties en bedrijven. De oprichting van een IOT-security test lab is cruciaal om de digitale weerbaarheid van onze samenleving te behouden en versterken.

Om **al deze uitdagingen** het hoofd te kunnen bieden is het noodzakelijk om samen te werken op het gebied van cybersecurity. Door gezamenlijk meer onderzoek te doen ontstaat er nieuwe kennis. Door de samenwerking tussen bedrijven, onderwijs- en kennisinstellingen en overheden te faciliteren, vindt er meer kennisdeling en –overdracht plaats, kunnen (cybersecurity) opleidingen worden ontwikkeld en meer studenten worden opgeleid tot professionals. Ook leidt nieuwe kennis tot nieuwe producten en diensten die door (Noord-Nederlandse MKB) bedrijven kunnen worden gebruikt en startups de kans bieden om te gaan ondernemen. Dit alles heeft tot gevolg dat bedrijven hun innovatiekracht en hun concurrentiepositie kunnen vergroten en dat de Noord-Nederlandse (digitale) economie blijvend kan groeien.

De ambitie van het Programma Cybersecurity Noord-Nederland is dan ook:
1. Versnellen en uitbreiden van onderzoek en kennisontwikkeling en dit nationaal en internationaal zichtbaar te laten zijn.
2. De weerbaarheid van (MKB) bedrijven te vergroten door middel van verbeterde kennis- en expertisedeling.
3. Te beschikken over uitmuntende faciliteiten voor het ontwikkelen van technologieën en diensten op het gebied van cybersecurity inclusief test faciliteiten en living labs.
4. Duizenden cybersecurity professionals te hebben opgeleid, zowel binnen het reguliere onderwijs als ook via het onderwijs voor professionals.
5. Te zorgen voor groei van het programma tijdens de uitvoering en continuïteit na de subsidiefase.

Groningen: de cybersecurity regio van Europa!
Het Ministerie van EZK heeft de Provincie Groningen nadrukkelijk als koploper benoemt op het gebied van digitale economie en -veiligheid. Deze positie willen we verder versterken. Door de geplande sterke

[3] Denial-of-service-aanvallen (DoS-aanvallen) en distributed-denial-of-service-aanvallen (DDoS-aanvallen) zijn pogingen om een computer, computernetwerk of dienst niet of moeilijker bereikbaar te maken voor de bedoelde klanten. Het verschil tussen een 'gewone' DoS-aanval en een distributed-DoS-aanval is dat in het laatste geval meerdere computers tegelijk de aanval op hun doelwit uitvoeren.

groei van het onderzoek, met daarbij een sterke focus op juridische en gedragswetenschappelijke aspecten, zal Noord-Nederland uiteindelijk kunnen uitgroeien tot **dé Cybersecurity regio van Europa.** Noord-Nederland kan zich daarmee profileren als dé regio in Europa waar de digitale kwantumsprong wel is gemaakt en rust op een sterk fundament, namelijk een goede cybersecurity infrastructuur. Een regio die bekend staat vanwege zijn excellente cybersecurity deskundigheid en waar nationaal- en internationaal gerenommeerde onderzoekers werken aan het thema cybersecurity. Daarnaast profiteert Noord-Nederland van een toename van het aantal aanbieders van cybersecurityproducten en -diensten en het aantal startups en zijn steeds meer wo-, hbo-, en mbo studenten met kennis van cybersecurity beschikbaar voor de arbeidsmarkt.
Analoog aan Eurosonic nodigt Noord-Nederland de toekomstige cybersecuritytalenten uit om in Groningen hun talenten te etaleren en verder te ontwikkelen. In 2023 is Noord-Nederland daarmee uitgegroeid tot de (digitaal) veiligste regio van Nederland. Noord-Nederland, met Groningen als dynamisch centrum, kan zich op dit gebied meten met andere regio's in Europa en de rest van de wereld. Veel organisaties zien het belang van het gezamenlijk uitvoeren van dit programma. Eurofins/Qbit, TNO, KPN, RDW, UMCG, Rabobank, Samenwerking Noord, NOO, NPAL, de Haan Advocaten en Notarissen, Groningen Seaports, Bedrijvenvereniging West, CGI, Sogeti en de kennisinstellingen RUG, Hanzehogeschool en Noorderpoort en Alfa-college hebben nu al toegezegd te willen deelnemen aan dit programma. Ook de organisaties VNO/NCW en MKB Noord en de Gemeente Groningen hebben hun sympathie uitgesproken. Bij het realiseren van de Groninger ambitie wordt ook verdere samenwerking gezocht met bedrijven, instituties en overheden in de Provincies Friesland en Drenthe. Juist door deze gezochte samenwerking hebben Politie Noord-Nederland en Justitie hun samenwerking op de initiatieven toegezegd.

1.3 Hoe wordt de ambitie gerealiseerd?

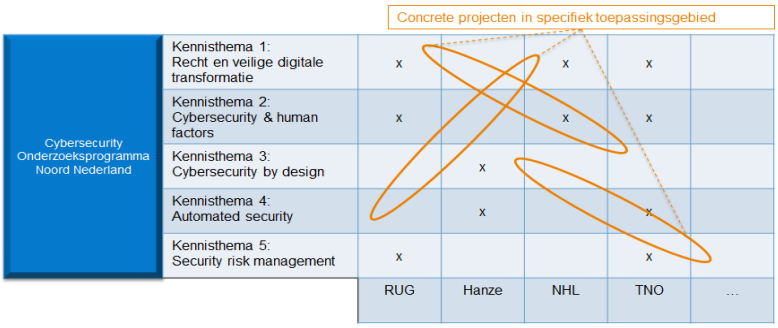
De in de vorige paragraaf genoemde 5 ambities worden hieronder verder uitgewerkt.

1. *Versnellen en uitbreiden van onderzoek en kennisontwikkeling*

Er is nieuwe kennis nodig om een leidende rol in cybersecurity te kunnen spelen. Niet alleen technische kennis, er is een grote behoefte aan juridische- en gedragswetenschappelijk kennis. Cybersecurity is bij uitstek een onderzoeksgebied dat multidisciplinair en op verschillende niveaus (WO, hbo, mbo) moet worden aangevlogen. Daarom is als onderdeel van dit programma een eerste aanzet gemaakt voor een **Noordelijke onderzoeksagenda cybersecurity**, waarin alle noordelijke onderzoeksinstituten (RUG, Hanzehogeschool, NHL, TNO, Noorderpoort, Friese Poort) samenwerken en waarbij ook nadrukkelijk de samenwerking met bedrijfsleven en overheden wordt gezocht. Ook nog niet aangesloten mbo-scholen in Noord-Nederland worden bij de agenda betrokken.
Bij de start van het programma "Cybersecurity Noord-Nederland" richt de RUG de leerstoel "**Recht en Veilige Digitale Transformatie"** in. De Hanzehogeschool breidt naar haar **lectoraten "Juridische aspecten van de arbeidsmarkt" en New Business & ICT** uit met het onderwerp cybersecurity. Noorderpoort en het Alfa-college stellen ten behoeve van het onderzoek gezamenlijk een **practor**[4] aan en TNO stelt zijn onderzoekexpertise op het gebied van cybersecurity beschikbaar.
Bij aanvang van het programma wordt de onderzoeksagenda verder uitwerkt tot een meerjarige "Cybersecurity onderzoeksagenda Noord-Nederland". De agenda kent meerdere kennisthema's (zie afbeelding hieronder). Aan elk kennisthema doen meerdere deelnemende onderzoekspartijen mee,

[4] een practor is een boegbeeld, inspirator en motor, verantwoordelijk voor kennisontwikkeling- verspreiding (in en extern) en –toepassing, praktijkgericht onderzoek en professionalisering van docenten in samenwerking met het bedrijfsleven

waarbij per thema één partijen de trekkersrol vervult (zie bijlage 3). In het programma worden projecten uitgevoerd, die meestal meerdere kennisthema's nodig heeft en waarbij meerdere partijen betrokken zijn. Een project kent altijd een specifiek toepassingsgebied, waarbij wordt aangesloten bij de toepassingsgebieden waarin Noord-Nederland sterk is, zoals autonoom vervoer, internet of things, energie, eHealth, fintech en 5G.



Figuur 2 Draft opzet Cybersecurity Onderzoeksprogramma Noord-Nederland

2. De weerbaarheid van (MKB) bedrijven te vergroten door kennis- en expertisedeling.

Bedrijven en organisaties, en met name het MKB, hebben behoefte aan ondersteuning door professionals en praktische tools om hun weerbaarheid op korte en lange termijn te vergroten. Het gaat hierbij niet alleen om technische tools maar juist ook om bewustwording, gedragsverandering en managementvaardigheden. Binnen dit programma worden deze tools ontwikkeld en geïmplementeerd. Belangrijke partner hiervoor is de Stichting Cybersecurity Centrum Noord-Nederland. Deze stichting regisseert voor Noord-Nederland het project Digital Trust Center (DTC), een initiatief van het Ministerie van EZK. Binnen het landelijke DTC zijn 6 samenwerkingsinitiatieven gestart, waaronder één in Noord-Nederland[5]. Het DTC-project organiseert roadshows (cyber to Go) waarmee bij groepen bedrijven cybersecurity onder de aandacht wordt gebracht. Daarnaast werkt het project aan een gecertificeerde security scan en – audit voor bedrijven en wordt een security pool, bestaande uit ca. 10 cybersecurity-deskundigen, gevormd. MKB-bedrijven kunnen gebruik maken van deze producten en diensten. Het DTC-project is waardevol, maar kleinschalig. Opname van dit project in het "Programma Cybersecurity Noord-Nederland" biedt de mogelijkheid tot grootschaligheid om zo meer en sneller MKB-bedrijven te kunnen helpen.

Een van de eerste activiteiten van het programma is dat er, ten behoeve van het MKB, in de **Werkplaats voor digitaal vakmanschap (Het Kasteel)** een supportfunctie wordt ingericht. Het MKB kan hier terecht met vragen op het gebied van cybersecurity. Ook worden op deze locatie (netwerk) bijeenkomsten en kleinere conferenties gehouden en worden er cursussen en trainingen verzorgd door o.a. de IT-Academy en worden er onderzoeksprojecten uitgevoerd. In de werkplaats voor digitaal vakmanschap gaan meerdere samenwerkingsverbanden zich vestigen, waaronder de NOO en Samenwerking Noord en wordt het een onderkomen voor bestaande en nieuwe startup's.

3. Het ontwikkelen van test faciliteiten

Zoals eerder beschreven is "Internet of Things (IoT)" een van de eerste toepassingsgebieden van het programma. Gevolg van de groei van de groei van het IoT is dat burgers en bedrijven meer last krijgen van criminele activiteiten (hacken, diefstal) en bedreigingen van hun veiligheid. Het is dus van groot belang dat (digitale) producten die op de markt komen veilig en beschermd zijn en dat deze uitvoerig getest zijn. Een van de eerste activiteiten van het programma is dat er, onder leiding van Qbit, **een**

[5] Deelnemers aan DTC project: Samenwerking Noord, Bedrijvenvereniging West, Connect.frl, De Friesland Zorgverzekeraar, Datadiensten Frysland, Stichting Cybersecurity Centrum Noord-Nederland (Groningen), Qbit, Stichting Cybersafety Noord-Nederland (Leeuwarden)

'virtueel IoT security test lab' opgezet in Groningen. In dit lab wordt de beveiliging van elektronica en IoT devices getest. Het lab wordt door Qbit in samenwerking met partners opgezet en kan ook door derden en op afstand (virtueel) worden gebruikt. In het lab wordt een zo representatief mogelijke test-omgeving gecreëerd waar zowel intrusive als non-intrusive kan worden getest. Het lab heeft aparte voorzieningen voor data, elektriciteit, water (en vooral de afvoer hiervan) en gas.
In 2022 werken ca 50 professionals in het test lab.

4. Via nieuwe kennis tot nieuwe producten en diensten en meer cybersecurity professionals
De uit de onderzoeksprojecten verkregen kennis is belangrijk voor de toekomst. Het draagt bij aan een veiligere digitale omgeving, zorgt voor nieuwe producten en diensten en het biedt startups de gelegenheid deze verworven kennis om te zetten in nieuwe innovaties. Ook wordt nieuwe kennis gebruikt voor het reguliere en commerciële opleidingen. Opleidingen die er weer voor zorgen dat een groot aantal deskundigen en/of studenten met kennis van cybersecurity op de markt verschijnen. Deskundigen waar bedrijven met smart op zitten te wachten. Het programma heeft een speciaal werkpakket ingericht gericht op **de valorisatie van resultaten.** Via werkwijzen en afspraken wordt ervoor gezorgd dat de ontwikkelde kennis en instrumenten beschikbaar wordt gesteld aan het werkveld en via trainingen en cursussen worden aangeboden via o.a. de IT Academy. Naar verwachting zullen na 4 jaar tenminste 1000 personen trainingen hebben gevolgd via ca. 10 nieuwe commerciële opleidingsprogramma's op het gebied van cybersecurity. Ook kan nieuwe kennis via startups leiden tot nieuw ondernemerschap. Valorisatie door ondernemerschap wordt ondersteund door het Marian van Os Centrum voor Ondernemerschap (HG) en het VentureLab (RUG). De verwachting is dat als gevolg van de valorisatie er uiteindelijk ca. 15 startups op het gebied van cybersecurity gaan ontstaan.
Nieuw verkregen kennis wordt uiteraard ook ingebracht in het reguliere WO, hbo en mbo-onderwijs. De verwachting is dat in 2022 ca. 4000-5000 studenten kennis hebben van cybersecurity. Onder kennis hebben verstaan we dat ze ca. 10 week een curriculum onderdeel hebben gevolg met als hoofdthema cybersecurity. De nieuwe kennis wordt ook beschikbaar gesteld aan initiatieven als ITurnIT (primair onderwijs) en andere initiatieven in het Voortgezet onderwijs, waardoor ook duizenden leerlingen van het basisonderwijs worden opgeleid in cybersafety.

5. Groei en continuïteit
Het is belangrijk dat de continuïteit van het programma tijdens en na afloop van de "subsidieperiode" geborgd wordt. Daarom worden er al snel projectactiviteiten gestart ter bevordering van deze contiguïteit.

