TKI Call for Proposals

Cyberweerbaarheid voor kritische ketens en systemen in Energie, Gezondheid & Zorg en Tuinbouw & Uitgangsmaterialen

Hoofddocument (NL)

1. Context

Cyberveiligheid gaat over het geheel aan maatregelen om schade te voorkomen door verstoring, uitval of misbruik van elektronische data en computers. De schade kan met opzet ontstaan door een cyberaanval maar ook een onbedoelde oorzaak hebben, bijvoorbeeld een fout in software(updates), menselijke fouten of een combinatie daarvan. Cyberweerbaarheid is niet alleen het voorkomen van schade maar ook "het vermogen te reageren op een cyberaanval en eventuele schade te herstellen". In deze call maken we gebruik van de term cyberweerbaarheid omdat we ook zoeken naar oplossingen voor het voorkomen van cyberincidenten en - als incidenten zich voordoen - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

Cyberweerbaarheid is een randvoorwaarde voor het veilig en toekomstbestendig functioneren van de Nederlandse samenleving, die in rap tempo digitaliseert. Dit geldt in zeer hoge mate voor ketens en systemen in de sectoren Energie, Gezondheid & Zorg en Tuinbouw als onderdeel van de Nederlandse voedselketen. Cyberweerbaarheid draagt ook bij aan economische groei. Het belang én de urgentie worden inmiddels onderkend. Het onderwerp heeft dan ook een belangrijke plek in het Missiegedreven Topsectoren en Innovatie Beleid, als één van de zeven digitale sleuteltechnologieën binnen Topsector ICT en KIA Digitalisering. De cross-over van kennis tussen genoemde sectoren en digitalisering is een voorwaarde voor een sterke cyberweerbaarheid in de keten en de hierin gebruikte systemen.

Het belang en de impact van digitalisering en de complexiteit van de bijbehorende nieuwe oplossingen en de verbetering en integratie van bestaande producten, maken het noodzakelijk dat multidisciplinair wordt samengewerkt, (Top-)sectoroverstijgend en in het gehele ecosysteem.

Binnen het Cybersecurity voor Nederland (CS4NL) programma werken de topsectoren samen om kennis en innovatie op het gebied van cybersecurity te stimuleren. Deze call op het thema systeem- en ketenweerbaarheid is tot stand gekomen binnen CS4NL, in samenwerking met de Topsectoren Energie, Tuinbouw & Uitgangsmaterialen, Life Sciences & Health en ICT. Projectaanvragen dienen zich te richten op minstens twee van deze Topsectoren. De call biedt tevens ruimte voor meta-projecten over meerdere sectoren.

2. Call for Proposals: Cyberweerbaarheid voor kritische ketens en systemen in Energie, Gezondheid & zorg en Tuinbouw en Uitgangsmaterialen

Deze call richt zich op het ontwikkelen van kennis en innovaties voor het verbeteren van de digitale veiligheid en weerbaarheid in de hele keten en het gehele systeem dat vitale diensten en producten voortbrengt binnen de genoemde Topsectoren.

Met een kritische keten bedoelen we het totaal aan activiteiten en verbindingen van de bron tot de eindgebruiker. Voorbeelden van ketens zijn:

- De productie, teelt, inpakken, sorteren, verhandelen van bijvoorbeeld tomaten voor de versmarkt.
- De productie, transport, opslag, conversie, distributie en verbruik van verschillende energievormen zoals elektriciteit, warmte, brandstoffen en gas.
- De keten van zorg- en gezondheidsinformatie tussen zorgprofessionals, clouddiensten en leveranciers en de thuissituatie.

Met een systeem bedoelen we een proces of onderdeel van de keten bijvoorbeeld de energiecentrale, de kas, het ziekenhuis, etc.

