Top Sectors combine capabilities for cybersecurity innovation in CS4NL

The Hague, 19 October 2022 – CS4NL, formerly the Broadly Supported Programme for Cybersecurity, brings together the innovative capabilities in the field of cybersecurity of all the various Dutch Top Sectors. The programme will address cybersecurity issues arising in connection with major societal transitions and organise efficient partnership chains to deal with them. The purpose of CS4NL is to improve cybersecurity awareness and innovation, by bringing together the supply and demand for specific issues, organising an ecosystem that extends across the entire commercialisation chain, and freeing up new financial resources from existing innovation instruments. “The overall goal of CS4NL goes beyond simply improving the cyber defences of Dutch organisations: instead, the effect will be a stronger Dutch economy and a more competitive position in the world at large,” explains Topsector ICT’s director Frits Grotenhuis. CS4NL will have a 5-year budget estimated at 27-36 million euros.

Partners in seven demand-driven themes

CS4NL will address seven demand-driven cyber-related themes in the major societal transitions facing the Netherlands: the energy transition, mobility innovation, and safe ways to move medical care to the home, for example. Each CS4NL theme is related to the cybersecurity issues facing two or more Top Sectors. The themes are security by design; secure data-driven work forms; secure connectivity; OT/IT security; cyber risk management; system and supply chain security; and cyber awareness, expertise and skills. dcypher director Eddy Boot explains, “For all these themes, we first investigated the possibilities for drawing on existing expertise and technology. Unfortunately, those proved unavailable: so much expertise and technology is still lacking, and existing concepts can’t be applied to specific transitions at this point. That’s what we’re going to remedy now.”

From themes to investing in expertise and innovation

For each of the themes, calls will go out for scientific and academic research. Knowledge institutions can submit their proposals, forming partnerships with companies, government agencies and social organisations. The idea is to reinforce the Dutch cybersecurity knowledge base. In-depth practical problem-solving cases, or “use cases”, have also been defined for each of the themes. These will serve as a point of reference for the various Top Sectors to issue calls for more specific innovation proposals, again from broadly composed consortiums.

So far, twelve cases have been defined, including secure digitalisation of remote patient care; assurances for the accuracy of sensor data from wind farms to ensure safe maintenance and security of the energy supply; improved understanding of the ever-more complex IT and OT systems and networks necessary for sectors of society such as energy, water management and horticulture; and cyber defences of smaller companies in sectors of the economy such as logistics. CS4NL expects to start issuing the theme-based calls for research and innovation use cases in 2023.

The importance of cybersecurity

Reliable and secure digitalisation is a key factor in the societal transitions facing the Netherlands. This makes cybersecurity one of the parameters for a responsible and future-proof functioning society in the Netherlands and for the country’s economic growth. That digital defences are both vital and urgent is widely acknowledged, reinforced by developments such as the frequency of ransomware attacks and the war in Ukraine. As a result, the topic has been included in the Mission-Driven Top Sectors and Innovation Policy.

Strong foundations
CS4NL is based on a broad ecosystem that extends to all ten Top Sectors. It also includes the organisations behind them, having been set up with the help of end users such as the Academic Cyber Security Society (ACCSS), the higher professional education sector, the Dutch Research Council, independent research organisation TNO, Cyberveilig Nederland (which promotes cyber awareness in the business community), Regional Development Companies (acting through Innovation Quarter) and the Dutch Ministry of Defence. The Ministries of Economic Affairs and Climate Policy and of Justice and Security are also involved, represented by the Security Knowledge and Innovation Agenda. The programme is an initiative of Topsector ICT and dcypher, as part of the Key Enabling Technologies Knowledge and Innovation Agenda.

Note to the editors

About Topsector ICT
Topsector ICT identifies, prioritises and organises ICT research and innovation. It does this by bringing together public and private operators whose focus is on ICT key enabling technologies and societal challenges. Its involvement covers the entire process, from fundamental research up to and including commercialisation. Training emerging talent, reskilling, upskilling, knowledge dissemination, a broad involvement of the SME sector and international alliances are all important features of Topsector ICT's mission. www.dutchdigitaldelta.nl

About dcypher
dcypher is the platform for partnerships in research and development in all matters concerning cybersecurity in the Netherlands. dcypher facilitates between companies, knowledge institutions and government agencies in search of partners to improve the security, strength and autonomy of the Dutch digital environment. dcypher brings together partners, funding and expertise for translating research into effective applications, training cybersecurity professionals at the highest level and improving cybersecurity expertise in the Netherlands. www.dcypher.nl

Further information
Tessa Weber
PR and Communications Adviser, Topsector ICT
E: tessa.weber@dutchdigitaldelta.nl
T: +316 1415 5898

Marcel Ruijken
Communications Adviser, dcypher
E: marcel.ruijken@dcypher.nl
T: +316 5436 2331