- De stuurgroep (Steering Committee, SC) is verantwoordelijk voor de continuïteit van het programma. Er wordt een "rolling agenda" ontwikkeld waarmee het programma inspeelt op de actualiteit en waarmee partners op gecoördineerde wijze werken aan de financiering van vervolgprogramma's.
- De ontwikkelde kennis en instrumenten worden beschikbaar gesteld aan het werkveld via trainingen en cursussen die worden aangeboden via o.a. de IT Academy. In de IT Academy werken RUG, HG en Noorderpoort al samen bij het aanbieden van allerlei IT-gerelateerde vormen van post-initieel onderwijs. Deze vorm van onderwijs wordt aangeboden tegen kostendekkende tarieven.
- Valorisatie door ondernemerschap wordt gestimuleerd en ondersteund door de hiertoe ingerichte organen van de kennis en onderwijsinstellingen
- Ook ontwikkelde (MKB) tools kunnen tegen een vergoeding door het MBK worden afgenomen.
- De onderzoeksinstellingen borgen de continuïteit van het onderzoek via leerstoel, lectoraat en practoraat door eigen financiering of door het verwerven nationale- en/of internationale subsidiegelden.

- Het programma heeft de ambitie om cybersafety uit te breiden naar heel Noord-Nederland en hierbij actief samen te werken met andere Noord-Nederlandse initiatieven (Friesland en Drenthe). Het programma gaat daarbij een beroep op de actieve deelname van diverse (Noord-Nederlandse) bedrijven en instellingen.
- Het programma sluit daarnaast zoveel mogelijk aan bij andere landelijke initiatieven, waaronder het DTC-programma.
- Er wordt onderzocht of ontwikkelde tools en activiteiten potentie hebben om zelfstandig nieuwe financiële middelen te genereren. Initiatiefnemers worden hierbij ondersteund met faciliteiten en programma's van Hanzehogeschool, Noorderpoort, Alfa-college en RUG.

2 Doelstelling en resultaten

2.1 Doelstellingen

Kerndoel van het Programma Cybersecurity Noord-Nederland is het leveren van een bijdrage aan het realiseren van de veilige digitalisering in kleine en grote organisaties. Voor veel (MKB) bedrijven ligt hier nog een grote opgave. Daarom moet enerzijds het bewustzijn vergroot worden en moeten kennis en praktische oplossingen ontwikkeld en beschikbaar komen. Door een ambitieus programma uit te voeren breiden we bestaande initiatieven uit en bouwen we aan onderzoeksprojecten waarin bedrijven, kennisinstellingen en de overheid nauw samenwerken aan het ontwikkelen en implementeren van cybersecurityoplossingen met als uiteindelijk doel dat onze (Noord-Nederlandse) samenleving beter beschermd wordt tegen cyberaanvallen.

2.2 Resultaten

De afgelopen jaren is er in onze regio al veel gedaan op het gebied van cybersecurity. Een aantal feiten:

- Het Openbaar Ministerie parket Noord heeft samen met een aantal IT-bedrijven uit Noord-Nederland waaronder het security bedrijf Qbit de pilot Yoda uitgevoerd. Hierbij is jonge cyber criminelen een alternatieve strafafdoening aangeboden (https://nos.nl/artikel/2214949-yoda-proef-voor-jonge-hackers-krijgt-vervolg-in-rest-van-het-land.html).
- In 2017 is een cybercrisis oefening uitgevoerd (scenario digitale ramp), waarbij een grootschalige stroomuitval in grote delen van Delfzijl en Eemsmond werd gesimuleerd. Voor eind 2018-begin 2019 staan vergelijkbare oefeningen voor bestuurders en betrokken bedrijven gepland waarbij de vitale infrastructuur (drinkwater) centraal staat.
- IT Academy Noord-Nederland heeft samen met het bedrijf Qbit een omscholingsprogramma ontwikkeld en verzorgd voor security officers. Inmiddels zijn 10 cursisten van diverse organisaties gestart met de opleiding. Daarnaast hebben IT Academy Noord-Nederland en Qbit samen de leergang Functionaris Gegevensbescherming en Ethical Hacking ontwikkeld.
- Diverse aanbieders leveren commerciële diensten zoals: securityscans- en -audits.
- De Stichting Cyber Security Noord-Nederland is samen met een Friese Stichting gestart met het Digital Trust Center project. Bedrijvenvereniging WEST, een grote Stad Groningen georganiseerde bedrijvenvereniging met 400 leden, is één van de partners in deze Stichting.
- Tijdens diverse in Noord-Nederland georganiseerde congressen en themabijeenkomsten wordt regelmatig aandacht besteed aan het onderwerp cybersecurity.
- Kennisinstellingen en bedrijven doen onderzoek naar de beveiliging van IoT. Een voorbeelden zijn de onderzoeken van het bedrijf Qbit in samenwerking met hogescholen naar de beveiliging van de omvormers van zonnepanelen, slimme verlichting, internet radio enzovoort.
- RUG heeft expertise opgebouwd op het gebied van security en recht, security en gedrag, security en technologie, security en media.
- De Hanzehogeschool heeft security als expliciet thema in de majoren Software Engineering en Network & Security Engineering van haar hbo-ICT-bachelor opleiding.
- TNO heeft een sterke Cybersecurity onderzoeksgroep (afdeling Cyber Security & Robustness) waarin wordt samengewerkt met vele partijen, waaronder banken, defensie, ander overheden en Europese onderzoeksinstellingen en organisaties. Ongeveer 20 van de 45 onderzoekers van deze groep hebben standplaats Groningen.

Voortbordurend op bestaande initiatieven streeft het programma er naar het bestaande in beeld te brengen en nieuwe ontwikkelingen in gang te zetten. Dit levert na vier jaar de volgende resultaten op:

- Een netwerk van bedrijven, kennisinstellingen, aanbieders van (cybersecurity) IT, overheidsinstellingen die gezamenlijk participeren in cybersecurity-projecten;
- Een onderzoeksomgeving op het gebied van cybersecurity met nationale- en internationale bekendheid met daarbinnen een nieuwe leerstoelgroep (Rijksuniversiteit Groningen, Faculteit Rechtsgeleerdheid) waarin onderzoek wordt gedaan naar het juridisch kader voor een veilige digitale transformatie. Binnen deze onderzoeksomgeving heeft de Hanzehogeschool haar lectoraten “Juridische aspecten van de arbeidsmarkt” en New Business & ICT uitgebreid met het onderwerp cybersecurity en doen de mbo-instellingen Noorderpoort en Alfa-college via haar practoraat onderzoek op het gebied van cybersecurity.
- Ruim 500 nieuwe banen die gerelateerd zijn aan het domein cybersecurity bij: 1. bestaande bedrijven die bezig zijn met de digitale transitie, 2. aanbieders van (digitale) diensten en 3. startups;
- 15 start ups die actief zijn in het werkveld van de cybersecurity;
- Een ‘virtueel IoT security test lab’, waarin in 2022 ca. ca 50 professionals werken;
- 4000/5000 studenten mbo, hbo, WO die via reguliere opleidingsprogramma’s kennis hebben verkregen van cybersecurity;
- 10 nieuw ontwikkelde commerciële opleidingsprogramma’s;
- 10 miljoen uitgaven voor R&D op gebied van cybersecurity;
- Een speciaal ingerichte MKB-support faciliteit, ingericht in de Werkplaats voor Digitaal Vakmanschap (Noorderpoort), waar ca. 1000 MKB-organisaties per jaar van informatie worden voorzien en waarin diverse (netwerk) bijeenkomsten en (mini)conferenties worden gehouden;
- Via netwerkbijeenkomsten, (miniconferenties) worden honderden bedrijven geïnformeerd over het belang van cybersecurity en het de resultaten van het onderzoek.

2.3 Montitoring, rapportage en evaluatie

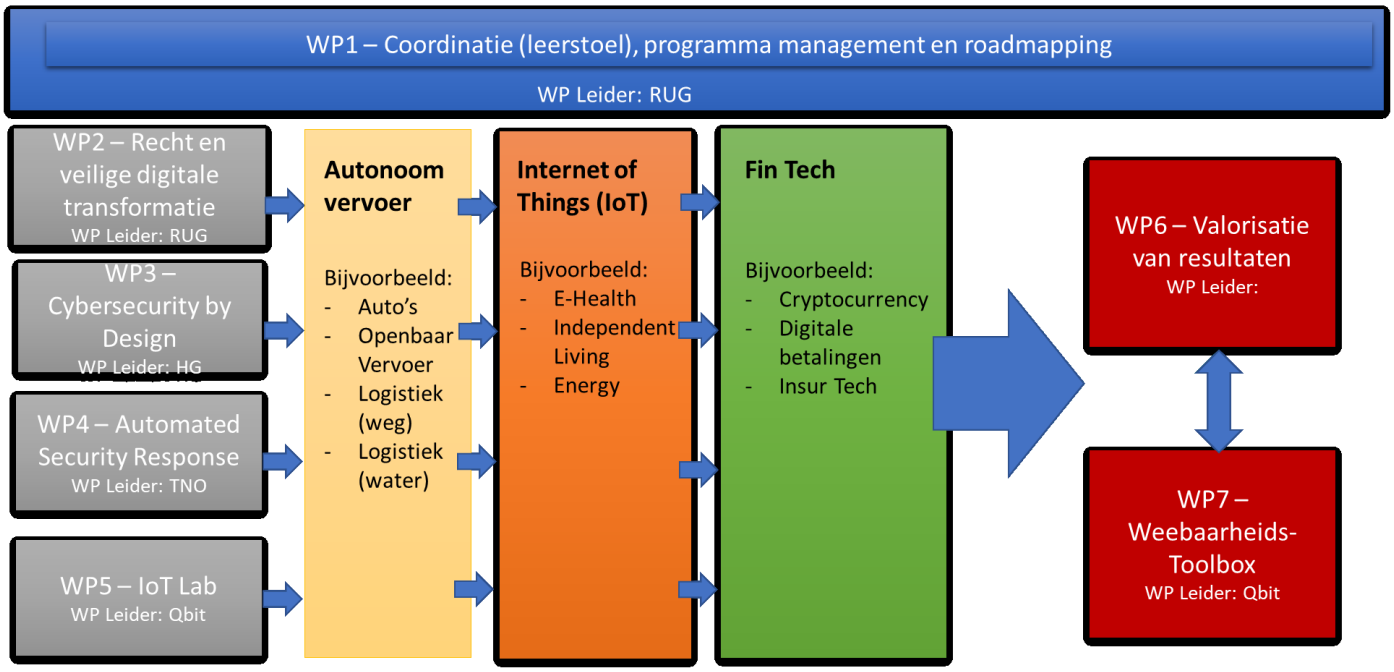
- Het monitoren, analyseren en evalueren van de voortgang van implementatie van het programma en de effectiviteit hiervan zal plaatsvinden op continue basis. Dit stelt het projectconsortium in het algemeen, en de SC in het bijzonder, in staat om tijdig bij te sturen, als dat nodig is.
- Jaarlijks zal het college van GS worden geïnformeerd over de voortgang van het project. Op basis van het REP-rapportageformulier zal een beknopte voortgangsrapportage over de uitvoering van het programma zal informerend worden voorgelegd aan Provinciale Staten volgens de reguliere P&C cyclus in het programma economie.
- De criteria op basis waarvan wordt gerapporteerd zijn overeenkomstig de gevraagde rapportageverplichting van de subsidievoorwaarden en de deliverables van het programma, zoals opgenomen onder hoofdstuk 3.9 Deliverables.
- De SC zal, op basis hiervan, waar nodig bijsturen. De SC legt verantwoording af aan de subsidieverstrekker. Zie voor de verdere consortiumorganisatie: 4.2 Organisatie en governance.

3 Programma & werkpakketten

Afgeleid van de eerste opzet van de onderzoeksagenda heeft het programma vooralsnog 4 thematische *werkpakketten* gedefinieerd. Ieder werkpakket staat onder leiding van een werkpakket leider.

Het programma Cybersecurity Noord-Nederland beoogt zowel weerbaarheid als onderzoek en innovatie te versnellen. Daarom zijn enerzijds pragmatische werkpakketten gedefinieerd, gericht op tools voor ondernemers en de korte termijn. Anderzijds zijn er kennisintensieve werkpakketten waarbij de nadruk ligt op het ontwikkelen van specifieke kennisgebieden en het onderscheidende vermogen van de regio. Door horizontale verbindingen te leggen tussen de werkpakketten vindt nieuwe kennis haar weg naar praktische toepassingen en innovaties in het bedrijfsleven. Onderstaande figuur toont de werkpakketten en de beoogde synergie-effecten

Het Programma Cybersecurity Noord-Nederland is weergegeven in het onderstaande Pert diagram:



Figuur 3 Pert diagram Programma Cybersecurity Noord-Nederland

Het programma richt zich vooralsnog op drie toepassingsgebieden: autonoom vervoer, 'Internet of Things' en fintech.

Waarom deze drie toepassingsgebieden?
Autonoom vervoer: Noord-Nederland is in sterke mate betrokken bij het testen en uitvoeren van trials van verschillende aspecten bij autonoom vervoer, bijv. autonoom openbaar vervoer op wegen (als onderdeel van de 5G trials), autonome auto's, autonome scheepvaart (met Groningen Seaports), Mobility Innovation Centre, etc. Terwijl veel van deze inspanningen zich richten op het voorbereiden van de technologie en infrastructuur zodat deze geschikt zijn voor gebruik in het publieke domein, zijn er nog vele uitdagingen op het gebied van cybersecurity die moeten worden opgelost. Onderzoek naar oplossingen is niet alleen van belang voor Noord-Nederland zelf, maar laat de verschillende betrokkenen die hieraan deelnemen een leidende rol spelen binnen de Europese en internationale ontwikkelingen op dit gebied.