Doordat ketens en hun aansturing steeds meer digitaliseren en IT (producten en diensten) afnemen kun je eigenlijk niet meer spreken van rechtlijnige ketens. Het zijn eerder complexe ecosystemen. Dit maakt het lastig om inzicht te krijgen in de samenstelling en functionaliteit van 'de keten'. Denk bijvoorbeeld aan zicht op de partij achter een (toe)leverancier die data opslaat of de software levert voor een beheerdersportaal van assets. Ook groeien de afhankelijkheden tussen

ketenpartijen doordat informatiesystemen onderling verbonden worden of omdat er gebruik gemaakt wordt van hard- of software van dezelfde leverancier. Bij essentiële diensten (bijvoorbeeld de levering van energie) worden digitale en informatietechnologieën gebruikt voor het monitoren, simuleren, voorspellen en besturen van systemen of ter ondersteuning van advies en besluitvorming. Er ontstaat een enorme groei in data verzameling en uitwisseling, waarbij data-gedreven methoden (zoals machine learning-algoritmen) een belangrijke rol spelen om de datastromen te analyseren en op basis daarvan (geautomatiseerd) te interveniëren. Als gevolg daarvan ontstaat een groeiende afhankelijkheid van derde partijen die cruciale IT leveren. Het uitvallen of slecht/verkeerd functioneren van systemen en diensten die zij aanbieden kunnen verstoringen teweegbrengen. Dat kan door een gerichte cyberaanval zijn maar ook een onbedoelde verstoring door personeel of software (update) fouten. De meer complexe digitale ketens en daarmee samenhangende onderlinge afhankelijkheden tussen ketenpartijen zorgen voor een risico op systeemniveau omdat de leveringszekerheid van vitale processen, zorg, energie, food in gevaar komt.

Een andere kwetsbaarheid ontstaat door de groei van het zogenaamde "aanvalsoppervlakte" door een toenemend aantal gedistribueerde schakels in de ketens, zoals omvormers voor zonnepanelen in huishoudens, slimme zorgapparatuur en geautomatiseerde kassen. Een cyberaanval op één van deze schakels kan leiden tot diefstal van gevoelige data en zelfs storing of uitval in de keten.

3. Vormen van onderzoek

Binnen de call passen R&D activiteiten die zich richten op technologische ontwikkeling. Het kan gaan om industrieel onderzoek of om experimentele ontwikkeling[1]. *Industrieel onderzoek* definiëren we als planmatig onderzoek dat is gericht op het opdoen van nieuwe kennis en vaardigheden met het oog op de ontwikkeling van nieuwe producten, procedés of diensten, of om bestaande producten, procedés of diensten aanmerkelijk te verbeteren. *Experimentele ontwikkeling* definiëren we als het verwerven, combineren, vormgeven en gebruiken van bestaande wetenschappelijke, technologische, zakelijke en andere relevante kennis en vaardigheden, gericht op het ontwikkelen van nieuwe of verbeterde producten, procedés of diensten. Binnen de call passen geen activiteiten die zich enkel richten op kennisontwikkeling op sociaalwetenschappelijke vraagstukken. Ook past implementatieonderzoek van al ontwikkelde producten, procedés of diensten niet binnen de kaders van deze call.

4. Innovatiethema's

Systeem en ketenweerbaarheid is een omvangrijk begrip. Om aandachtsgebieden te onderscheiden volgt hieronder een beschrijving in zes perspectieven. Inhoudelijk dienen de projecten kennis en innovaties te ontwikkelen in één of meerdere van de onderstaande gebieden. In alle gevallen geldt dat speciale aandacht wordt gevraagd voor het toegankelijk maken van relatief dure technologieën voor mkb.

1. **Identificeren en aanpakken:** Vanwege de complexe en dynamische afhankelijkheden op keten- en systeemniveau zijn innovatieve technieken nodig om beter zicht te krijgen op hoe de kritische ketens en systemen in de genoemde sectoren in elkaar zitten, waar afhankelijkheden bestaan en welke cyberrisico's daaruit voorkomen. Dit aandachtsgebied richt zich op het identificeren en monitoren van deze risico's en het ontwikkelen van ingrepen om daarop te handelen. Een voorbeeld van een risico is de afhankelijkheid van software van derde partijen, waardoor de behoefte bestaat om de impact van een kwetsbaarheid in dit soort software te identificeren en monitoren. Een ander voorbeeld betreft de cloud infrastructuur waarvan bekend is dat de onderliggende hardware, software en configuraties kwetsbaar kunnen zijn. Dat geldt ook voor IoT apparaten en sensoren van leveranciers, waarvan data kunnen worden gestolen of gemanipuleerd. Meer generiek is bijvoorbeeld te denken aan slimme methoden en tools om dit soort risico's te identificeren en monitoren (o.a. smart zelfscans, pentests). Naast het identificeren en monitoren is

