Research, Innovation
and Education for
Cyber Defence and Security

CYBERCAMPUS SWEDEN

Why Cybercampus?

If our digital infrastructures are not secure, then most functions of our society are at risk.

Cybersecurity is of utmost importance for Sweden today and increasingly so, as the digitalization continues. Unfortunately, building and operating secure systems has turned out to be a formidable challenge. The consequence of weak security is increased demand on the cybersecurity workforce. Very high skill-levels are required to defend the remarkably vulnerable systems that constitute society's digital infrastructures.

The solutions to these problems consist of developing better tools and methods for secure system design and operation, and training of the workforce. Both solutions must be based on continuous research and innovation.

A surprisingly large number of organizations are involved in the defence of the Swedish cyberspace. This fragmentation stretches into higher education and research where uncoordinated research groups are distributed over universities and institutes across the country.

Other European countries, e.g., Norway, Switzerland, France and Germany, have addressed the fragmentation problem by establishing national hubs for cybersecurity research, innovation and education, sometimes called Cyber Campuses. We believe that there is a need for a Swedish Cyber Campus where cybersecurity researchers, practitioners and stakeholders collaborate.

Cybercampus Sweden will conduct joint research and innovation, offer cybersecurity education, coordinate EU participation in research projects, act as a competent body of expertise for Swedish decision makers and increase Sweden's international visibility. The campus will constitute a national research infrastructure and be organized as a joint venture between several universities, research institutes, government agencies and companies across Sweden.

Sigbritt Karlsson
President, KTH

Pia Sandvik
CEO, RISE

Micael Bydén
Chief Commander
Swedish Armed Forces

A critical need for research, innovation and education

Recent cybersecurity attacks have taught us that it is effectively impossible to build and maintain secure software systems.

Consider the major operating systems, which are fundamental building blocks of our digital infrastructure. These systems are developed by the world's largest enterprises, employing many of the most talented software and security experts. Despite all their competence, these companies release security updates every month, typically reporting several dozens of newly discovered vulnerabilities, of which many are critical. This remarkable, persistent security failure manifests how hard the problem of developing secure software systems really is.

According to a recent study, Europe is currently understaffed by close to 200,000 cybersecurity professionals.

Source: (ISC)^2 Cybersecurity Workforce Study, 2021

When a problem is too difficult for humans to solve, technology oftentimes comes to the rescue. This is also the case in software development and operation: We need more secure programming languages, network protocols, development platforms, testing methods, system administration and security operations tools. There is no other way to overcome the security challenges that currently endanger our digital infrastructure. New tools and methods are the products of scientific research and innovation. Alas, research efforts in cybersecurity have not kept pace with the rapid progress of digitalization. And Swedish innovation advances in cybersecurity lag those of games, media, finance, health and education.

To compensate for the lack of secure technologies and procedures, an exceptionally competent cybersecurity workforce is required. But, even organizations employing the most competent and well-resourced cybersecurity experts fail to secure their systems. For the many organizations that are less skilled, the situation is even more precarious. The magnitude of this cybersecurity problem has resulted in a worrisome workforce gap. According to a recent study, Europe is currently understaffed by close to 200,000 cybersecurity professionals.

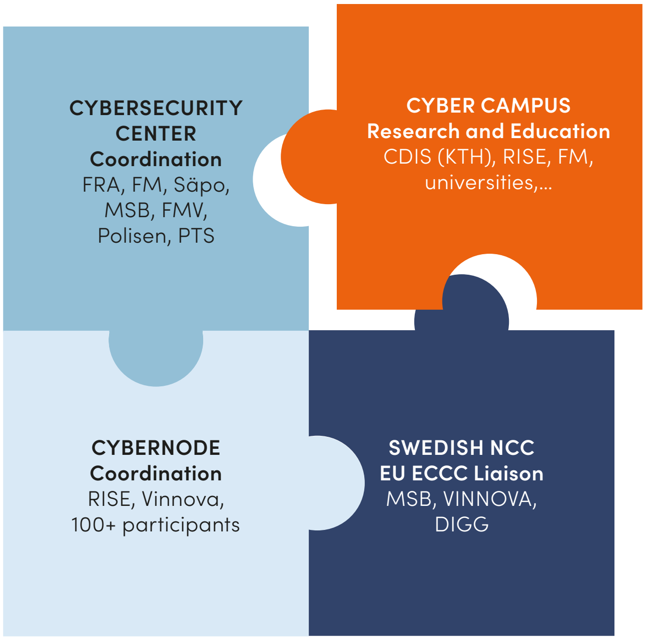
Unfragmented research, education and innovation