Internet of Things: Naar verwachting zijn in 2020 ruim 20 miljard apparaten aangesloten op het Internet en dat aantal zal alleen nog maar toenemen. De uitdagingen ten aanzien van cybersecurity bij deze

apparaten zijn meervoudig. Burgers en bedrijven worden blootgesteld aan criminele activiteiten (hacken, diefstal) en bedreigingen van de veiligheid (niet intentionele gevaren), maar ook kan er sprake zijn van maatschappelijke verstoringen. Miljarden met elkaar verbonden apparaten…wat kunnen mensen doen om ervoor te zorgen dat hun informatie veilig blijft? Is iemand in staat om de koffieautomaat van een bedrijf te hacken en daardoor toegang te krijgen tot het gehele bedrijfsnetwerk? Een andere bron van zorgen waar veel bedrijven mee te maken krijgen is het probleem van de enorme hoeveelheid data die al deze apparaten produceren. Bedrijven moeten wegen vinden om deze data op een veilige manier op te slaan, bij te houden, te analyseren en te gebruiken (conform de daarvoor geldende wetgeving). Onderzoek naar manieren om het bewustzijn en de weerbaarheid van burgers en bedrijven te verhogen staat centraal bij een veilige digitale transitie op vele gebieden. In dit programma ligt de nadruk op de thema's Internet of Things (IoT), e-Health, onafhankelijk leven en smart energy. Deze thema's zullen de healthy ageing verder benadrukken en de overgang naar duurzame energie, thema's die beide reeds lange tijd speerpunten in Noord-Nederland zijn. Vanwege het belang van dit thema wordt binnen dit programma een test-omgeving gecreëerd waar producten kunnen worden getest op hun security.

Fintech: Fintech beschrijft het gebruik van technologie voor het leveren van financiële diensten aan bedrijven en consumenten. Dit kan in het bank-, verzekerings- en investeringswezen zijn – alles wat met financiën te maken heeft. Een rapport van 2017[6][1][1] toont aan dat meer dan 70% van de financiële instellingen cybersecurity als hun grootste bedreiging ziet bij de digitale innovatie binnen de financiële sector. Het is belangrijk om niet alleen samen te werken met financiële instellingen (waaronder het verzekeringswezen) om bedreigingen ten aanzien van cybersecurity aan te pakken, maar ook om te werken met fintech-bedrijven om diensten aan te kunnen bieden aan de financiële sector die reeds cyber secure zijn. Het begrijpen van de behoeften en vervolgens het opzetten van vaardigheidstrainingen om te voorzien in deze behoeften kan leiden tot verbeteringen en meer veiligheid voor fintech-bedrijven en consumenten.

[6][1] Simmons and Simmons Study (2017) https://www.information-age.com/cyber-security-biggest-barrier-financial-innovation-123465595/

3.1 Werkpakket 1: Coördinatie & Leerstoel

Werkpakket	1	**WP Leider**	RUG
WP titel	**Coördinatie, Leerstoel, programma management en roadmapping**		
Start maand	1	**Eind maand**	60

Doelen:

- Het opzetten van een specifieke leerstoel en leerstoelgroep.
- Het voeren van de coördinatie en het programma management conform het Programma Plan.
- Het opstellen van een Consortium Overeenkomst.
- Het waarborgen van de kwaliteit en voortgang van het programma en de programma doelen.
- Het administreren van het programma en de financiële administratie.
- Het rapporteren naar de subsidieverstrekker.
- Het organiseren van consortium bijeenkomsten en externe bijeenkomsten.
- Het uitvoeren van een roadmapping exercitie voor de sustainability van het programma Cybersecurity Noord-Nederland.
- Het verkennen van aanvullende subsidies/financieringsmogelijkheden.

Werkbeschrijving:

Taak 1.1: Het opzetten van een nieuwe leerstoel en leerstoelgroep
Lead partner: RUG
De Rijksuniversiteit Groningen en de Faculteit Rechtsgeleerdheid zien goede inhoudelijke mogelijkheden voor de ontwikkeling van een nieuwe leerstoelgroep, waarin onderzoek wordt gedaan naar het juridisch kader voor een veilige digitale transformatie. Deze leerstoel sluit aan bij binnen de Faculteit Rechtsgeleerdheid aanwezige expertise. De faculteit heeft een sterke positie als het gaat om onderzoek op het terrein van recht en technologie, rakend aan bijvoorbeeld privacy & data protection, digital security & governance, elektronisch contracteren en internet governance. Verschillende facultaire onderzoekers zijn op deze terreinen werkzaam (Groningen Centre for Technology Law (i.o.)).

Taak 1.2: Programma definitie
Lead partner: RUG
De programma coördinator zal:

1) Het Programma Plan opstellen in samenspraak met de consortium partners.
2) De Consortium Overeenkomst opstellen die de activiteiten van het consortium, de rollen en verplichtingen van de consortium partners, de besluitvormingsprocedures, de monitoring van de kwaliteitsborging en de conflictresolutie regelt.
3) De startup van het programma organiseren waarbij het consortium, vertegenwoordigd door de Steering Committee (SC), bijeenkomt.
4) De leden van de Externe Adviesraad selecteren en voordragen voor benoeming door Steering Committee (SC).

Taak 1.3: Coördinatie en programma management
Lead partner: RUG
De programma coördinator leidt de activiteiten van de Steering Committee (SC) inclusief o.a.:

1) Het regelmatig dissemineren van informatie m.b.t. het programma;
2) Het faciliteren van de samenwerking tussen de Steering Committee de WP-leiders en de programma partners;
3) Het organiseren van regelmatige gezamenlijke programma bijeenkomsten.

De Programmamanager ondersteunt de Programmacoördinator en ambassadeur met o.a. de volgende taken:
- Accountmanagement/relatiemanagement richting de deelnemende partners en bedrijven;
- Organisatie van de verschillende workshops;
- Steering Committee Meetings en disseminatie en valorisatie events;
- Organisatie van seminars voor stakeholders;
- Verbinden van het onderzoek met de praktijk zowel intern als ook extern;
- Actief verkennen van aanvullende subsidies/financieringsmogelijkheden.

Taak 1.4: Kwaliteitsborging en onderzoeksintegriteit
Lead partner: RUG
De programma coördinator monitort de voortgang van het programma middels het toetsen van de resultaten aan de hand van:
- Het Programma Plan;
- De Programma Planning (Gantt Chart);
- Interim en definitieve rapportages;
- Guidelines onderzoeksintegriteit gebaseerd op de bestaande protocollen binnen de betrokken partners.

Taak 1.5: Financiële administratie
Lead partner: RUG, Samenwerkingspartners: alle consortium partners
De programma coördinator bewaakt de subsidiegelden en de overall financiële rapportage verzorgen aan de subsidieverstrekker (op basis van de partner rapportages).

Taak 1.6: Stakeholder matrix
Lead partner: RUG/TNO, Samenwerkingspartners: alle consortium partners
Zoals in Taak 6.1 beschreven heeft het programma Cybersecurity Noord-Nederland een community van stakeholders. Om deze stakeholders en hun interesses en belangen goed in kaart te brengen heeft deze taak als doel om te komen tot een stakeholder matrix. Vanaf de start van het programma wordt een matrix van afzonderlijke stakeholders (bedrijfsleven, (lokale)overheden, MKB, kennis- en onderzoeksinstellingen en andere belanghebbenden) gecreëerd en verder uitgebreid. De valorisatie en disseminatie activiteiten van het programma richt zich op de relevante stakeholder groepen zoals gedefinieerd in de stakeholder matrix. Daarnaast kunnen stakeholder op basis van hun expertise, interesses en/of belangen aansluiten als samenwerkingspartners in het programma.

Taak 1.7: Road Map Cybersecurity Noord-Nederland
Lead partner: TNO/RUG, Samenwerkingspartners: HG, NP/AC (en stakeholders voortkomend uit Taak 1.7)
Een belangrijk doel van deze roadmapping exercitie is de sustainability van het programma Cybersecurity Noord-Nederland. Tijdens de looptijd van het programma wordt een strategie gedefinieerd die is gericht op het bepalen van de vereisten met betrekking tot de sustainability van het programma en de resultaten van het werk uitgevoerd binnen het programma. Het doel is om tools en adviezen te ontwikkelen (zie ook WP6 en WP7) die de partners en overige stakeholders faciliteren om de aanbevelingen en resultaten van het programma verder te implementeren.

Er is een begin gemaakt met een Noordelijke onderzoeksagenda (zie bijlage 3). In deze taak wordt deze agenda verder uitgekristalliseerd en wordt een Road Map Cybersecurity Noord-Nederland opgesteld die jaarlijks wordt getoetst en daar waar nodig bijgesteld. De Road Map Cybersecurity Noord-Nederland bevat de inhoudelijk onderzoeksvragen, relevant voor Noord-Nederland, die kunnen worden opgepakt en per onderzoeksvraag de

partijen die bij het onderzoek betrokken moeten worden. De agenda moet passen in de ontwikkelingen zowel globaal als in Nederland. Bovendien moet het in lijn zijn met de NCSRA en aansluiten bij de sterke punten die er zijn in Noord-Nederland. De onderzoeksonderwerpen zullen als focus cybersecurity en cybersafety hebben, maar kunnen zich wel op verschillende expertises richten zoals techniek, Human Factors, Artificial Intelligence, Machine learning, Big data, juridische kaders, regelgeving etc.
Resultaten **D1.1 – Rapport m.b.t. het opzetten van de leerstoel en leerstoelgroep (M48)** **D1.2 – Programma Plan (M6)** **D1.3 – Consortium Overeenkomst (M6)** **D1.4 – Stakeholder Matrix (12)** **D1.5 – Cybersecurity onderzoeksagenda en roadmap Noord-Nederland (M60)**

3.2 Werkpakket 2: Recht en veilige digitale transformatie

Werkpakket	2	**WP Leider**	RUG
WP titel	**Recht en vellige digitale transformatie**		
Start maand	7	**Eind maand**	60

Doelen:

- De juridische issues analyseren die een veilige digitale transformatie in de volgende drie thema's omringen: Autonoom Vervoer, Internet of Things, fintech.
- Juridische oplossingen voor de gedefinieerde issues aanbevelen

Werkbeschrijving:

Taak 2.1a: In de autonoom vervoer sectie: het onderzoeken van nieuwe bestuursmodellen voor het verlenen van kentekens voor autonome voertuigen.

Lead partner: RUG, Samenwerkingspartners: (RDW)

In het afgelopen decennium zijn er grote veranderingen en ontwikkelingen geweest op het gebied van technologieën die autonoom vervoer mogelijk maken. Er is daadwerkelijk een verschuiving geweest van de initiële onderzoeksfasen op het gebied van geautomatiseerde voertuigen naar 'Proof of Concept' naar meer en meer de piloting van autonome voertuigen op openbare wegen en ruimtes. Deze technische ontwikkelingen moeten vergezeld worden door juridische kaders die zorgdragen voor de veiligheid van de openbare ruimte waarbinnen deze autonome voertuigen gebruikt worden, de gebruikers van de autonome voertuigen en de personen in en de omgeving waarin deze autonome voertuigen zich bewegen. Tot nu toe voorzien de juridische kaders met name in specifieke regelgeving voor de autoriteiten die zich bezighouden met de kentekens en vergunningen voor voertuigen, zodat deze op de openbare weg gebruikt kunnen worden en voor autoriteiten die de bestuurders het recht geven om een voertuig op de openbare weg te besturen. Deze traditionele bestuursmodellen moeten aangepast worden door de technologische ontwikkelingen. Dit niet alleen vanwege de realiteit dat er geen 'bestuurder' meer in de autonome voertuigen zal zijn, maar ook omdat de certificering voor veiligheid en bescherming van de inzittenden veel lastiger zal zijn. Nieuwe bestuursmodellen zijn dus noodzakelijk.

Dit PhD onderzoek zal, gebruik makend van het hedendaagse onderzoek op het gebied van aansprakelijkheidsproblematiek in het autonoom vervoer, de verschillende bestuursmodellen onderzoeken die ontwikkeld kunnen worden voor de regulering en afgifte van kentekens voor autonome voertuigen. Dit onderzoek zal worden uitgevoerd in nauwe samenwerking met de Rijksdienst Wegverkeer (RDW) en andere

partijen die betrokken zijn bij het autonome voertuigen ecosysteem waaronder verzekeringsmaatschappijen, (auto)fabrikanten en onderzoeksinstituten die de technologieën die worden gebruikt in deze voertuigen onderzoeken en ontwikkelen.

Taak 2.1b: In de autonoom vervoer sectie: Autonome voertuigen als een dienst: het onderzoeken van de juridische issues met betrekking tot het creëren van een nieuwe circulaire economie.
Lead partner: RUG, Samenwerkingspartners: (RDW)
Velen voorspellen dat het vervangen van een 'bestuurder' of 'piloot' van een autonoom voertuig door autonome technologie een verandering teweeg zal brengen in de eigendomsconstructies van autonome voertuigen. Van een constructie waarin fabrikanten (eventueel via dealers) een voertuig verkopen aan eindgebruikers of leasemaatschappijen tot een constructie waarin een mobiliteitsbedrijf haar mobiliteitsdiensten aanbiedt. Deze verandering in het commerciële model kan ook leiden tot andere veranderingen in het huidige begrip 'transport'. Het adopteren van een circulaire economie voor mobiliteitsdiensten kan verder worden onderzocht als een oplossing voor een meer duurzaam groeimodel in de transportsector.
Dit PhD onderzoek heeft als doel om de juridische problematiek die wordt ondervonden in het versterken van de circulaire economie beter te begrijpen. Het zal zich primair richten op de noodzaak voor een (juridisch) veilige transitie naar mobiliteit als een dienst waarbij de duurzaamheid van de middelen en veiligheid in acht worden genomen.

Taak 2.2a: In de Internet of Things sectie: Het onderzoeken van de overlap in strafrechtelijke en civielrechtelijke verantwoordelijkheden in de context van het Internet of Things.
Lead partner: RUG
De meeste 'slimme' (en minder 'slimme') huizen en kantoren worden in toenemende mate gevuld met verschillende gadgets die door hun connectie met een groter netwerk (waaronder het Internet) kwetsbaar kunnen zijn voor ongeautoriseerde inbreuk of misbruik voor illegale doeleinden. Daar waar cybersecurity experts 'veilig' gebruik adviseren om de kansen voor inbreuk te verminderen, volgen de meeste 'eigenaren' of 'gebruikers' van deze gadgets de adviezen niet op. Of ondanks het feit dat er maatregelen worden genomen om inbreuk te voorkomen, vind de inbreuk en de daarbij behorende schadelijke activiteiten nog steeds plaats.

Welke juridische maatregelen kunnen worden genomen om het illegale gebruik van IoT gadgets te voorkomen? Dit PhD onderzoek kijkt naar hoever de civielrechtelijke en strafrechtelijke aansprakelijkheid van 'eigenaars' en 'gebruikers' van IoT devices reikt. Het zal onderzoeken in hoeverre welke regelgeving (m.b.t. aansprakelijkheid) van toepassing is en gebruikt kan worden als een tool om het gebruik van veiligere 'Slimme' omgevingen te promoten.