[1] Voor uitgebreide definities van industrieel onderzoek en experimentele ontwikkeling, zie https://www.rvo.nl/subsidies-financiering/mit/rd-samenwerkingsprojecten/definities.

behoefte om door middel van ingrepen de aanvalsoppervlakte in kritische ketens of systemen direct te verkleinen. Bijvoorbeeld door nieuwe manieren om keten breed intelligente beveiligingspatches te genereren en door te voeren. Ook zijn mogelijk nieuwe decentrale systeemontwerpen een oplossing. Met nieuwe methoden moeten de sectoren in staat gesteld worden om de (optimale) digitale veiligheid van (componenten van) een keten of systeem te bepalen en te handelen.

2. **Delen**: Data is één van de meest waardevolle middelen geworden. Kritieke ketens en systemen genereren grote hoeveelheden sensitieve data. Op ketenniveau, waar verschillende partijen nauw samenwerken, is ontsluiting van data en informatie op transparante en veilige wijze essentieel. Interoperabiliteit van de onderliggende systemen is hiervoor randvoorwaardelijk. Hoe kunnen we versleutelde databases ontwikkelen die verschillende typen data kan verbinden? Hoe kunnen we voorkomen dat data-gedreven besluitvorming van buitenaf wordt beïnvloed? Hoe kunnen we berekeningen inrichten op een manier dat sensitieve data zo min mogelijk hoeven worden gedeeld? Kunnen we *verifiable computing* en cryptografische technieken toepassen? Hoe maken we onderdelen van de keten interoperabel op een veilige manier?
3. **Simuleren:** Voor de bewustwording van de effecten die een slechte weerbaarheid in de keten heeft en/of het trainen van hoe men moet reageren bij een incident is het essentieel medewerkers trainen. De ontwikkeling van simulatiemodellen is hierbij belangrijk, evenals het creëren van de simulatie ervaring. Welke modellen kunnen ontwikkeld worden voor simulatie? Welke data zijn daarvoor nodig? Welke technologie is geschikt voor het nabootsen van een incident of gedetecteerd risico?
4. **Detecteren:** Het is van belang om, wanneer een cyberaanval plaatsvindt, dit gelijk te detecteren. Hiervoor is het nodig om signalen te ontdekken die duiden op afwijkingen in IT, OT en IoT-omgevingen. Dat kan bijvoorbeeld gaan om het detecteren van onderschepping of manipulatie van datastromen die gebruikt worden in kritieke operationele systemen of binnen ketens. Ook kan onderzoek zich richten op de detectie van malware binnen ketens. Detectie door middel van machine learning algoritmen lijkt veelbelovend, maar vergt nog verdere ontwikkeling. Kunnen we deze algoritmen gebruiken om niet alleen de complexiteit van de ketens in kaart te brengen, maar ook voor tijdige detectie van aanvallen? Welke data(bronnen) zijn daarvoor nodig, voorafgaand aan en tijdens een incident? Hoe evalueren we voortdurend de kwetsbaarheid van software? Kunnen technieken zoals 'federated learning' helpen bij het inschatten en mitigeren van risico's in gedistribueerde systemen?
5. **Reageren en herstellen:** Projecten kunnen zich tot slot richten op oplossingen en maatregelen die bijdragen aan het herstelvermogen van ketens en systemen na een cyberaanval. Dat kan bijvoorbeeld gaan om het verbeteren de systeemweerbaarheid tegen load altering attacks. Niet alleen herstel is hierbij van belang, maar ook het snel vinden van de oorzaak (relatie met het aandachtsgebied detecteren).

Onderaan dit document zijn ter inspiratie voor de Topsectoren Tuinbouw & Uitgangsmaterialen, Energie, en Life Science & Health voorbeelden uitgewerkt (punt 10), om een indruk te geven van de sectorale uitdagingen en behoeften aan R&D.

