TKI Call for Proposals

Cyber resilience for critical chains and systems in Energy, Life Sciences and Health and Horticulture & Starting materials

Call for proposals

Health~Holland
SHARED CHALLENGES, SMART SOLUTIONS

TOPSECTOR
TUINBOUW & UITGANGSMATERIALEN

TOPSECTOR
ICT
dutch digital

topsector
energie

1. Context

Cyber security is about the set of measures to prevent damage caused by disruption, failure or misuse of electronic data and computers. The damage can be intentional as a result of a cyber-attack but may have unintended origins, such as a malfunction in software (updates), human error or a combination thereof. Cyber resilience includes not only the prevention of damage but also “the ability to respond to a cyber-attack and repair any damage.” In this funding call, we use the term cyber resilience as we are seeking solutions to both prevent cyber incidents and - if incidents do occur - to detect them, mitigate damage and facilitate recovery.

Cyber resilience is a precondition for the safe and future-proof functioning of Dutch society, which is rapidly digitalizing. Cyber resilience is consequently of great importance for chains and systems in the Energy, Health & Care and Horticulture sectors as building blocks of Dutch society and economy. The importance and urgency of these issues are now being recognized. The theme of this funding call, therefore, holds an invaluable position in the Mission Driven Top Sectors and Innovation Policy, as one of the seven digital key technologies within Top Sector ICT and KIA Digitalization. The cross-over of knowledge between the aforementioned sectors and digitalization is a prerequisite for strong cyber resilience in the chain and the systems used in it.

The importance and impact of digitalization, the complexity of the associated new solutions and the improvement and integration of existing products necessitate multidisciplinary collaboration; (Top) cross-sector and across the ecosystem.

Within the Cybersecurity for the Netherlands (CS4NL) program, the Top Sectors collaborate to enhance knowledge and innovation in the field of cyber resillience. This call, focused on the theme of system and chain resilience, was created within CS4NL, in collaboration with the Top Sectors Energy, Horticulture & Starting Materials, Life Sciences & Health and ICT. Project proposals must focus on at least two of these Top Sectors. The call also allows for meta-projects across multiple sectors.

2. Call for Proposals: Cyber resilience for critical chains and systems in Energy, Life Sciences and Health and Horticulture and Starting Materials

This funding call is focused on developing knowledge and innovations for improving digital security and resilience across the entire chain and system that produces vital services and products within the aforementioned Top Sectors.

Critical chain, in this context, refers to the total of activities and connections from the source to the end user. Examples of such chains are:

- The production, cultivation, packing, sorting, trading of, for example, tomatoes for the fresh market.
- The production, transmission, storage, conversion, distribution and consumption of various forms of energy such as electricity, heat, fuels and gas.
- The chain of health and care information between healthcare professionals, cloud services and providers and the home environment.

A system denotes a process or part of the chain-for example, the power plant, greenhouse, hospital, etc.

Given that chains and their management are increasingly digitalizing, and IT (products and services) are decreasing, it is no longer appropriate to consider chains rectilinear. Rather, they are complex ecosystems. This makes it challenging to gain insight into the composition and functionality of “the chain". Consider, for example, the party behind a supplier that stores data or supplies the software for an asset management portal. Dependencies between chain parties are increasing due to the interconnection of information systems or the use of hardware or software from the same supplier. In critical services (for example, energy supply), digital and information technologies are used to monitor, simulate, predict and control systems or to support advice and decision-making. There is a tremendous growth in data collection and exchange, with data-driven methods (such as machine learning algorithms) taking an integral role in analyzing data streams and intervening (automatically) based on them. As a result, there is a growing dependence on third-party providers of critical IT. The failure or poor/erroneous functioning of systems and services they provide can cause disruptions. This could be due to a targeted cyber attack but may equally be an unintended disruption caused by personnel or software (update) errors. The more complex digital chains and related interdependencies between chain parties pose a system-level hazard as the security of supply of vital processes, healthcare, energy, food is compromised.

An additional vulnerability arises from the growth of the so-called "attack surface" due to an increasing number of distributed links in chains, such as inverters for household solar panels, smart healthcare equipment and automated greenhouses. A cyber-attack on one of these chains' causes, among other things, failure, disruption and possibly theft of personal or business-sensitive data.