Taak 2.2b: In de Internet of Things sectie: Het onderzoeken van de toepasbaarheid van het juridische kader voor de certificering van medische apparatuur voor IoT devices in e-health.
Lead partner: RUG, Samenwerkingspartners: HG, Qbit, (UMCG)
Het garanderen van de veiligheid van medische apparatuur die gebruikt wordt in de zorg is al lange tijd een aandachtspunt van zorginstellingen. In Nederland en de Europese Unie bestaat er al lange tijd regelgeving m.b.t. de certificering van medische apparatuur. Deze regelgeving is ook van toepassing op software die wordt gebruikt in de diagnose, preventie en behandeling van medische aandoeningen. Dit onderzoek richt zich op het analyseren of het huidige juridische kader nog goed genoeg is om de veiligheid van de patiënt te garanderen bij het gebruik van IoT e-health toepassingen in de gezondheidszorg.

Taak 2.3a: In de FinTech sectie: Zorgen voor samenhang in de wettelijke kaders: door het onderzoeken van de issues met betrekking tot het gebrek aan samenhang in de wettelijke kaders gecreëerd door de nieuwe

regelgeving voor gegevensbescherming i.h.b. in vergelijking met andere bestaande verplichtingen in de financiële sector.

Lead partner: RUG

Digitalisering en het toenemende gebruik van data leiden toto nieuwe wetgeving. Sommige van deze wetgeving brengen 'radicale' veranderingen in aanpak die soms totaal tegenstrijdig zijn met de doelen van reeds bestaande wetgeving. Deze conflicterende doelen kunnen een belangrijke impact hebben om de samenhang van nationale wettelijke kaders. Een voorbeeld hiervan (een van de vele) is naar voren gekomen als gevolg van de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) in mei 2018. Deze wetgeving is geïntroduceerd om het gebruik van persoonsgegevens dat exponentieel gegroeid is door het gebruik van gedigitaliseerde diensten beter te beschermen. Het niet voldoen aan deze regelgeving kan tot hoge boetes voor organisaties leiden. Echter, een aantal van deze regels gaan in tegen de regels die een aantal organisaties verplicht zijn te volgen. Bijvoorbeeld, banken en financiële instellingen zijn verplicht om conform de anti-witwaswetgeving een uitgebreide administratie bij te houden. De eisen m.b.t. deze administratieverplichting is mogelijk in strijd met de regels in de AVG en daarmee wordt een zekere onzekerheid gecreëerd voor financiële instellingen m.b.t. de samenhang in de wettelijke kaders die zij moeten volgen. Dit PhD onderzoek richt zich op de mogelijke oorzaken van het gebrek aan samenhang en haar impact op de nationale wettelijke kaders.

Taak 2.3b: In de FinTech sectie: Worden consumenten adequaat beschermd in de nieuwe digitale FinTech omgevingen?

Lead partner: RUG

Consumenten worden geconfronteerd met het gebruik van nieuwe technologieën in de financiële sector. Ontwikkelingen zoals het gebruik van 'virtual currencies', 'crowdfunding', geautomatiseerde (robo-) adviesgesprekken en het gebruik van consumenten data op innovatieve wijze maken de consumenten kwetsbaar voor cyberfraude. Tot op heden bestaat er geen een alomvattende aanpak gericht op het bereiken van een regelgevend- en toezichtskader dat de rechten van de consument beschermt.
Dit PhD onderzoek brengt de bestaande wettelijke kaders in kaart en identificeert de hiaten in de wetgeving waardoor consumenten niet beschermd worden zowel in de nationale context als ook in een grensoverschrijdende context. Dit onderzoek zal de mogelijke aanpassingen in het regelgevend- en toezichtkamer identificeren voor een adequate consumentenbescherming te bewerkstelligen.

Taak 2.4: Het ontwikkelen van onderwijsprogramma's voor professionals in de drie hiervoor beschreven secties.

Lead partner: RUG

Professionals worden in hun dagelijks werk steeds vaker geconfronteerd met issues direct of indirect gerelateerd aan de digitale transformatie. Bestaande vakkennis is vaak niet toereikend om goed met deze issues om te kunnen gaan en specifieke training en opleidingen ontbreken vaak. Deze taak richt zich op het ontwikkelen van onderwijsprogramma's voor professionals op het gebied van veilige digitale transformatie met een specifieke focus op de thema's: Autonoom Vervoer, Internet of Things, fintech.

Resultaten

D2.1 - Workshop on governance models for automated vehicles (M24)
D2.2 – Onderzoeksrapport Research on new goverance models for the licensing of automated vehicles (M54)
D2.3 – Onderzoeksrapport Research on Autonomous vehicles as a service: exploring the legal challenges in creating a new circular economy (M54)

D2.4 – Workshop on legal issues in IoT security and safety (M30)
D2.5 – Onderzoeksrapport Research on the overlap in criminal and civil responsibilities in the context of internet of things (M54)

D2.6 – Onderzoeksrapport Research on the applicability of the legal framework for the certification of medical devices for IoT devices in e-health (M54) **D2.7 – Workshop on legal issues in Fintech cybersecurity and safety (M36)** **D2.8 – Onderzoeksrapport Research on ensuring coherence of legal frameworks (M54)** **D2.9 – Onderzoeksrapport Research on consumer protection in new fintech digital environments (M54)**

3.3 Werkpakket 3: Cybersecurity by design

Werkpakket	3	**WP Leider**	HG
WP titel	**Cybersecurity by Design**		
Start maand	7	**Eind maand**	54

Doelen:

- Ontwikkeling handreikingen voor methode safety by design.
- Omschrijven praktische adviezen m.b.t. toegankelijkheid medische informatie in afzonderlijke ehealth producten of diensten of systemen
- Ontwikkelen MKB-gereedschappen voor detecteren en inperken van digitale kwetsbaarheden

Werkbeschrijving:

Task 3.1: ICT MKB Security by design
Lead partner: HG, Samenwerkingspartners: TNO, RUG
De software die wordt ontwikkeld door ICT-bedrijven wordt ontwikkeld in een constante ratrace met de ontwikkelingen in enerzijds cybercriminaliteit en anderzijds wet & regelgeving. Voor het MKB is dit niet of nauwelijks zelfstandig bij te houden. Hoe plaats en borg je dit in het software ontwikkelproces? Hoe realiseer je effectieve monitoring hiervan in de ontwikkelstraat? Hoe doe je dit op een manier die ook haalbaar is voor de (kleine) MKB'er? Het programma adviseert deze bedrijven in een wisselwerking tussen juridische en technische perspectieven over de te gebruiken handvatten onder de noemer 'safety by design'.

Task 3.2: In IoT: eHealth CyberSafety
Lead partner: HG, Samenwerkingspartners: RUG, (UMCG)
Het Noorden heeft ingezet in diverse ehealth ontwikkelingen (bv PGO, Regiegroep PCH, dHealthLab). Bij alle producten, diensten en systemen die binnen die context worden ontwikkeld is Cybersecurity een meer dan gemiddeld belangrijk thema vanwege de vertrouwelijkheid van medische gegevens. Binnen deze activiteit wordt met inachtneming van de specifieke wet & regelgeving in het health domein gewerkt aan adequate vormen van toegankelijkheid van medische informatie.

Taak 3.3: MKB Digitale weerbaarheid
Lead partner: HG, Samenwerkingspartners: nader invullen
Elk bedrijf krijgt in meer of mindere – maar zeker in toenemende – mate te maken met digitale middelen voor het doen van business. Daarmee worden die bedrijven ook steeds kwetsbaarder, enerzijds door onoordeelkundig gebruik van digitale middelen, anderzijds door opzettelijk toegang en misbruik door derden. Met een groep van 5 MKB-ers worden tools geselecteerd, getest en evt. aangepast voor het inventariseren en inperken van kwetsbaarheden. Vervolgens worden die case-bie-case – op verzoek van andere MKB'ers toegepast en eventueel bijgesteld.

Resultaten

D3.1 – Op MKB toegespitste handreikingen voor 'safety by design' (M36) 5+ praktische adviezen voor MKB ICT ontwikkelaars.
D3.2 – 5+ Praktische adviezen m.b.t. toegankelijkheid medische informatie in afzonderlijke ehealth producten of diensten of systemen (M48)
D3.3 – Geteste en op MKB toegespitste gereedschappen voor detecteren en inperken van digitale kwetsbaarheden:

- **Als gevolg van onoordeelkundig handelen**
- **Als gevolg van opzettelijk misbruik**

5+ praktische adviezen voor afzonderlijke MKB'ers

3.4 Werkpakket 4: Automated Security Response

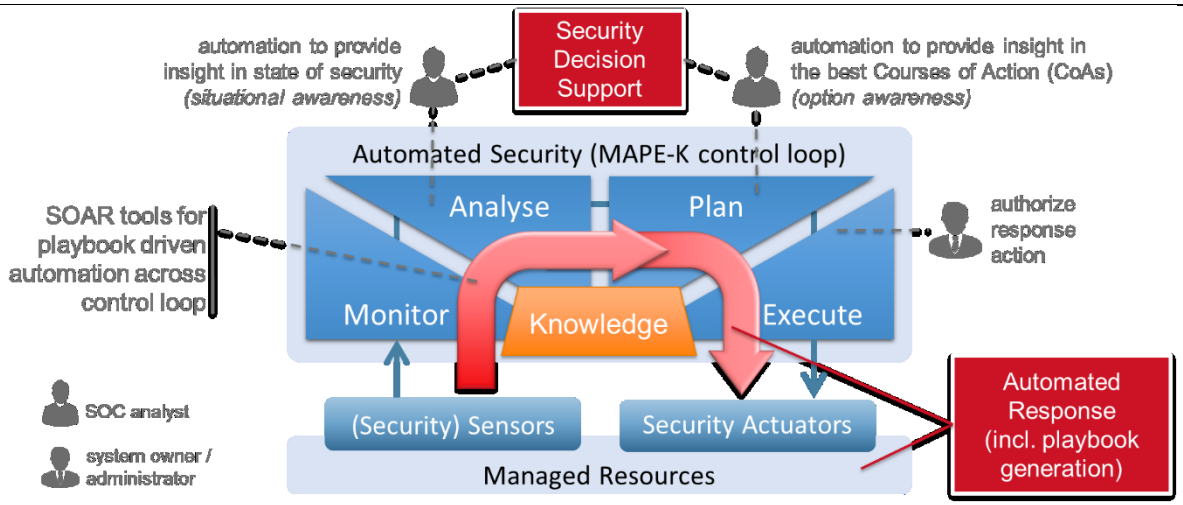
Werkpakket	4	**WP Leider**	TNO
WP titel	**Automated Security Response**		
Start maand	7	**End maand**	54

Doelen:
Met nieuwe innovaties de security operators ondersteunen bij het reageren en oplossen van security incidenten. Enerzijds door ondersteunende tools te ontwikkelen, anderzijds door een deel van het werk van de security operator te automatiseren

Werkbeschrijving:

N.B.: onderstaande taken zijn gedefinieerd naar de huidige stand van zaken. Taak 4.1 (met D4.1 t/m D4.3) zal in 2019 worden uitgevoerd, bijstellen van de planning en de definitie van eventuele nieuwe taken zal jaarlijks plaatsvinden.

Taak 4.1: Automated Security
Lead partner: TNO, Samenwerkingspartners: RUG, HG, (NHL, bedrijven)
Het is voor security analisten een steeds grotere uitdaging om cyber dreigingen en aanvallen tijdig te pareren. Belangrijke reden hiervoor is dat cyber aanvallen in toenemende mate geautomatiseerd worden uitgevoerd. Menselijk handelen volstaat hierdoor niet meer om aanvallen snel en effectief te beheersen. Daar komt nog eens bij dat er een structureel tekort is aan gekwalificeerde cybersecurityspecialisten. Om de snelheid van detectie en response te matchen met die van een cyberaanval is een "game changer" nodig. TNO ziet automatisering van security als deze "game changer" en werkt aan technologieën voor geautomatiseerde analyse en mitigatie van digitale aanvallen op ICT-infrastructuur.



Figuur 1. Visie op automatisering van security

Taak 4.1 heeft de volgende doelstellingen:

A. Onderzoek naar en ontwikkeling van de proof-of-concept Security Decision Support tool. In het bijzonder:
- Feedback vergaren van stakeholders/eindgebruikers (i.e. SOC analist) via een workshop over de inzet van dergelijke tools. De feedback zal gebruikt worden voor o.a. user-interface ontwikkeling en ontwikkelen van vervolgprojecten.
- Uitbreiden en verbeteren van attack analyse component van de proof-of-concept. In het bijzonder onderzoeken of en hoe de MITRE ATT&CK matrix kan worden gebruik voor modelleren van attack steps.
- Tools ontwikkelen voor automatisch generen van ICT Infrastructuur modellen.

B. Onderzoek naar en toepassing van Automated Response met Security Orchestration. De focus zal liggen op kennis op bouwen over:
  - automatische response bij administratieve domein overschrijdingen;
  - dynamische generatie van Incident Response (IR) Playbooks met behulp van AI.

In deze taak worden de volgende activiteiten ontplooid:

Activiteit A1: SOC user interaction & use cases
Deze activiteit is gericht op vergaren van feedback van stakeholders en kennisontwikkeling over toepassing van ADG gebaseerde in de use cases. Deze activiteit zal bestaan uit deskresearch en workshops met beoogde eindgebruikers.

Activiteit A2: Proof-of-concept development
In deze activiteit zal verder ontwikkelingen worden uitgevoerd aan de proof-of-concept Security Decision Support. Er zal gebruik gemaakt worden van stagiaires. Gebruik van de resultaten uit activiteit A1 is hierbij van groot belang.

Activiteit B1: Automated Response multi-administrative domain
In deze activiteit zal deskresearch gedaan worden naar technische en organisatorisch uitdagingen bij automatisch response. Hiervoor zal ook contact gezocht worden met stakeholders. Ook zullen oplossingsrichtingen worden verkend.

Activiteit B2: Automated playbook generation
In deze activiteit wordt onderzoek gedaan naar automatisch generatie van playbooks voor Automated Response. Er wordt een scrum-achtige aanpak gebruikt. Elke iteratie (3 maanden) levert tussenresultaten. Activiteiten zullen gebruik maken van TNO Research Cloud en Splunk Phantom platform (SAOR-platform).