5. Beschikbaar budget

Het totale beschikbare budget voor deze call is €2.500.000,=. Het beschikbare budget wordt uitgezet vanuit de TKI PPS-innovatieregeling door TKI Energie, TKI T&U (Tuinbouw & Uitgangsmaterialen), TKI Life Sciences & Health (Health~Holland) en TKI ICT, indien aansluitend bij de betreffende kennis- en innovatie agenda's en uitvoeringsprogramma's.

6. Voorwaarden samenwerkingsprojecten

Publiek-private samenwerkingsprojecten zijn projecten die worden uitgevoerd door een samenwerkingsverband (consortium) van bedrijven en kennisinstellingen. De minimale omvang van een consortium is één kennisinstelling en één onderneming. Consortia waarin universiteiten en

praktijkgerichte onderzoekers (hogescholen en/of TO2 instellingen) samenwerken worden aangemoedigd.

Voor het vormgeven van een samenwerkingsproject gelden de volgende richtlijnen:

De subsidiepercentages die gehanteerd worden, zijn afhankelijk van de categorie onderzoek dat wordt uitgevoerd:

- Industrieel onderzoek: de maximale subsidie is 50%, met per project een minimum van € 100.000 en een maximum van € 500.000,= (dit betekent een maximale totale projectomvang van € 1.000.000,=).
  Experimentele ontwikkeling: maximaal 25% van de subsidiabele kosten, met per project een maximum van € 250.000,= (dit betekent een maximale totale projectomvang van € 1.000.000,=).
  Meer informatie over deze vormen van onderzoek vind je hier.
- Om deelname van Mkb-ondernemers te stimuleren wordt een opslag gegeven voor een samenwerkingsproject waar een Mkb-onderneming deel van uitmaakt: 10% extra subsidie voor Industrieel onderzoek en 15% extra subsidie voor Experimentele ontwikkeling.
- Het participerende bedrijfsleven moet minimaal 25% van de cofinanciering genereren.
- Cofinanciering kan zowel cash als in-kind worden gegenereerd, met voorkeur voor een deel cash bijdrage.
- Doorlooptijd van projecten is maximaal 3 jaar. Projecten dienen voor 01-12-2025 te starten en uiterlijk voor 31-12-2029 te zijn afgerond.

Voor de financiële inrichting van de projecten gelden verder de voorwaarden voor de TKI PPS innovatieregeling (zie Annex 1. Guide for Project Plan and Program Tender). In principe zullen de projectvoorstellen met een positief besluit door het betreffende TKI Bestuur in één keer voor het totale subsidiebedrag worden toegekend, binnen de grenzen zoals hierboven aangegeven.

7. Geldigheidsduur call for proposals

Deze call is geldig tot en met de uiterlijke sluitingsdatum **25 oktober 2024 (24.00 uur)**. Projecten kunnen tot deze deadline te allen tijde worden ingediend via cyberweerbaarheid@tki-energie.nl. Daarbij dient gebruik te worden gemaakt van de bijhorende formats (project template, begrotingsformat en template consortium agreement), welke niet aangepast mogen worden. Het beoordelingsproces voor alle ingediende voorstellen zal pas van start gaan na het verstrijken van de deadline.

8. Beoordeling en honorering

De beoordeling van de samenwerkingsprojecten wordt gebaseerd op een advies van een selectiecommissie bestaande uit experts uit de wetenschap en het bedrijfsleven uit de deelnemende Topsectoren en missieteams. Er wordt daarbij gestreefd naar een advies op basis van de beoordelingen en een evenredige balans van toegekende projecten over de verschillende Topsectoren heen. Het uiteindelijke besluit tot honorering/afwijzing zal gemaakt worden door het bestuur van de relevante Topsector.

De voorstellen worden beoordeeld op kwaliteit van onderzoek, innovativiteit en bijdrage aan de bovengenoemde innovatiethema's en kennis- en innovatie agenda's van de betreffende Topsectoren. Het beschikbare budget vanuit een bepaald TKI kan enkel ingezet worden als er een projectvoorstel wordt gehonoreerd met relevantie voor de innovatieagenda van de betreffende Topsector. Een advies voor een te honoreren project zal uiteindelijk voorgelegd worden aan het desbetreffende TKI voor de definitieve besluitvorming en toekenning, waardoor het betreffende consortium ook aan één TKI verantwoording dient af te leggen. Voor definitieve toekenning kan het betreffende TKI nog aanvullende informatie vragen.