3. Innovation themes

This grant call focuses on R&D activities that are oriented toward technological development. These activities comprise either industrial research or experimental development. Industrial research is defined as planned research aimed at acquiring new knowledge and skills for the development of new products, processes or services, or for the significant improvement of existing products, processes or services. We define experimental development as the acquisition, combination, shaping and use of existing scientific, technological, business and other relevant knowledge and skills, aimed at developing new or improved products, processes or services. Activities that focus solely on knowledge development on social sciencerelated matters do not fit within this grant call. Similarly, implementation research of already developed products, processes or services does not fit within the framework of this call.

System and chain resilience is a comprehensive concept. To differentiate areas of interest, a description is provided below in five areas. In terms of content, the projects should develop knowledge and innovations in one or more of the areas below. In all cases, special attention is requested for making relatively expensive technologies accessible to SMEs.

1. **Identify and address:** Owing to the complex and dynamic dependencies at the chain and system level, innovative techniques are needed to improve visibility into how the critical chains and systems in the aforementioned sectors are put together, where dependencies exist, and what cyber risks arise from them. This area of emphasis focuses on identifying and monitoring such risks and developing interventions to act on them. An example of a risk is the dependence on third-party software, which creates the need to identify and monitor the impact of a vulnerability in this type of software. Another example involves cloud infrastructure where it is known that the underlying hardware, software and configurations have the potential to be vulnerable. The same applies to vendor IoT devices and sensors, whose data can be stolen or manipulated. More generically, smart methods and tools to identify and monitor these types of risks (e.g., smart self-scans, pen tests) could be considered. In addition to identification and monitoring, there is a need to directly reduce the attack surface in critical chains or systems through interventions. For example, through new ways to generate and implement chain-wide intelligent security patches. New decentralized system designs may also be a solution. New methods should enable sectors to determine and act on the (optimal) digital security of (components of) a chain or system.
2. **Sharing:** Data has emerged as one of the most valuable resources. Critical chains and systems generate significant amounts of sensitive data. At the chain level, where different parties work closely together, disclosure of data and information in a transparent and secure manner is essential. Interoperability of the underlying systems is a prerequisite for this. How can we develop encrypted databases that can connect different types of data? How can we prevent data-driven decision-making from outside influence? How can we design computations in a way that minimizes the need to share sensitive data? Can we apply verifiable computing and cryptographic techniques? How do we make parts of the chain interoperable in a secure way?
3. **Simulate:** To raise awareness of the effects that poor resilience has in the chain and/or train how to respond in an incident, it is essential to train employees. Developing simulation models is important here, as is creating the simulation experience. What models can be developed for simulation? What types of data are needed for this? What technology is suitable for simulating an incident or detected risk?
4. **Detect:** It is critical, when a cyber attack occurs, to detect it as soon as it occurs. This requires detecting signals that indicate anomalies in IT, OT and IoT environments. This can include, for example, detecting interception or manipulation of data streams used in critical operational systems or within chains. Research can also focus on the detection of malware within chains. Detection by machine learning algorithms seems to hold promise but requires further development. Can we use these algorithms not only to map the complexity of chains, that is, to ensure timely detection of attacks? What data (sources) are needed for this, prior to and during an incident? How do we continuously evaluate software vulnerability? Can techniques such as federated learning help assess and mitigate risk in distributed systems?
5. **Respond and recover:** Finally, projects can focus on solutions and measures that contribute to the resiliency of chains and systems after a cyberattack. This could include, for example, improving system

resilience against load altering attacks. Not only recovery is important here, but also early discovery of the cause (relationship to the detect focus area).

Illustrative examples for the Top Sectors Horticulture & Starting Materials, Energy, and Life Science & Health have been developed at the bottom of this document (item 9) to give an impression of the sectoral challenges and R&D needs.

4. Available budget

The total available budget for this call is €2,500,000. The available budget will be deployed from the TKI PPP Innovation Scheme by TKI Energy, TKI T&U (Horticulture & Starting Materials), TKI Life Sciences & Health (Health~Holland) and TKI ICT, if consistent with the relevant knowledge and innovation agendas and implementation programs.

5. Terms and conditions for collaborative projects

Public-private partnership projects are projects carried out by a partnership (consortium) of companies and knowledge institutions. The minimum size of a consortium is one knowledge institution and one company. Consortia in which universities and practice-oriented researchers (colleges and/or TO2 institutions) work together are encouraged.