Taak 4.2: Automated vulnerability discovery, patch generation and deployment
Lead partner: TNO, Samenwerkingspartners: RUG, HG, (bedrijven)
In deze taak wordt gewerkt aan methoden om automatisch kwetsbaarheden te ontdekken en vervolgens kwetsbaarheden op te lossen (bijvoorbeeld middels patching). Hiertoe wordt gebruik gemaakt van tools die infrastructuur kunnen modelleren.

Resultaten

D4.1 – White Paper on Automated Security

D4.2 – Proof-of-concept van Security Decision Support

D4.3 – Proof-of-concept van Automated Response

D4.4 – Proof-of-concept van automated vulnerability discovery
D4.5 – Proof of concept van automated patch generation and deployment

3.5 Werkpakket 5: IoT Security Testlab

Werkpakket	5	**WP Leider**	Qbit
WP titel	IoT Security testlab		
Start maand	1	**Eind maand**	54

Doelen: Qbit ontwikkelt en realiseert in 2019 een IoT security test lab. Hierbij gaat het om de infrastructuur, de methoden en technieken (software en hardware) waarmee IoT apparaten structureel kunnen worden getest en onderzocht. Het lab levert vanaf de start in 2019 vijf directe arbeidsplaatsen op. Het doel is dat het lab in 2022 in totaal vijftig arbeidsplaatsen oplevert en leidt tot tenminste tien nieuwe bedrijven. Dit wordt gedaan door samen met kennispartners studenten op te leiden, structureel onderzoek te laten doen om de beveiliging van IoT apparaten slim en innovatief te verbeteren. Hiertoe wordt, in samenwerking met Hanzehogeschool, Noorderpoort Alfa-college ook een gecombineerd lectoraat – practoraat opzet.

Taak 5.1: IoT Security testlab
Lead partner: Qbit, Samenwerkingspartners: RUG, HG, NP/AC, TNO
Netwerkpartners: Consumentenbond, EnTrance

Qbit ontwikkelt een (virtueel) IoT security test lab dat zich voornamelijk richt op de het structureel testen en onderzoeken van de beveiliging van slimme consumentenelektronica. Het lab wordt in samenwerking met partners opgezet en kan ook door derden en op afstand (virtueel) worden gebruikt. In het lab wordt een zo representatief mogelijke test-omgeving gecreëerd (huiskamer, badkamer, keuken, bijkeuken) waar zoveel *intrusive* als *non-intrusive* kan worden getest. Virtueel betekent dat slimme apparaten door een leverancier via een portal met het lab kunnen worden verbonden zodat vanuit het lab in Groningen, zoveel mogelijk

geautomatiseerd, een aantal basistest kan worden uitgevoerd zonder dat de apparaten worden opgestuurd dan wel verscheept naar het lab. Daarnaast kunnen medewerkers van het lab en onderzoekers zoveel mogelijk van de faciliteiten van het lab op afstand gebruiken. Het lab test en onderzoekt de beveiliging verschillende onderdelen van een IoT-apparaat: fysiek object met een voeding (bekabeld/batterij), verwerkingseenheid, niet-vluchtig geheugen, connectiviteit (bedraad/draadloos), sensoren en de software waarmee het apparaat wordt beheerd. Vooral voor het testen van de hardware en het inzetten van technieken zoals *fuzzing* en *reverse engineering*[7] wordt specifieke apparatuur aangeschaft en/of ontwikkeld.

Studenten, docenten en onderzoekers (WO, hbo en mbo) werken in het lab samen aan het verbeteren van de security en privacy van IoT in de zorg, energie, mobiliteit, leefbaarheid en landbouw. Hierbij richt het WO (Rijksuniversiteit Groningen) op fundamenteel onderzoek, hbo (Hanzehogeschool Groningen) zich op toegepast onderzoek en ontwerp (security by design) en het mbo (Alfa- college en Noorderpoortcollege) zich op dataverzamelingen en toepassing van kennis in de praktijk. Daarnaast kan het lab door andere bedrijven en kennisinstellingen worden gebruikt om de beveiliging van consumentenelektronica te testen en te onderzoeken.

Resultaten

D5.1: IoT security testlab (infrastructuur, de methoden en technieken).
D5.2: Gecombineerd lectoraat – practoraat.
D5.3: 50 arbeidsplaatsen (bij Qbit en andere organisaties).
D5.4: 10 nieuwe bedrijven (starts-ups).

3.6 Werkpakket 6: Valorisatie van Resultaten

Werkpakket	6	**WP Leider**	RUG/Hanze/TNO
WP titel	**Valorisatie van Resultaten**		
Start maand	1	**Eind maand**	60

Doelen

- Het valoriseren en dissemineren van de resultaten van het programma;
- Het ontwikkelen van tools en adviezen op het gebied van beleid, onderwijs en kennisoverdracht voor de betrokken stakeholders vanuit de kennis die ontwikkeld is in de werkpakketten 2, 3 en 4;
- Het onderhouden van relaties met interne en externe stakeholders.

Taak 6.1 Valorisatie en disseminatie
Lead partner: RUG, Samenwerkingspartners: alle consortium partners
Deze taak is van strategisch belang omdat het alle andere activiteiten ondersteunt en het de communicatie van de programma resultaten binnen een grotere community van stakeholders faciliteert.
Bij de uitvoering van deze taak wordt optimaal gebruik gemaakt van bestaande organisaties, samenwerkingsverbanden en platforms op het gebied van ondernemerschap, innovatie en professional education. Valorisatie door ondernemerschap wordt ondersteund door het Marian van Os Centrum voor Ondernemerschap (HG), VentureLab (RUG), en de RUG Holding.
Innovatie wordt ondersteund door de werkplaats voor digitaal vakmanschap (Het Kasteel NP), de Digital Society Hub (HG) en het Groningen Digital Business Center (RUG).

[7] Fuzz-testen of fuzzing is een techniek die de software van een apparaat test. De techniek dient om programmeerfouten of beveiligingsgaten te vinden door willekeurige data, genaamd fuzz, in het systeem te sturen in een poging om het te doen crashen. Reverse engineering is het onderzoeken van een product om daaruit af te leiden wat de eisen zijn waaraan het product probeert te voldoen, of om de precieze interne werking ervan te achterhalen.

De ontwikkelde kennis en instrumenten worden beschikbaar gesteld aan het werkveld via trainingen en cursussen die worden aangeboden via de IT Academy. Het onderwijs wordt aangeboden tegen kostendekkende tarieven.
Zoals beschreven in sectie 5 van dit document worden verschillende communicatie en disseminatie mechanismen gebruikt voor de verschillende stakeholders van het programma. Deze mechanismen worden beschreven in een communicatie en disseminatie strategie. Een initiële opzet van deze communicatie en disseminatie strategie is in sectie 5 weergegeven.

Deliverables
D6.1: **– Rapport m.b.t. valorisatie activiteiten plus aanpak (M60)**

Taak 6.2: Ontwikkeling van Smart Instruments
Lead partner: TNO/RUG Samenwerkingspartners: alle partners
Een initieel ontwerp van **Smart Instruments** wordt ontwikkeld gedurende het programma. Met behulp van de stakeholder analyse (Taak 1.7) en roadmapping exercitie (Taak 1.8) in WP1 wordt gedefinieerd welke bronnen van informatie worden gebruikt voor het komen tot **Smart Instruments** voor de verschillende stakeholder groepen.

Taak 6.3: Creëren van Smart Instruments voor Cybersecurity Stakeholders
Lead partner: TNO/RUG, Samenwerkingspartners: all partners
De tools en adviezen ontwikkeld binnen Werkpakket 2-5 vormen de basis voor **Smart Instruments**. Op basis van tussentijdse resultaten uit WP2-5 worden gesynthetiseerde resultaten opgesteld die getoetst worden met de relevante stakeholders alvorens deze tot **Smart Instruments** worden verwerkt. De aanbevelingen voor stakeholders op alle niveaus bestaan o.a. uit de implementatie en/of verbetering van beleid en beleidsadviezen, maatregelen op het gebied van onderwijs en een roadmap voor de verdere kennisoverdracht.

Taak 6.4: Smart Instruments 'Roadshow'
Lead partner: RUG, Samenwerkingspartners: alle partners
In samenwerking met WP1 worden verschillende stakeholder meetings georganiseerd in Noord-Nederland (en indien relevant ook buiten de regio) om de resultaten van het programma Cybersecurity Noord-Nederland en de **Smart Instruments** te dissemineren.

Deliverables
D6.2 – Smart Instruments design
D6.3 – Smart Instruments voor Cybersecurity Stakeholders

Taak 6.5: Ambassadeursrol/Ambassadeurschap
Lead partner: Stuurgroep (SC)
Samenwerkingspartners: RUG, Qbit, Hanzehogeschool, TNO, Alfa College, Noorderpoort College (alle programmapartners).
De programmapartners besluiten in de stuurgroep (Steering Committee, SC) gezamenlijk over het aanstellen van een ambassadeur en de organisatorische inbedding en financiering van deze functionaris. De ambassadeur werkt samen met het programmamanagement en neemt op uitnodiging deel aan de vergaderingen van de SC, maar heeft geen stemrecht. De ambassadeur zorgt voor verbreding van het netwerk, enthousiasmeert potentiële partners en draagt bij aan de continuïteit van het programma door ondernemerschap te stimuleren en alternatieve financiering aan te trekken.

De ambassadeur brengt de resultaten van WP2 t/m 5 en 7 onder de aandacht van relevante stakeholders en speelt daarmee een sleutelrol in de kennisoverdracht op het gebied van: 'Recht en veilige digitale transformatie', 'Cybersecurity by Design', 'Automated Security Response' en 'IoT en security' d.m.v. onderwijsprogramma's voor professionals (taak 2.4) samenwerking met MKB (taak 3.3), kennisontwikkeling (taak 4.1 en taak 4.2), samenwerking met studenten, docenten en onderzoekers (taak 5.1) en thematische workshops voor de stakeholders in Noord-Nederland en daarbuiten. Bouwend op de activiteiten in WP1 zullen de relaties met stakeholders en de verschillende initiatieven op de genoemde gebieden verder worden ontwikkeld. Daarnaast zal er ook specifiek worden gekeken naar verdere financiering voor het onderzoek in de thematische gebieden zowel via subsidies als ook door het sluiten van samenwerkingsverbanden met organisaties in Noord-Nederland.

Resultaten:
D6.4: Plan en Rapportage van jaarlijkse events mbt matchmaking en innovatie met ondernemers, MKB en geselecteerde sectoren (M24, M48, M60)
D6.5: Rapportage over de houdbaarheid en continuïteit van het programma en de uitbreiding van het aantal gecontracteerde samenwerkingspartners op het gebied van cybersecurity in Health, IoT en Fintech (M24, M48, M60)
D6.6: Rapportage over de ontwikkeling van een Noord-Nederlands MKB-netwerk op het gebied van Cybersecurity en de continuïteit hiervan (M24, M48, M60)

3.7 Werkpakket 7 Weerbaarheidstoolbox

Werkpakket	7	**WP Leider**	Qbit
WP titel	**Weerbaarheidstoolbox**		
Start maand	1	**Eind maand**	60

Doelen:
Dit pakket heeft tot doel organisaties te helpen veilig digitaal te ondernemen. Hierbij gaat het vooral om alle organisaties die niet tot de vitale sectoren behoren in Noord-Nederland. Het gaat hierbij om duizenden organisaties variërend van zzp-ers tot en met het grootbedrijf. Om voldoende toekomstbestendig te blijven moeten organisaties zich steeds meer zelf wapenen tegen toenemende dreigingen van de cybercriminelen. Dit zijn vaak geen simpele veranderingen. Om voldoende in competitie te blijven moeten organisaties zich op meerdere terreinen transformeren. We onderscheiden binnen het programma een aantal van deze transformaties:

- Organisaties moeten zich bewust zijn van het gevaar van cybercrime en andere cyber dreigingen;
- Organisaties moeten inzicht hebben in de status van hun cybersecurity;
- Medewerkers moeten over de juiste kennis en vaardigheden beschikken om zich te kunnen wapenen. Hierbij is het van belang dat organisaties en mensen zich blijvend aanpassen aan de nieuwe digitale ontwikkelingen.

Taak 7.1
Leadpartner: Qbit
Samenwerkingspartners: NP/AC
Netwerkpartners: NPAL, VNO/NCW, Stichting Cybersecurity Noord-Nederland, MKB, Samenwerking Noord

Voor groepen bedrijven, denk aan bedrijvenverenigingen, branche- en beroepsverenigingen, en organisaties zoals MKB-Noord en VNO/NCW, worden awareness sessies georganiseerd (Cyber to Go). Deze bijeenkomsten worden verzorgd door professionals en mbo-studenten. Tijdens zo'n bijeenkomst komt onder andere het volgende aan de orde: de kwetsbaarheid en de kenmerken van onveilige WiFi-netwerken en hoe deze te beveiligen, de kwetsbaarheid van de mobiele telefoon, de kwetsbaarheid van apparaten zoals webcams, en het

belang van sterke wachtwoorden. De bijeenkomsten zijn interactief en praktisch van aard. De kwetsbaarheden worden gedemonstreerd door een hacker en studenten van mbo-instellingen geven bijvoorbeeld praktische tips over de beveiliging van mobiele telefoons en dergelijke.

Resultaten
D7.1: Standaardprogramma voor het verzorgen van awareness sessies.
D7.2: Er worden in totaal 72 awareness sessies uitgevoerd met een bereik van minimaal 1.000 organisaties.

Taak 7.2
Leadpartner: Qbit
Samenwerkingspartners: NP/AC
Netwerkpartners: Veiligheidsregio's, Politie Noord-Nederland, NPAL, Groningen Seaports

Om het belang van samenwerking binnen ketens aan te tonen faciliteert het programma Cybercrisis oefeningen met ketenpartijen. In 2017 is een cybercrisis oefening uitgevoerd met een grootschalige stroomuitval in grote delen van Delfzijl en Eemsmond. Verschillende organisaties waren bij de oefening betrokken, zoals de veiligheidsregio, ondernemingen, ambulance, brandweer, gemeenten, politie en het waterschap. Eind 2018 wordt door VR Groningen in kaart gebracht welke verschillende actoren een rol spelen bij digitale dreigingen. Vanaf 2019 worden vergelijkbare oefeningen voor bestuurders en betrokken bedrijven georganiseerd, waarbij de vitale infrastructuur centraal staat. De oefeningen richten zich onder andere op de Noordelijke havens en het drinkwater.