Gehonoreerde projecten zullen tijdens de uitvoering verplicht worden deel te nemen aan minimaal jaarlijkse bijeenkomsten ten behoeve van kennisuitwisseling tussen de verschillende projecten binnen het CS4NL programma, naast de monitoringsverplichting vanuit het financierende TKI.

9. Samenwerkende Topsectoren

Nederland staat voor grote maatschappelijke uitdagingen: gezonder ouder worden, betaalbare zorg, zuinig omgaan met grondstoffen en natuur, minder uitstoot van broeikasgassen, betaalbare en duurzame energie, voldoende en gezond voedsel, een veilig Nederland om te wonen en te werken en meer digitale veiligheid. Het Missiegedreven Topsectoren en Innovatiebeleid (MTIB) is sinds 2023 gericht op vijf centrale maatschappelijke thema's:

Energietransitie;
Circulaire economie;
Gezondheid en zorg;
Landbouw, water en voedsel;
Veiligheid.

De maatschappelijke thema's vormen de basis voor vijf missiegedreven Kennis- en Innovatieagenda's (KIA's). Naast deze missie-KIA's zijn er drie dwarsdoorsnijdende KIA's. Dit zijn de KIA Sleuteltechnologieën (ST), de KIA Maatschappelijk Verdienvermogen (MV) en de KIA Digitalisering (D). De tien sterk ontwikkelde Topsectoren, dragen met hun kennis, onderzoek en ecosystemen bij aan de oplossingen voor de uitdagingen voor morgen (meer informatie: https://www.topsectoren.nl/missiesvoordetoekomst). Om deze grote maatschappelijke transities te faciliteren met behulp van onderzoek en innovatie is samenwerking van wetenschappers uit verschillende disciplines, overheden, bedrijven en maatschappelijke partijen noodzakelijk.

De Topsectoren hebben als doel het op structurele wijze stimuleren en realiseren van de publiek-private samenwerking op het vlak van onderzoek en ontwikkeling in deze sectoren. Dit betreft innovatie door middel van fundamenteel en toegepast onderzoek en de valorisatie en disseminatie van de kennis, ervaringen en resultaten. In deze call werken de Topsectoren Energie, Tuinbouw & Uitgangsmaterialen, Life Sciences & Health en ICT samen ten behoeve van toegepast onderzoek.

Cybersecurity voor Nederland (CS4NL) is een programma waarin alle topsectoren kennis en innovatie op het gebied van cybersecurity stimuleren. Het opereert binnen het kader van de KIA Digitalisering. CS4NL betreft de hele innovatieketen: wetenschappelijk en toegepast onderzoek, cybersecurity bedrijven, de industrie die cybersecuritytoepassingen in producten verwerkt én de private en publieke eindgebruikers. CS4NL beoogt door het bespoedigen van samenwerking via programmering van open en gerichte subsidieoproepen (calls) een substantiële impuls te geven aan cybersecurity-kennis en -innovaties in Nederland. Deze kennis en innovaties dienen bij te dragen aan oplossingen die maatschappelijke transities en de bijbehorende veilige digitale transformaties bespoedigen.[2]

10. Voorbeelden van uitdagingen binnen de Topsectoren

De onderstaande voorbeelden zijn bedoeld om een indruk te geven van de uitdagingen op het gebied van cybersecurity binnen de verschillende sectoren. Voorstellen zijn niet beperkt tot de onderstaande onderwerpen genoemd in de voorbeelden; ze dienen ter inspiratie voor mogelijke toepassingsgebieden in de projectvoorstellen voor industrieel onderzoek en/of experimentele ontwikkeling op het gebied van systeem- en ketenveiligheid.