The following guidelines apply to shaping a collaborative project:

- The subsidy percentages used depend on the category of research being carried out as described below. More information on these forms of research can be found here
    - Industrial research: the maximum grant is 50%, with a minimum of €100,000 and a maximum of €500,000 per project (this means a maximum total project size of €1,000,000).
    - Experimental development: a maximum of 25% of the eligible costs, with a maximum of € 250,000 per project (this means a maximum total project size of € 1,000,000).
- To stimulate participation of SMEs, a bonus is given for a collaborative project in which an SME is part of: 10% extra subsidy for Industrial Research and 15% extra subsidy for Experimental Development.
- The participating industry must generate at least 25% of the co-financing.
- Co-financing can be generated both cash and in-kind, with a preference for a partial cash contribution.
- Duration of projects is maximum 3 years. Projects should start before 01-12-2025 and be completed by 31-12-2029 at the latest.

The financial design of the projects is subject to the conditions of the TKI PPP innovation scheme (see Annex 1. Guide for Project Plan and Program Tender). In principle the project proposals with a positive decision by the relevant TKI Board will be awarded at once for the total subsidy amount, within the limits indicated above.

6. Validity period call for proposals

This call is valid until the final closing date of October 25, 2024 (midnight). Projects can be submitted at any time up until this deadline via cyberweerbaarheid@tki-energie.nl. The accompanying templates (project template, budget template and template consortium agreement) must be used, which may not be modified. The evaluation process for all submitted proposals will not start until after the deadline.

7. Assessment and awarding

The assessment of the collaborative projects will be based on a advice from a selection committee consisting of experts from science and business from the participating Top Sectors and mission teams. The aim is to provide an advice based on the assessments and a proportionate balance of awarded projects across the different Top Sectors. The final decision will be made by the involved Top Sectors directive board.

The proposals will be assessed in terms of quality of research, innovativeness and contribution to the above innovation themes and knowledge and innovation agendas of the relevant Top Sectors. The budget available from a particular TKI can only be allocated to project proposals that are relevant within the innovation agenda of this Top Sector. A recommendation for a project to be awarded funding will ultimately be submitted to the TKI in question for final decision making and awarding, whereby the consortium in question must, in addition, render account to a single TKI. Additional information may be requested by the TKI in question prior to definitive allocation.

During the execution, awarded projects will be required to participate in yearly meetings aimed at mutual knowledge exchange between the various projects within the CS4NL program, in addition to the monitoring obligation from the funding TKI.

8. Samenwerkende Topsectoren

The Netherlands faces major societal challenges such as: healthy aging, affordable care, economical use of raw materials and nature, reduced greenhouse gas emissions, affordable and sustainable energy, sufficient and healthy food, a secure Netherlands to live and work in, and increased digital security. The Mission-Driven Top Sectors and Innovation Policy (MTIB) has focused on five central societal themes since 2023:

- Energy transition;
- Circular economy;
- Health and care;
- Agriculture, water and food;
- Safety.

The societal themes form the basis for five mission-driven Knowledge and Innovation Agendas (KIAs). In addition to these mission KIAs, there are three cross-cutting KIAs. These are the KIA Key Technologies (ST), the KIA Social Earning Capacity (MV) and the KIA Digitalization (D). The ten highly developed Top Sectors, contribute with their knowledge, research and ecosystems to the solutions for tomorrow's challenges (more information: https://www.topsectoren.nl/missiesvoordetoekomst). To facilitate these major societal transitions with the help of research and innovation, cooperation of scientists from different disciplines, governments, businesses and societal parties is necessary.

The Top Sectors aim to structurally encourage and realize public-private research and development cooperation in these sectors. This concerns innovation through fundamental and applied research and the valorization and dissemination of the knowledge, experiences and results. In this call, the Top Sectors Energy, Horticulture & Starting Materials, Life Sciences & Health and ICT collaborate to promote applied research.

Cybersecurity for the Netherlands (CS4NL) is a program in which all top sectors foster knowledge and innovation in the field of cybersecurity. It operates within the framework of the KIA Digitalization. CS4NL involves the entire innovation chain: scientific and applied research, cybersecurity companies, the industry that incorporates cybersecurity applications into products as well as private and public end-users. CS4NL aims to substantially advance cybersecurity knowledge and innovations in the Netherlands by accelerating collaboration through programming open and targeted funding calls. Such expertise and innovations should contribute to solutions that accelerate societal transitions and associated secure digital transformations.