Resultaten
D7.3: Opzet plus draaiboek voor de opzet van een cybercrisis oefening
D7.4: Er worden jaarlijks minimaal 2 oefeningen uitgevoerd (8 in totaal).

Taak 7.3
Leadpartner: Qbit
Samenwerkingspartners: HG, NP/AC
Netwerkpartners: Perfect Day Cyber Security, NPAL, Noordelijke Online Ondernemers, Samenwerking Noord.

Organisaties kunnen hun digitale weerbaarheid laten toetsen via een security scans. Tijdens de audit wordt een aanval op de processen van de organisatie gesimuleerd en wordt de weerbaarheid vastgesteld. De scan maakt in korte tijd de relevante kwetsbaarheden inzichtelijk, resulteert in een praktische to-do-lijst met afgewogen prioriteiten. De scan kijkt naast techniek ook naar het menselijk handelen. Hierbij komen aspecten aan de orde zoals de beveiliging van websites, webshops, mobiele devices, toegang tot vertrouwelijke informatie, CEO-fraude, phishing mails, fysieke toegang tot bedrijfsruimtes, kwetsbaarheid voor cyberaanvallen, wachtwoordgebruik, de omgang met phishing mails, datalekken via laptops et cetera. De scan houdt rekening met de typologie van het bedrijf. De feitelijke doorontwikkeling van de scan wordt overgelaten aan marktpartijen. Het programma onderzoekt, dan wel bewaakt, in hoeverre de scans ook door organisaties worden ingezet.

Resultaten
D7.5: Eerste opzet voor cyber security scan (voor verschillende type bedrijven).
D7.6: In drie verschillende sectoren is bij in totaal 30 bedrijven de scan getoetst.
D7.7: De scans worden door tenminste drie verschillende marktpartijen aangeboden
D7.8: Tenminste 100 organisaties hebben een scan laten uitvoeren.

Taak 7.4
Leadpartner: Qbit
Samenwerkingspartners: HG
Netwerkpartners: Warpnet, IT Academy Noord-Nederland, Samenwerking Noord

Via opleiding en trainingen, via de IT Academy Noord-Nederland, kunnen medewerkers van organisaties hun kennis en vaardigheden vergroten. IT Academy Noord-Nederland heeft samen met onder meer de Groningse cyber security bedrijven Qbit en Warpnet een aantal opledingen ontwikkeld. Een voorbeeld is een leergang waarmee mensen worden omgeschoold tot Security Officer. Inmiddels zijn 10 cursisten van diverse organisaties gestart met de leergang. Ook is een leergang Ethical Hacking ontwikkeld en gestart. Aan deze opleiding worden in de komende jaren nieuwe opleidingen specifiek toegevoegd voor zzp-ers en het midden- en kleinbedrijf. De ervaringen met de security scan worden hiervoor als input gebruikt.

Het programma faciliteert het ontstaan van een Security Pool. Dit is een shared resource pool waaraan medewerkers van verschillende organisaties kunnen deelnemen. Via een gericht opleiding- en trainingsprogramma worden de leden van de pool op het gewenste niveau gebracht. Een niveau waarbij ze hun eigen organisatie kunnen ondersteunen én eventueel inzetbaar zijn voor andere (partner)organisaties. Via een bijeenkomsten worden ervaringen gedeeld en nieuwe kennis verworven. De pool speelt niet alleen in op het enorme tekort aan security professionals. Een belangrijk doel is ook om security- en privacy professionals betere groei- en carrièremogelijkheden te bieden en te voorkomen dat ze het vakgebied verlaten voor lijn-of managementfunctie.

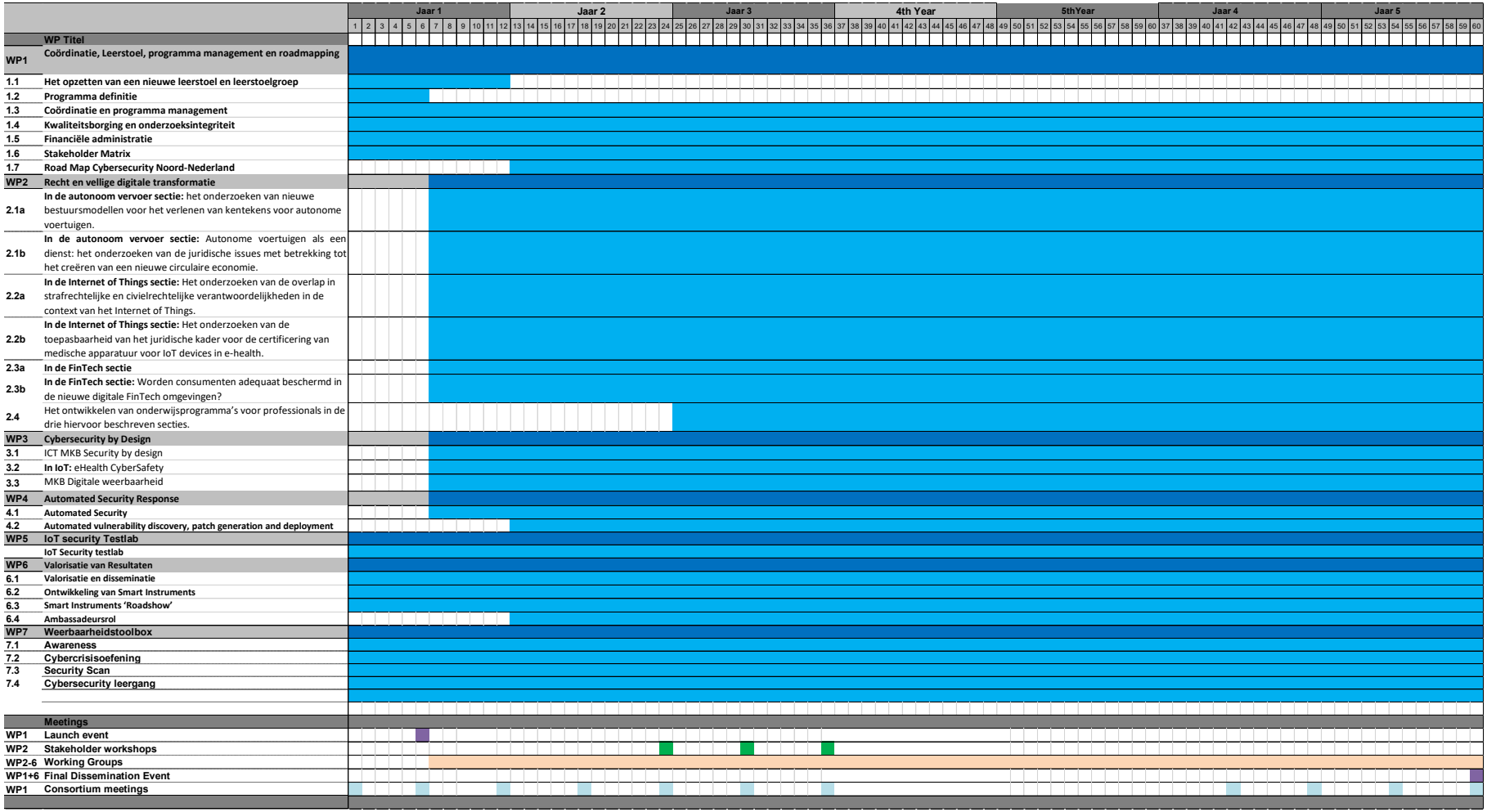
Uitgangspunt is dat elke deelnemende organisatie in de loop van de tijd de kennis en vaardigheden kunnen benutten die bij de aard en volwassenheid van de organisatie passen. De professionals kunnen zich binnen hun vakgebied in de brede en diepte ontwikkelen. Organisaties kunnen mensen en of middelen inbrengen. De professionals worden tegen kostprijs plus ingezet. Hierbij wordt ervoor gezorgd dat kennis binnen organisaties blijft geborgd en kennis zoveel mogelijk wordt gedeeld. Op termijn is het doel dat hierdoor de kosten dalen (alleen nog beheer en onderhoud).

Resultaten:
D7.9: 10 ontwikkelde leergangen die door 1.000 professionals zijn gevolgd.
D7.10: Een shared security pool met minimaal 50 professionals die ruim 200 organisaties ondersteunt.

.

3.8 Planning

Onderstaande Gantt chart geeft een overzicht van de planning van de werkpakketten, taken en gerelateerde meetings en events.



Figuur 4 Programma Cybersecurity Noord-Nederland Gantt Chart

3.9 Deliverables

Onderstaande tabel geeft een overzicht van de tussentijdse resultaten en deliverables van het programma.

Deliverable (nr.)	Deliverable titel	WP nr.	Lead partner	Indiening (M)
D1.1	Rapport m.b.t. het opzetten van de leerstoel en leerstoelgroep	1	RUG	48
D1.2	Programma Plan	1	RUG	6
D1.3	Consortium Overeenkomst	1	RUG	6
D1.4	Stakeholder Matrix	1	RUG	12
D1.5	Cybersecurity onderzoeksagenda en roadmap Noord-Nederland	1	RUG	60
D2.1	Workshop on governance models for automated vehicles	1	RUG	24
D2.2	(Proefschrift) Research on new goverance models for the licensing of automated vehicles	1	RUG	54
D2.3	(Proefschrift) Research on Autonomous vehicles as a service: exploring the legal challenges in creating a new circular economy (M54)	2	RUG	54
D2.4	Workshop on legal issues in IoT security and safety (M30)	2	RUG	30
D2.5	(Proefschrift) Research on the overlap in criminal and civil responsibilities in the context of internet of things (M54)	2	RUG	54
D2.6	(Proefschrift) Research on the applicability of the legal framework for the certification of medical devices for IoT devices in e-health (M54)	2	RUG	54
D2.7	Workshop on legal issues in Fintech cybersecurity and safety	2	RUG	36
D2.8	(Proefschrift) Research on ensuring coherence of legal frameworks	2	RUG	54
D2.9	(Proefschrift) Research on consumer protection in new fintech digital environments	2	RUG	54
D3.1	Op MKB toegespitste handreikingen voor ‘safety by design’	3	HG	36
D3.2	5+ Praktische adviezen mbt toegankelijkheid medische informatie in afzonderlijke ehealth producten of diensten of systemen	3	HG	48
D3.3	Geteste en op MKB toegespitste gereedschappen voor detecteren en inperken van digitale kwetsbaarheden	3	HG	48
D4.1	White Paper on Automated Security	4	TNO	12
D4.2	Proof-of-concept van Security Decision Support	4	TNO	12
D4.3	Proof-of-concept van Automated Response	4	TNO	12
D4.4	Proof-of-concept van automated vulnerability discovery	4	TNO	24
D4.5	Proof of concept van automated patch generation and deployment	4	TNO	24
D5.1	IoT security testlab (infrastructuur, de methoden en technieken)	5	Qbit	12
D5.2	Gecombineerd lectoraat – practoraat	5	Qbit	36
D5.3	50 arbeidsplaatsen (bij Qbit en andere organisaties)	5	Qbit	54

D5.4	10 nieuwe bedrijven (starts-ups)	5	Qbit	54
D6.1	Rapport m.b.t. valorisatie activiteiten (M60)	6	TNO/ RUG/HG /AC/NP	60
D6.2	Smart Instruments design	6	RUG	60
D6.3	Smart Instruments voor Cybersecurity Stakeholders	6	RUG	60
D6.4	Plan en Rapportage van jaarlijkse events mbt matchmaking en innovatie met ondernemers, MKB en geselecteerde sectoren	6	TNO/ RUG/HG /AC/NP -	24, 48, 60
D6.5	Rapportage over de houdbaarheid en continuiteit van het programma en de uitbreiding van het aantal gecontracteerde samenwerkingspartners op het gebied van cybersecurity in Health, IoT en Fintech	6	TNO/ RUG/HG /AC/NP	24, 48, 60
D6.6	Rapportage over de ontwikkeling van een Noord-Nederlands MKB-netwerk op het gebied van Cybersecurity en de continuiteit hiervan	6	TNO/ RUG/HG /AC/NP	24, 48, 60
D7.1	Standaarprogramma voor het verzorgen van awareness sessies	7	Qbit	15
D7.2	Er worden in totaal 72 awareness sessies uitgevoerd met een bereik van minimaal 1.000 organisaties	7	Qbit	60
D7.3	Opzet plus draaiboek voor de opzet van een cybercrisis oefening	7	Qbit	12
D7.4	Er worden jaarlijks minimaal 2 oefeingen uitgevoerd (8 in totaal)	7	Qbit	60
D7.5	Eerste opzet voor cyber security scan (voor verschillende type bedrijven)	7	Qbit	18
D7.6	In drie verschillende secoren is bij in totaal 30 bedrijven de scan getoetst	7	Qbit	60
D7.7	De scans worden door tenminste drie verschillende marktpartijen aangeboden	7	Qbit	60
D7.8	Tenminste 100 organisaties hebben een scan laten uitvoeren	7	Qbit	60
D7.9	10 ontwikkelde leergangen die door 1.000 mensen zijn gevolgd	7	Qbit	60
D7.10	Een shared security pool met minimal 50 professionals die ruim 200 organisaties ondersteunt	7	Qbit	60

Figuur 5 Deliverables Programma Cybersecurity Noord-Nederland

4 Projectorganisatie

4.1 Inleiding

Het programma wordt uitgevoerd door een publiek private samenwerking van ondernemers, kennisinstellingen en (semi-) overheden. Deze partijen werken intensief samen aan de uitvoering van de werkpakketten en zorgen er door de samenwerking voor dat kennisoverdracht plaatsvindt en innovatiekracht en weerbaarheid worden vergroot.

Naast de groep uitvoerende partijen is er een schil van betrokken stakeholders, zoals bedrijvenverenigingen, die de maatschappelijke impact van het programma vergroten.

Programma partners	**Partner short name**	**Type organisatie**
Rijksuniversiteit Groningen (Coördinator)	RUG	WO
Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	TNO	Onderzoeksinstituut
Hanzehogeschool Groningen	HG	Hbo
Noorderpoort	NP	Mbo
Alfa-college	AC	Mbo
Qbit	Qbit	MKB

Het programma is zodanig vormgegeven dat het voor partijen mogelijk is om later aan te sluiten.
Een aantal publieke (onderwijsinstellingen) en private partners (bedrijven) hebben zich nu al bereid verklaard de samenwerking aan te gaan om het programma tot een succes te maken. Zij leveren een bijdrage aan het tot stand komen van deze aanvraag en leveren een (in kind) bijdrage aan de ontwikkeling en uitvoering van het programma. Zij stellen zich daarmee garant voor de oprichting en de continuïteit.
Daarnaast zijn er gesprekken gevoerd met diverse andere partijen. Omdat meerdere partijen hebben aangegeven het initiatief te ondersteunen, zal het aantal partners jaarlijks groeien.
Ook hebben diverse partijen aangegeven het initiatief een warm hart toe te dragen. Zij hebben de intentie tot samenwerking ondertekend.