Topsector Life Science & Health (Gezondheid & Zorg)

In de zorgsector vindt momenteel een aanzienlijke digitaliseringsslag plaats. Ziekenhuizen streven ernaar om zoveel mogelijk patiënten op afstand te monitoren en begeleiden. Zodoende vindt communicatie tussen zorgverlener en patiënt steeds vaker digitaal plaats. Deze ontwikkeling is ingezet om de zorg betaalbaar te houden en het hoofd te bieden aan het personeelstekort. Bovendien worden er voortdurend nieuwe digitale technologieën ontwikkeld voor diverse

[2] Informatie over andere thema's en activiteiten van het CS4NL, zie https://dcypher.nl/page/view/e0d6006e-c1b5-4816-9d52-bafe165dec2b/bgp-breed-gedragen-programma https://dcypher.nl/page/view/e0d6006e-c1b5-4816-9d52-bafe165dec2b/bgp-breed-gedragen-programma

toepassingen.

In de zorgsector wordt aan de zorgverlening kant een toenemende afhankelijkheid van digitale oplossingen waargenomen. Domotica-oplossingen worden steeds vaker ingezet. Bijvoorbeeld, slimme sloten en camera's helpen bij het voorkomen dat cliënten met dementie, hun woning verlaten. Thuiszorgmedewerkers maken ook steeds meer gebruik van slimme medicijndispensers, waardoor ze minder vaak controles ter plaatse hoeven uit te voeren. Belangrijke zorgtaken zijn dus steeds afhankelijker van digitale oplossingen, vaak gehost door gebruik te maken van cloudoplossingen. Het risico van deze afhankelijkheid werd recentelijk duidelijk toen een gehandicaptenzorginstelling werd getroffen door een DDoS-aanval die hun alarmsysteem verstoorde. Ook een cyber-incident bij Tunstall, een leverancier van alarmknoppen, zorgde ervoor dat alarmmeldingen van meerdere zorginstellingen niet doorkwamen. Veel van deze monitoringoplossingen worden geleverd door externe leveranciers die zowel de software, hardware als hosting verzorgen. Deze leveranciers zijn vaak op hun beurt afhankelijk van derden, waardoor een complex ecosysteem van afhankelijkheden ontstaat.

Naast de groeiende afhankelijkheid van digitale oplossingen voor monitoring en domotica, worden ook bedrijf kritische applicaties en elektronische patiënten/cliëntendossiers steeds vaker in de cloud gehost door leveranciers. In de GGZ, ouderenzorg, jeugdzorg en gehandicaptenzorg is er meestal een 'cloud tenzij'-beleid, waarbij de voorkeur wordt gegeven om een applicatie af te nemen in de cloud. Dit brengt echter ook een grotere afhankelijkheid van leveranciers met zich mee, waardoor een incident bij één leverancier vaak impact heeft op meerdere zorginstellingen.

Naast de veranderingen in de zorg zelf en de digitalisering, evolueert ook het dreigingslandschap. Cybercriminaliteit is geprofessionaliseerd en treft niet alleen zorginstellingen zelf, maar ook hun leveranciers. Dit kan variëren van datadiefstal tot gijzelsoftware, wat kan leiden tot ernstige verstoringen van de primaire zorgtaken. Ook vinden er door politieke spanningen de afgelopen 2 jaar steeds vaker DDoS-aanvallen plaats die ook impact hebben op zorginstellingen.

Topsector Energie

In de energiesector vindt een transitie plaats die het energiesysteem fundamenteel verandert. Grootschalige centrale opwek uit fossiele bronnen wordt aangevuld met meer decentrale opwek en verbruik. Nieuwe duurzame ketens van zonnevelden en windparken, evenals rond de laadinfrastructuur voor elektrische voertuigen, batterijsystemen en elektrolysers, worden aan het energiesysteem toegevoegd. Naast dat het systeem op technisch vlak meer complex wordt, komen er meer partijen in de keten. Ook gaan gebruikers -bewoners, ondernemers, grootverbruikers- zelf energie opwekken en terugleveren, wat grote impact heeft op energiestromen in het systeem. Systeemintegratie tussen energiedragers, bijvoorbeeld de conversie van elektriciteit naar groene waterstof, zorgt ook voor meer complexiteit, zowel in de specifieke ketens zelf als in het energiesysteem als geheel. De toenemende complexiteit en het grote aantal betrokken partijen, dragen bij aan een verhoogd cyberrisico zowel op keten- als systeemniveau.