9. Examples of challenges within the participating Top Sectors

The examples below are intended to provide an impression of cybersecurity challenges within different sectors. Proposals are not limited to the topics mentioned in the examples below; they serve as inspiration for possible application areas in the project proposals for industrial research and/or experimental development in the field of system and chain security.

Topsector Life Science & Health

A significant digitalization effort is currently taking place in the healthcare sector. Hospitals are striving to monitor and assist patients remotely as often as possible. As a result, communication between care provider and patient is increasingly taking place digitally. These developments are necessary to keep healthcare affordable and to cope with staff shortages. Moreover, new digital technologies are constantly being developed for various applications.

In the healthcare sector, an increasing reliance on digital solutions can be observed on the care delivery side. Home automation solutions are increasingly being used. For example, smart locks and cameras help prevent clients with dementia, from leaving their homes. Home care workers are also increasingly using smart medication dispensers, reducing the need for on-site checks. Important care tasks are accordingly increasingly dependent on digital solutions, often hosted using cloud solutions. The inherent danger of this dependency was recently demonstrated when a disability care facility was hit by a DDoS attack that disrupted their alarm system. Similarly, a cyber incident at Tunstall, a provider of alarm buttons, caused alarm notifications from multiple healthcare facilities to fail. Many of

these monitoring solutions are provided by third-party vendors who provide both software, hardware and hosting. These vendors, in turn, often depend on third parties, creating a complex ecosystem of dependencies.

In addition to the growing reliance on digital solutions for monitoring and home automation, business critical applications and electronic patient/client records are increasingly being hosted in the cloud by vendors. In the mental health care, elder care, youth care and disability care sectors, there is usually a "cloud unless" policy, where preference is given to cloud applications. This, however, creates a great dependence on vendors to supply to several parties, meaning an incident at one vendor often impacts multiple healthcare organizations.

Aside from the changes in healthcare itself and digitalization, the threat landscape itself is also evolving. Cybercrime has professionalized greatly and affects not only healthcare institutions themselves, but also their suppliers. This can range from data theft to hostage software, leading to serious disruptions to primary care tasks. Moreover, due to political tensions, DDoS attacks have been increasingly taking place over the past 2 years, which has impacted healthcare facilities.

Topsector Energy

In the energy sector, a transition is taking place that is fundamentally changing the energy system. Large-scale centralized generation from fossil sources is being supplemented by more decentralized generation and consumption. New sustainable chains of solar fields and wind farms, as well as a battery charging infrastructure for electric vehicles, battery systems and electrolysers, are being added to the energy system. In addition to the system becoming more technically complex, more parties are entering the chain. Furthermore, users -residents, entrepreneurs, large consumers- will generate their own energy and supply it back, which will have a major impact on energy flows in the system. System integration between energy carriers, for example the conversion of electricity to green hydrogen, is also adding complexity, both in the specific chains themselves and in the energy system as a whole. The increasing complexity and the large number of parties involved, contribute to increased cyber risk at both the chain and system levels.

Parallel to the energy transition, digitalization is taking place through which digital and information technologies are assuming a more central role in the energy system. An example of a digitalized energy system at the local level is a "Smart Energy Hub" where entrepreneurs in a business park or residents in an energy community exchange energy among themselves (so far mainly electricity). A software-based Energy Management System forms the core of the Hub and is used to measure, predict and simulate generation, storage and consumption, automatically control physical assets and trade surplus energy if necessary. Given that decisions about supply, storage and consumption of energy are made through pre-programmed or self-learning technology, which introduces both vulnerabilities and benefits. The system becomes increasingly dependent on the availability of data to function properly, for example to create a secure balance between supply and demand. In turn, this introduces a vulnerability to cyber-attacks involving manipulation of the data streams used in these data-driven models for monitoring, prediction or control. As different components become more intertwined, one problem can cascade, potentially causing outages in energy supply.