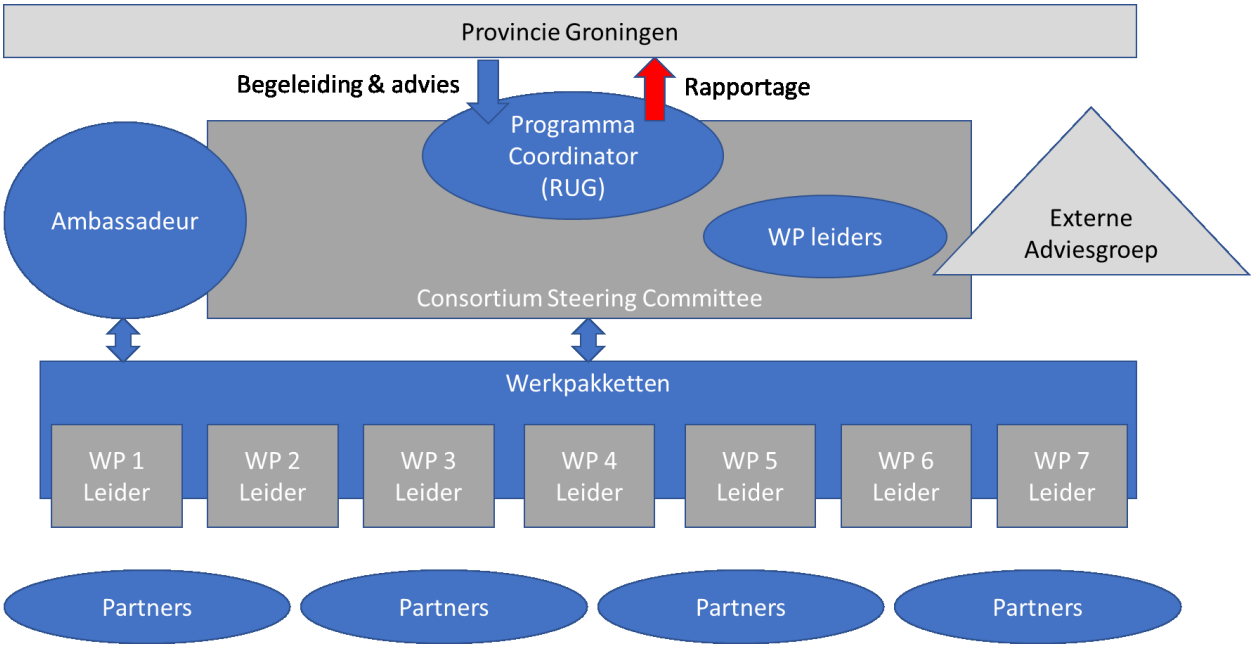
De partijen in de onderstaande tabel hebben toegezegd mee te doen in het netwerk:

Network partners	**Partner short name**	**Type organisatie**
Rijksdienst Wegverkeer*	RDW	Nationale Overheid
Universitair Medisch Centrum Groningen	UMCG	Zorginstelling
Gemeente Groningen	GG	Lokale Overheid
KPN*	KPN	Bedrijfsleven
Samenwerking Noord	SN	Samenwerkingsverband
Noordelijke Online Ondernemers	NOO	Samenwerkingsverband
Rabobank*	RABO	Bedrijfsleven

De Noordelijke ProductiviteitsAlliantie	NPAL	Samenwerkingsverband
Groningen Seaports	GSea	Bedrijfsleven
De Haan Advocaten	HaAd	Bedrijfsleven
Sogeti	SO	Bedrijfsleven
MKB/Noord	MNO	Samenwerkingsverband
VNO/NCW	VN	Samenwerkingsverband
Bedrijvenvereniging West*	BW	Bedrijfsleven
CGI	CGI	Bedrijfsleven
Vereniging Samenwerkende Bedrijven Eemsdelta	SBE	Bedrijfsleven

* support letter volgt.

4.2 Organisatie en governance



Figuur 6 Governance Structuur Programma Cybersecurity Noord-Nederland

4.2.1 Consortium

Het consortium bestaat uit de in paragraaf 4.1 benoemde partner organisaties die vanaf de start bij het programma betrokken zijn. De partners vertegenwoordigd in het consortium zijn vertegenwoordigd in de Consortium Steering Committee.
De partner organisaties zijn individueel verantwoordelijk voor de correcte en tijdige uitvoering van de programma-activiteiten en de inhoudelijke en financiële rapportage naar de subsidiegever, via de penvoerder. De afspraken tussen de consortium partners en het dagelijks management van het programma worden vastgelegd in de Consortium Overeenkomst die met alle consortium partners wordt afgestemd en door alle partijen wordt ondertekend.

Als subsidieverstrekkende partij zal de Provincie Groningen jaarlijks worden geïnformeerd over de voortgang van het project, zoals vastgesteld in de subsidievoorwaarden. Gedeputeerde Staten hebben de mogelijkheid om op basis van deze rapportage en evaluatie, in nauw overleg met de SC, bij te sturen. De SC blijft eindverantwoordelijk voor de uitvoering van het project.

4.2.2 Consortium Steering Committee (SC)

De Consortium Steering Committee is het besluitvormingsorgaan van het programma. De Steering Committe legt verantwoording af aan de subsidieverstrekker. De Steering Committee is verantwoordelijk voor:

- Essentiële beslissingen nemen over het management van het programma, waaronder:
  - Goedkeuring van het projectplan, het evaluatieplan, de tussentijdse rapporten en de eindverslagen en elke wijziging van die documenten.
  - Opnieuw toewijzen van budgetten.
  - Herbestemming of beëindiging van bestaande werkpakketten en wijzigingen in de timing van individuele werkpakketten.
  - Creëren en toewijzen van nieuwe werkpakketten (indien nodig).
- Beëindiging van de deelname van in gebreke blijvende partners en subcontractors.
- In samenspraak met de programma coördinator het contact onderhouden met de Externe Adviesgroep (EA).
- In de Steering Committee zitten de leadpartners van de verschillende werkpakketten en de programma coördinator. De ambassadeur neemt deel aan de vergaderingen van de steering committee, maar heeft geen stemrecht. De programma coördinator is voorzitter van de Steering Committee.

4.2.3 Programma Coördinator (PC)

Het belangrijkste doel van het programma management is om een gericht, lean maar effectief kader te bieden om het consortium te ondersteunen bij het bereiken van de doelstellingen van het programma. Efficiënte besluitvormingsprocessen en een snelle reactie op veranderende omstandigheden zijn vereist. De programma coördinator (PC) neemt de verantwoordelijkheid voor het algemene programma management. Dit omvat de interacties met de Provincie Groningen op contract gerelateerde kwesties en het voorzitten van regelmatige Steering Committee Meetings. De PC heeft onder meer een aantal administratieve en financiële taken - het consortium vertegenwoordigen in workshops en officiële vergaderingen, het verzamelen van administratieve rapporten van partners en het doorsturen van periodieke rapporten aan de projectmedewerker, het voorbereiden en bijwerken van de Consortium Overeenkomst tussen de partners, het beheer van projectmiddelen en projectuitgaven, beheer van de ethische en onderzoek integriteit issues, coördinatie van de valorisatie van de programma resultaten. De PC wordt ondersteund door een projectmanager voor het algemene programma management.

4.2.4 Werkpakket Leiders (WP-leiders)

Elk werkpakket wordt geleid door een ervaren lid van het consortium met expertise op het betreffende gebied. Werkpakket leiders zullen verantwoordelijk zijn voor het succes van hun werkpakket en verantwoording afleggen aan de programma coördinator. Om het beheer van de taken in elk werk pakket te **vergemakkelijken**, zal de werkpakket leider daar waar nodig worden bijgestaan door een kernteam van 2 tot 4 partners om de taken uit te voeren.

Naast de inhoudelijke activiteiten in het werkpakket speelt de WP-leider een belangrijke ambassadeursrol (m.n. voor de content WPs 2-5) naar de externe stakeholders. Deze rol en taken zijn beschreven in de relevante Werkpakketen.

4.2.5 Ambassadeur (ABS)

De programmapartners besluiten in de SC gezamenlijk over het aanstellen van een ambassadeur en de organisatorische inbedding en financiering van deze functionaris. De ambassadeur werkt samen met het programmamanagement aan de positionering en impact van het programma.
De ambassadeur faciliteert in de kennisoverdracht naar onderwijsprogramma's voor professionals, thematische workshops etc. Bouwend op de inhoud van de werkpakketten onderhoudt hij/zij relaties met stakeholders, boort nieuwe relaties (marktpartijen) aan voor deelname aan een van de werkpakketten, probeert de uitvoering van nieuwe onderzoeksprogramma's mogelijk te maken en is betrokken bij de totstand koming van Startups. Ook zorgt hij/zij voor de noodzakelijke aanvullende financiering van de onderzoeksprogramma's. De ambassadeur is daarnaast betrokken bij de organisatie van (netwerk)bijeenkomsten, congressen etc. en de overige externe communicatie over het programma. Daarnaast onderhoudt de ambassadeur contacten met andere landelijke en regio (Friesland, Drenthe) initiatieven.
De ambassadeur wordt uitgenodigd bij vergaderingen van de SC, maar is als onafhankelijke functionaris geen partner en heeft daarom geen stemrecht.

4.2.6 Partners

Er zijn gesprekken gevoerd met diverse andere partijen. Omdat meerdere partijen hebben aangegeven het initiatief te ondersteunen, zal het aantal partners jaarlijks groeien. Ook hebben diverse partijen aangegeven het initiatief een warm hart toe te dragen (zie bijlage 5). Zij hebben de intentie tot samenwerking ondertekend. De in paragraaf 4.1 benoemde partijen die reeds hebben toegezegd mee te willen doen met het programma kunnen worden aangevuld met partners uit de stakeholder analyse zoals deze wordt uitgevoerd in Taak 1.8.

4.2.7 Externe Adviesgroep (EA)

De EA bestaat uit uitgenodigde genomineerde deskundigen die zich bezighouden met cybersecurity en cybersafety en die (internationale) wetshandhavingsinstanties, nationale inlichtingeninstituten, bedrijven, overheden, onderwijs- en onderzoeksinstellingen en overige stakeholder groepen vertegenwoordigen. Het is bedoeld om de wisselende belangen van de stakeholders van het programma te vertegenwoordigen.
De EA is verantwoordelijk voor:

- Toezicht houden op bepaalde aspecten van het programma (beleidsrichting in tegenstelling tot het dagelijks beheer).
- Optreden als 'ambassadeurs' voor het programma, het promoten van haar activiteiten, het identificeren van geschikte kandidaten om op te nemen in de stakeholder matrix van het programma en het identificeren van geschikte evenementen waar het programma haar bevindingen kan presenteren.
- Wetenschappelijk en praktisch advies geven op het gebied van hun expertise.
- Feedback op programma geven en resultaten beoordelen.
- Expertise toevoegen aan het consortium.

- Evaluatie, in samenwerking met de programma coördinator, van de resultaten en evenementen voor verspreiding.
- Assisteren van de projectpartners bij het bereiken van impact.

5 Communicatieactiviteiten

De communicatie is in eerste instantie gericht op het bekend maken en laten toenemen van de bekendheid van het Programma Cybersecurity Noord-Nederland. De boodschap die in deze fase wordt uitgedragen is het belang van cybersecurity, de beschikbare hulp en het uit te voeren onderzoek. In alle uitingen wordt opgenomen dat dit initiatief mede mogelijk is door de betrokkenheid en ondersteuning van de provincie Groningen.
De communicatie verloopt via een speciaal ontwikkelde middelen (o.a. website, Facebookpagina, twitter etc.) en via speciale momenten waarop het programma onder de aandacht wordt gebracht (Presentaties/workshops op congressen, netwerkbijeenkomsten, bedrijvenbijeenkomsten etc.) In de latere communicatie wordt ook nadrukkelijk aandacht besteed aan behaalde resultaten van het onderzoek. Onderzocht wordt de mogelijkheid om via een periodieke column aandacht te schenken aan het onderwerp cybersecurity.

De Valorisatie en disseminatie strategie voorziet in het gebruik van de volgende mechanismen om de stakeholders op de verschillende niveaus te bereiken:

Nr.	Mechanisme	Beschrijving	Doelgroepen
1	Website en social media	Interactief online portaal verdeeld in een publiek en een afgeschermd gedeelte. Het publieke deel bevat informatie over het programma, alle openbare deliverables van de onderzoeksprojecten, links naar andere relevante netwerken/initiatieven/ projecten. Het afgeschermde deel bevat een veilige werkomgeving waarin partners kunnen deelnemen als onderdeel van de programma-activiteiten.	Alle doelgroepen van het programma
2	Presentatie/brochure	Korte presentatie over het waarom en aanpak van het programma, inclusief een overzicht van de tools/producten die in het project moeten worden ontwikkeld. Deze presentatie/brochure wordt gebruikt als het visitekaartje van het programma.	Alle doelgroepen
3	Video’s	Er wordt een aantal video’s opgenomen met korte impressies over onderdelen uit het project (resultaten, producten, bijeenkomsten). Deze video’s worden via de website gepresenteerd.	Deelnemende en geïnteresseerde bedrijven, politiek en overige geïnteresseerden
4	Publicaties	Publicaties en artikelen hebben een brede verspreiding. De consortiumpartners zullen de impact van de verspreidingsactiviteiten versterken door formele rapporten en wetenschappelijke artikelen in open access, peer-reviewed tijdschriften, te publiceren. Deze zorgen ervoor dat het programma een	Academici en geïnteresseerden in cybersecurity.

		langdurig effect heeft, met name voor het academici met interesse voor de aandachtsgebieden/thema's.	
5	Stakeholders workshops en conferentie	Er worden verschillende stakeholderworkshops georganiseerd tijdens het programma. Aan het einde is er een slotconferentie. Deze evenementen worden gebruikt om de resultaten van het programma te verspreiden en te valideren.	Alle doelgroepen
6	Presentaties	De partners van het consortium geven presentaties en lezingen voor op seminars, relevante evenementen en geselecteerde internationale conferenties. Een lijst van conferenties zal in de loop van het project worden ontwikkeld, met als doel een goede disciplinaire en nationale verspreiding te bereiken	Alle doelgroepen

Figuur 7 Valorisatie en Disseminatie Strategie

Overige activiteiten

Daarnaast worden de volgende activiteiten uitgevoerd om het programma meer bekend te maken:

- Bijwonen van congressen/workshops;
- Bijeenkomsten georganiseerd in samenwerking met VNO/NCW, MKB;
- Bijeenkomsten voor bedrijvenverenigingen;
- Column in bv NDC die zich speciaal richt op het gevaar van cybercriminaliteit voor burgers en bedrijfsleven;
- Netwerkbijeenkomsten waar het programma op mee kan liften;
- Netwerkbijeenkomsten door het programma georganiseerd;
- Individuele gesprekken met partijen (bedrijven, brancheorganisaties, belangengroepen, overheid, DTC-programma, Innovation Board Noord-Nederland);
- Aansluiten bij cybersecurityinitiatieven in andere sectoren Energie, Healthy Ageing;
- Aansluiten bij start up bijeenkomsten;
- Aansluiten bij cybersecurityinitiatieven en bijeenkomsten van decentrale landelijke overheidsdiensten Politie, Justitie en Defensie, Veiligheidsregio;
- Deelname aan gezamenlijk organiseren van cybersecurityoefeningen.