Parallel aan de energietransitie vindt digitalisering plaats waardoor digitale en informatietechnologieën een centralere rol spelen in het energiesysteem. Een voorbeeld van een gedigitaliseerd energiesysteem op lokaal niveau is een ‘Smart Energy Hub’ waar ondernemers op een bedrijventerrein of bewoners in een energiegemeenschap onderling energie uitwisselen (tot nu toe voornamelijk elektriciteit). Een softwarematig Energie Management Systeem vormt de kern van de Hub en wordt gebruikt voor het meten, voorspellen en simuleren van opwek, opslag en verbruik, het geautomatiseerd aansturen van fysieke assets en het eventueel verhandelen van overtollige energie. Doordat besluiten over levering, opslag en verbruik van energie worden genomen door middel van voorgeprogrammeerde of zelflerende technologie brengt dat naast voordelen ook kwetsbaarheden met zich mee. Het systeem raakt in toenemende mate afhankelijk van de beschikbaarheid van data om goed te functioneren, bijvoorbeeld om een veilige balans tussen vraag en aanbod te creëren. Dit introduceert een kwetsbaarheid voor cyberaanvallen waarbij manipulatie plaatsvindt van de datastromen die in deze data-gedreven modellen worden gebruikt voor monitoring, voorspelling of aansturing. Doordat verschillende onderdelen meer verweven raken kan één probleem cascade veroorzaken, met mogelijk uitval in de energievoorziening tot gevolg.

Een andere systeemkwetsbaarheid ontstaat door de groei van het 'aanvalsoppervlakte' door een toenemend aantal gedistribueerde grid assets, 'grid-edge' apparaten en IoT-verbonden apparatuur met een hoger vermogen. Door hun (in)directe internetverbinding zijn al deze apparaten en assets kwetsbaar voor cyberaanvallen. Het gaat bijvoorbeeld om IoT-sensoren in elektriciteitsinfrastructuur of industriële installaties, maar ook om zgn. 'slimme' omvormers voor zonnepanelen, batterijsystemen, thermostaten, warmtepompen, EV-laadpunten. Ook zijn Energie Management Systemen in opkomst (op verschillende schaalniveaus) die deze apparaten en assets met elkaar verbinden en aansturen, en dus toegang hebben tot grotere vermogens. Een cyberaanval op groot aantal van dergelijke gedistribueerde apparaten, waarbij ze gecoördineerd aan- of uitgezet worden, zorgt voor een plotselinge verandering in de netbelasting met mogelijke uitval van de stroomvoorziening tot gevolg (zgn. 'load altering attacks'). Door een toenemend aandeel van wind en zon in de elektriciteitsmix neemt de netstabiliteit en daarmee de tolerantie voor dit soort 'load altering' aanvallen af, met toenemend risico op blackouts. Omdat duurzame energieketens vaker gedistribueerd zijn, is het bovendien moeilijk om de locatie van een kwetsbaarheid te achterhalen en een oplossing te implementeren om schade te beperken.

Topsector Tuinbouw en Uitgangsmaterialen

Als het gaat om voedselvoorziening staat ook Nederland voor grote uitdagingen. Voedselzekerheid zoals wij deze al jaren gewend zijn is niet zomaar meer een gegeven. Invloeden van buitenaf zorgen steeds vaker voor een disruptie van de supply chain wat leidt tot lege schappen. Een van de disrupties kan ontstaan door het "ontregelen" van de informatiesystemen, besturingssystemen, bij schakels en in de keten. Denk aan de kas, het koelhuis, bewerkings- en of pakstations en informatiesystemen voor handel, logistiek etc. Alhoewel bloemen & planten geen voedsel zijn is het economisch belang voor Nederland dusdanig dat een disruptie van deze ketens ook grote gevolgen heeft.

> UIT DE PRAKTIJK
> Op 11 april 2024 werd het geautomatiseerde warehouse in Zaandam van Albert Heijn getroffen door een stroomstoring van een uur. Ruim tien dagen later zorgt het euvel nog altijd voor lege schappen in veel winkels in het land. Een op het eerste oog kleine disruptie in deze volledige gedigitaliseerde keten van aanvoer, bestellen, distributie en toelevering werd vrijwel volledig ontregeld door het plan gaan van diverse informatiesystemen t.g.v. geen stroom. Een "kabelbreuk" werd niet digitaal herkend waardoor alle systemen platgingen. Een scenario wat identiek zou zijn aan een inbreuk in de informatiesystemen in de digitale voedselketen.