Another system vulnerability arises from the growth of the "attack surface" due to an increasing number of distributed grid assets, "grid-edge" devices and higher-power IoT-connected devices. By virtue of their (in)direct Internet connection, all of these devices and assets are vulnerable to cyber-attacks. These include, for example, IoT sensors in electricity infrastructure or industrial plants, but also so-called 'smart' inverters for solar panels, battery systems, thermostats, heat pumps, EV charging points. Energy Management Systems have also emerged (at various scales) that connect and control these devices and assets, thus accessing larger capacities. A cyber-attack on large number of such distributed devices, turning them on or off in a coordinated manner, creates a sudden change in grid load resulting in potential power outages (so-called load altering attacks). With an increasing share of wind and solar in the electricity mix, grid stability and thus tolerance for these types of load altering attacks is decreasing, with increasing risk of blackouts. Moreover, because renewable energy chains are more often distributed, it is challenging to identify the location of a vulnerability and implement a mitigation solution.

Top Sector Horticulture and Starting Materials

When it comes to food supply, the Netherlands is also faced with major challenges. Food safety the likes of which we have been accustomed to for years is no longer a given. External influences increasingly disrupt the supply chain leading to empty shelves. One of the disruptions can occur by "disrupting" information systems, control systems, at links and in the chain. Think of the greenhouse, cold store, processing and or packing stations and information

systems for trade, logistics etc. Although flowers & plants are not food, their economic importance to the Netherlands is of such magnitude that a disruption of these chains has major consequences.

> RECENT EXAMPLE
> On April 11, 2024, Albert Heijn's automated warehouse in Zaandam was hit by a one-hour power outage. Over ten days later, the fault was reportedly still causing empty shelves in many stores around the country. A seemingly minor disruption in this fully digitalized chain of supply, ordering, distribution and delivery was almost completely disrupted by the plan going of various information systems due to no power. A "cable break" was not digitally recognized causing all systems to go down. A scenario that would be identical to a breach of information systems in the digital food chain.

The horticultural & Horticultural Materials chain means all steps including supply from greenhouse to cash register or from field to flowerbed. This involves a large digital infrastructure. This process is also highly dependent on other crucial chains such as natural gas, electricity and water.
The present research challenge focuses on improving digital security and resilience throughout the Horticulture & Horticulture & Horticulture Supply Chain and the entire system that produces vital services and products. Knowledge development can focus on:

1. **Identify and address**: Complex and dynamic dependencies exist in the Horticulture & Starting Materials chain- as at system level in the links, companies such as breeding companies, growers, packers, processors. These include complex cultivation systems, suppliers of "inputs" such as plants, minerals, etc., as well as various actors around packaging, trade, marketing and export. In these, frequent real-time transfer of cultivation data and stocks takes place. Solutions that identify risks and bottlenecks in these transfers are needed. For example, smart self-scans for cultivation systems, trade applications, etc. Digital dependencies in the sector must also be more widely recognized in order to subsequently develop tools to monitor and adequately assess these risks and consequently mitigate them. Consider the interaction between various applications in the greenhouse, at the packing station and between actors or systems in the chain.
2. **Sharing:** The horticultural chain has changed from "a green finger" controlled production in greenhouse and field, in sheds and packing stations to a data driven chain. Solutions that contribute to the creation of a preventive framework and learning chain with cooperation and knowledge sharing between chain parties. incl. solutions for improved access to information at the chain level. This includes the secure use of increasing amounts of data. Think of data sharing in the chain from cultivation to retailer. This includes sharing data between greenhouse climate, sensors and cultivation decision support systems.
3. **Simulate:** For training, awareness and risk analysis, simulations are essential. These simulations incorporate the various actors in horticulture such as sensors, control systems and business information systems, and in doing so automatically estimate and validate indication of risk. This creates a digital agent for improving cyber resilience in the chain.
4. **4. Detecting:** Detecting signals that indicate anomalies in IT, OT and IoT environments (integral anomaly detection). This involves:
   > Control systems/controls in the greenhouse;
   > Control systems/control in equipment including robot(platforms);
   > Control systems for packaging, processing, cutting, etc.;
   > Control systems for cooling/storage:
   > Sensor (networks incl. vision);
   > Chain information systems and trading platforms;
   > etc.
5. **Respond and recover:** Solutions and measures that contribute to the recovery capability of chains and systems after a cyber-attack. This includes both automatic response and controlled information facilities, decision support systems, that help in adequate response by chain links including informing other links in the chain for possible involvement in a breach.

Generally, this can include the use of digital and information technologies and innovative digital solutions, as well as innovation in collaboration.