6 Kostenbegroting

Zie bijlage 4

7 Lijst met figuren

Bijlagen

Bijlage 1 Voorbeelden cybercrime

- De cyberaanval in 2014 door Noord-Korea op het wereldwijde televisie-, film- en studioconcern Sony Pictures was volgens de Amerikaanse geheime diensten de ernstigste aanval op een Amerikaans doelwit. Hierbij werden nog niet gepubliceerde films en gevoelige informatie gelekt.
- In de zomer van 2014 kwam de Amerikaanse beveiligingsfirma 'Hold Security' erachter dat er maar liefst 1,2 miljard gebruikersnamen en wachtwoorden én meer dan 500 miljoen e-mailadressen van over de hele wereld zijn 'gestolen'. de hack werden er op deze manier 5.600 Nederlandse websites getroffen.
- De hackersgroep Impact Team hackte in de zomer van 2015 de datingswebsite Ashley Madison. Bij deze hack heeft de hackersgroep een grote hoeveelheid klantgegevens bemachtigd. Er werden gegevens van maar liefst 37 miljoen gebruikers gestolen.
- Hackers maken slim gebruik van de situatie wanneer ING te maken krijgt met een storing. Klanten van ING konden uren geen gebruikmaken van de services van de (App en Mijning). Tijdens de storing stuurden hackers een nep ING-mail gestuurd waarin stond dat ING overgestapt is naar een beter beveiligend systeem. In deze mail bevond zich ook een link om vervolgens, na het klikken, doorgestuurd te worden naar een phisingwebsite. Wanneer de klant terecht komt op deze phisingwebsite, is het bijna niet te onderscheiden van de echte website van ING. Deze website lijkt dus op de oorspronkelijke website van ING, maar wordt gebruikt om inloggegevens, rekeningnummers, pasnummers en verdere (persoonlijke) informatie te bemachtigen.
- Almi is een middelgroot metaalbedrijf uit Vriezenveen. Producten gaan de hele wereld over, als eigen eindproduct of als toelevering aan andere bedrijven. In de enorme fabriekshal gaat veel digitaal en automatisch. Via een cyberaanval ging juist door de vergaande automatisering bijna alles plat. E-mail, ordersysteem, facturatie, ons automatisch magazijn, niets werkte meer. Het gijzelvirus richtte daardoor overall een schade aan van minstens 60.000 euro.

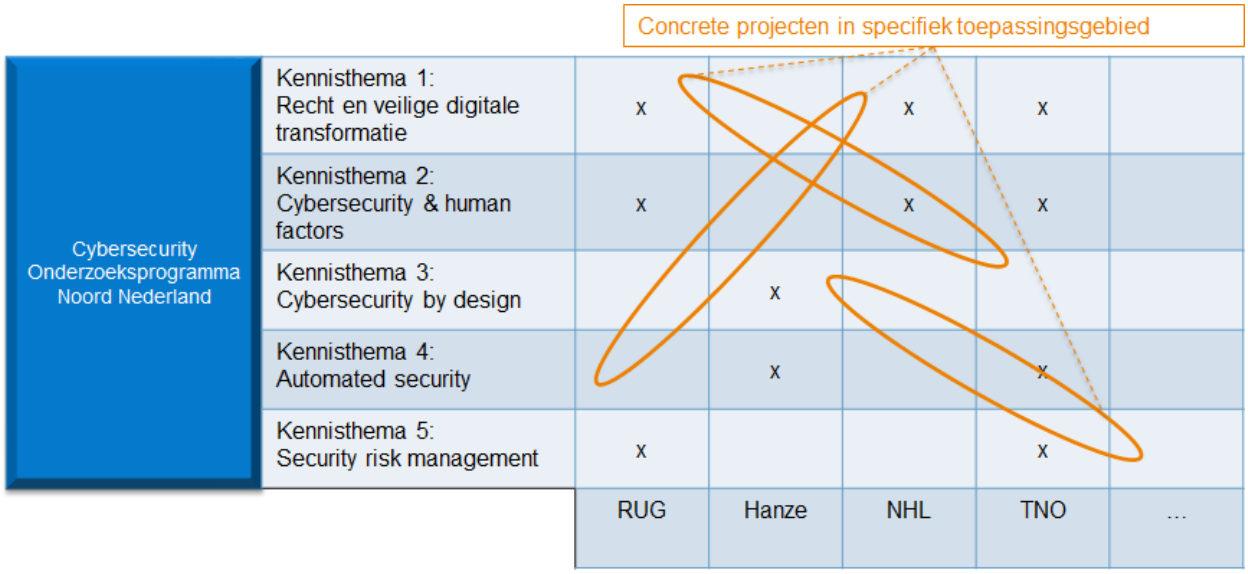
Bijlage 2 Studies

- Uit onderzoek, dat in opdracht van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (Ministerie van Veiligheid & Justitie) is uitgevoerd door Plato en Ockham, blijkt dat er in 2014 in Nederland ongeveer 7.000 personen werkzaam waren in cyber security[8]. Het aantal vacatures in dat jaar was 1.316, met een verwachte jaarlijkse groei van 10%. Doorgerekend betekent dat bijna 1900 openstaande vacatures in 2018.
- Een EZ-studie uit 2016 schat dat er in 2014 in de ICT-sector alleen al 16.400 personen zijn die zich bezighouden met cyberactiviteiten, met een gemiddelde groei tussen 2010 en 2014 van 7%.[9] Dat betekent in 2018 ca. 21.500 personen.
- In de EZ-studie wordt het gebrek aan beschikbaarheid van gekwalificeerd personeel als grootste zwakte en als grootste bedreiging van de marktontwikkeling genoemd. Het gaat daarbij naast technisch ook om meer mens of beleid gericht personeel (security officer, beleidsmedewerker, juristen).
- Steeds meer functies krijgen een cybersecurity-component en daarmee ontstaat er een groeiende vraag naar Post hbo-trajecten en korte 'nieuwsgierigheidscursussen' zoals Ethical Hacking. Uit onderzoek van het ISACA blijkt dat initiële opleidingen aan studenten maar een deel van de benodigde competenties en ervaring voor cybersecurity-profielen op strategisch-tactisch niveau leveren.[10] Werkervaring en extra cursussen zorgen voor aanvullende competenties of specialisaties.
- Uit gesprekken die de Stichting Cybersecurity Noord-Nederland heeft gevoerd met diverse bedrijven is duidelijk geworden dat ook Noord-Nederland grote behoefte heeft cybersecuritypersoneel. Bestaande leveranciers kunnen de almaar groeiende vraag niet aan. Dit wordt bevestigd door het onderzoek "Stand van zaken op de Noord-Nederlandse arbeidsmarkt Update NOA 2017-2020". 11 Hierin is beschreven dat er krapte is op de Noord-Nederlandse arbeidsmarkt van ICT'ers door de aantrekkende economie en de toenemende digitalisering. Het aantal studenten dat zich specialiseert en afstudeert is nog te beperkt.

[8] PLATO & Ockham IPS (2014). Arbeidsmarkt voor Cyber Security Professionals.
[9] SEO/VKA (2016). Economische kansen Nederlandse Cybersecurity-sector.
[10] ISACA & RSA (2016). 'State of cybersecurity. Implications for 2016.'
[11] Stand van zaken op de Noord-Nederlandse arbeidsmarkt Update NOA 2017-2020

Bijlage 3: Noordelijke Onderzoeksagenda Cybersecurity

Cybersecurity is bij uitstek een onderzoeksgebied dat multidisciplinair en op verschillende niveaus (WO, hbo, mbo) moet worden aangevlogen. Daarom is voor het programma een eerste aanzet gemaakt voor een Noordelijke onderzoeksagenda cybersecurity, waarin alle noordelijke onderzoeksinstituten (RUG, Hanzehogeschool, NHL, TNO, Noorderpoort, Friese Poort) samenwerken en waarbij ook nadrukkelijk de samenwerking met bedrijfsleven en overheden wordt gezocht. Het is de intentie om ook de niet aangesloten mbo-scholen in Noord-Nederland uit te nodigen en te betrekken. In het programma wordt deze onderzoeksagenda verder ontwikkeld en wordt gewerkt met een meerjarige "Cybersecurity onderzoeksagenda Noord-Nederland" die jaarlijks concreet wordt ingevuld. De onderzoeksagenda bestaat uit meerdere kennisthema's (zie afbeelding hieronder) waar diepgaande kennis wordt opgebouwd. Elk kennisthema heeft meerdere deelnemende onderzoekspartijen, waarbij één van de partijen de trekkersrol heeft voor een thema. In het programma worden projecten uitgevoerd, die meestal meerdere kennisthema's nodig heeft en waarbij meerdere partijen betrokken zijn. Een project kent altijd een specifiek toepassingsgebied, waarbij wordt aangesloten bij de toepassingsgebieden waarin Noord-Nederland sterk is, zoals energie, chemie, eHealth en 5G.



Figuur 7 Draft opzet Cybersecurity Onderzoeksprogramma Noord-Nederland

De RUG is trekker van kennisthema 1 en richt daartoe de leerstoel "**Recht en Veilige Digitale Transformatie"** in (zie §3.2; WP2). Hier wordt onderzoek gedaan naar o.a.: 1. Bescherming van intellectuele eigendomsrechten bij digitalisering; 2. Strafrechtelijke en civielrechtelijke aansprakelijkheid van eigenaren en gebruikers van 'Internet of Things devices' in geval van inbreuk en misbruik, 3. De juridische implicaties van robotisering en 'automation', bijvoorbeeld in de arbeidsorganisatie (maakindustrie) of in de vervoerssector (autonome auto's).
Netwerkpartner NHL Stenden is bezig met van kennisthema 2. Zij doen o.a. onderzoek naar de mate van weerbaarheid van en slachtofferschap onder het MKB. Tevens doet de NHL Stenden onderzoek naar de 'law enforcement' aspecten van digitale ontwikkelingen. Bij het onderwerp 'de zelfrijdende auto' (WP2) is een belangrijke vraag wat dat betekent voor strafrechtelijke en/of bestuurlijke handhaving. Van nieuwe maatregelen/ontwikkelingen is 'handhaafbaarheid' dan wel de betekenis van die ontwikkeling voor handhaving en opsporingsbeleid een onderwerp waarop de maatregel/ontwikkeling dient te worden beoordeeld om er als samenleving goed mee om te kunnen gaan.

De Hanzehogeschool is trekker van kennisthema 3. Ze breidt **haar lectoraten "Juridische aspecten van de arbeidsmarkt" en New Business & ICT** uit met het onderwerp cybersecurity. Tevens wordt dit onderwerp daarmee een centraal thema binnen de Digital Society Hub waarbinnen studenten i.s.m. docentonderzoekers en mensen uit het bedrijfsleven werken aan CyberSafety vragen uit bedrijven en instellingen. De Hanzehogeschool onderzoekt onder meer hoe er tijdens de ontwerpfase rekening kan worden gehouden met veiligheid en juridische kaders (zie §3.3; WP3). Onderzoeksvragen daarbij zijn: 1. Welke privacyaspecten en AVG-vraagstukken kunnen in de ontwerpfase worden meegenomen? 2. Welke beleidsmaatregelen (wachtwoordenbeleid, regels voor online betaling, veiligheidsaudits, etc.) kunnen in de ontwerpfase al worden ingebouwd? Het onderzoek van de Hanzehogeschool heeft ook een sterke juridische component. De Noorderpoort en het Alfa-college nemen ook deel aan deze projecten. Zij stellen gezamenlijk een practor[12] aan die een rol vervult in de projecten (§3.7; WP7).
TNO is trekker van kennisthema's 4 en 5 (zie §3.4; WP3). De Noordelijke vestiging van TNO heeft expertise op deze thema's en er lopen al diverse projecten bij TNO; er zit ook een aantal Europese (H2020) projecten in de pijplijn waarin deze onderwerpen worden geadresseerd. TNO is per definitie multidisciplinair ingericht op het onderwerp cybersafety en kan ook in de andere kennisthema's belangrijke bijdragen leveren.

[12] een practor is een boegbeeld, inspirator en motor, verantwoordelijk voor kennisontwikkeling- verspreiding (in en extern) en –toepassing, praktijkgericht onderzoek en professionalisering van docenten in samenwerking met het bedrijfsleven

Bijlage 4: overall begroting
Bijlage 4.1 t/m 4.6: details

Bijlage 5:
5.1 Bijdragen derden

Supportbrieven:
Noordelijke Online Ondernemers
Samenwerking Noord
Groningen Seaports
UMCG
Sogeti
Noordelijke Productiviteits Alliantie
De Haan Advocaten en Notarissen
MKB-Noord
VNO-NCW
Vereniging Samenwerkende Bedrijven Eemsdelta
Gemeente Groningen

Bijlage 5.2 Commitment Consortiumpartners

Alfa College
Hanzehogeschool Groiningen
Noorderpoort College
Qbit
Rijksuniversiteit Groningen (penvoerder)
TNO