Onder de keten van Tuinbouw & Uitgangsmaterialen verstaan we alle stappen inclusief de toelevering van kas tot kassa of van veld tot perk. Hiervoor is een grote digitale infrastructuur actief. Hierbij zijn we ook afhankelijk van andere cruciale ketens zoals aardgas, elektriciteit en water.

Deze onderzoek uitvraag richt zich op het verbeteren van de digitale veiligheid en weerbaarheid in de hele Tuinbouw & Uitgangsmaterialenketen en het gehele systeem dat vitale diensten en producten voortbrengt. Kennisontwikkeling kan zich richten op:

1. **Identificeren en aanpakken**: In de Tuinbouw & Uitgangsmaterialen keten- als op systeemniveau in de schakels, bedrijven zoals veredelingsbedrijven, telers, verpakkers, verwerkers, bestaan complexe en dynamische afhankelijkheden. Het gaat om complexe teeltsystemen, leveranciers van "inputs" zoals planten, mineralen etc., maar ook om diverse actoren rondom verpakking, handel, afzet en export. Hierin vind frequent real-time overdracht van teeltdata en voorraden plaats. Oplossingen die risico's en knelpunten in deze overdrachten identificeren zijn benodigd. Bijvoorbeeld smart zelfscans voor teeltsystemen, handelsapplicaties, etc. Ook moeten digitale afhankelijkheden in de sector beter bekend worden om er vervolgens tools voor te ontwikkelen om deze risico's te monitoren en adequaat risico's in te schatten en ze

vervolgens te beperken. Denk aan de interactie tussen diverse applicaties in de kas, in het pakstation en tussen actoren of systemen in de keten.

2. **Delen**: De tuinbouwketen is veranderd van "een groene vinger" gestuurde productie in kas en op het veld, in de loodsen en pakstations naar een data gestuurde keten. Oplossingen die bijdragen aan het scheppen van een preventief kader en lerende keten met samenwerking en kennisdeling tussen ketenpartijen. incl. oplossingen voor het beter ontsluiten van informatie op ketenniveau. Dit is inclusief het veilig gebruik van steeds grotere hoeveelheden data. Denk aan data delen in de keten van teelt naar retailer. Maar ook aan het delen van data tussen kasklimaat, sensoren en teelt beslissingsondersteunende systemen.
3. **Simuleren:** Voor training, awareness en risicoanalyse zijn simulaties essentieel. Deze simulaties bevatten de diverse actoren in tuinbouw zoals sensoren, besturingssystemen en bedrijfsinformatiesystemen en hierbij automatisch indicatie van risico's inschatten en valideren. Hierdoor creëren van een digital agent voor verbeteren van de cyberweerbaarheid in de keten.
4. **Detecteren:** Het ontdekken van signalen die duiden op afwijkingen in IT, OT en IoT-omgevingen (integrale anomalie-detectie). Hierbij betreft het:
   > Regelsystemen/ besturing in de kas;
   > Regelsystemen/ besturing in equipment incl. robot(platforms);
   > Regelsystemen voor verpakken, bewerken, snijden etc.;
   > Regelsystemen/ besturing voor koelen/ bewaren:
   > Sensor(netwerken incl. vision);
   > Keteninformatiesystemen en handelsplatvormen;
   > etc.
5. **Reageren en herstellen:** Oplossingen en maatregelen die bijdragen aan het herstelvermogen van ketens en systemen na een cyberaanval. Hierbij gaat het om zowel automatische response als gecontroleerde informatievoorzieningen, beslissingsondersteunende systemen, die helpen bij een adequate response door ketenschakels inclusief het informeren van andere schakels in de keten voor mogelijke betrokkenheid bij een inbreuk.

Hierbij kan generiek worden gedacht aan de inzet van digitale en informatietechnologieën en innovatieve digitale oplossingen, evenals innovatie op het gebied van samenwerking.