A large number of government agencies share responsibility for defending the Swedish cyber space. Notably, these organisations often do not build or operate Sweden's critical digital infrastructure; that work is mainly performed by a multitude of private sector companies, who are equally important for defending Swedish cyber space. The fragmentation of responsibilities is not limited to the development and operation of today's digital infrastructure, but it extends into cybersecurity research, innovation and education.

The current Swedish cybersecurity research effort consists of small and medium-sized research groups across the country with limited collaboration. It is therefore difficult to gain the momentum needed for addressing challenges on national and international levels and for establishing and maintaining infrastructures, such as cyber ranges, compute resources, and quantum computers. The lack of collaboration inhibits innovation, since the required resources and personnel to engage in entrepreneurship are oftentimes not available. With respect to education, no academic institution has all the competences and staff required for a comprehensive cybersecurity education program and for high-volume continuous education. The fast dynamics of cyberspace clash against the pace of organizational change in universities, making it difficult to respond to rapidly changing demands in society. The aim is however not to replace but to complement current academic activities by providing a cross-university structure that meets urgent cybersecurity needs in agile education, joint research and disruptive innovation.

In fact, Sweden has a great potential to improve the state of cyber security in a short time: the research conducted for instance at the Center for Cyber Defence and Information Security at KTH and at RISE is of high international repute, the education at Swedish universities is of good quality and up-to-date, and university innovation support and large industry interest are present. The problem is fragmentation of efforts, and lack of common priorities and action.

To solve this Swedish problem, we see the need for a national centre for cybersecurity research, innovation and education, in which universities and research institutes engage with government agencies and the private sector. Sweden needs a Cyber Campus.



Cybercampus Sweden complements other national initiatives. A national *Cybersecurity Center* has been established with the task of coordinating government agencies and the private sector. The Swedish Civil Contingencies Agency (MSB) hosts Swedish NCC, a National Coordination Center associated with the European Cybersecurity Competence Center, ECCC. RISE and Vinnova have established *CyberNode*, a cybersecurity innovation node.

CDIS is the KTH Center for Cyber Defence and Information Security.

In contrast to these coordination initiatives, Cybercampus Sweden will focus on conducting research, education and innovation that support the other sectors and meet demands not addressed by them.

Initiatives in other nations

Cybersecurity is a global concern with a broad scope from human and societal considerations to engineering and mathematical aspects. The need to address security in full requires joint activities in research, innovation and business development, education and training. We find this manifested around the world and relate our initiative to comparable cybersecurity hubs and campuses in Europe from where we take inspiration.

The established European campuses that serve as examples for a Swedish effort are the Cyber Defence Campus in Switzerland, the Norwegian Centre for Cyber and Information Security, Research Institute CODE in Germany, and Pôle d'Excellence Cyber in France. We briefly describe them below. We then mention some other notable efforts for innovation and research.

Cyber Defence Campus, CYD, Switzerland
Armasuisse, the Swiss federal office for defence procurement, leads the collaborative initiative to strengthen the Swiss capabilities to handle cybersecurity threats by working across sectors from universities, federal and cantonal agencies to businesses. There are three sites: at the Armasuisse site in Thun and the Federal Institutes of Technology, EPFL and ETH Zurich. CYD started in 2019 when the three locations were inaugurated. The budget is around 10 million CHF per year with over 25 partners collaborating in some 50 projects that range from research to innovation and business development. CYD is the *primary example* for our initiative.

Center for Cyber and Information Security, CCIS, Norway
The CCIS is a national centre for research, testing, education and training. It was founded in 2010 in a public-private, civil-military and international partnership with more than forty national and international partners and an annual budget of 100 million NOK. Complementary innovation activities are done through the Norwegian Centre for Cybersecurity in Critical Sectors, NORCICS, for collaboration among nearly twenty member organizations that represent industry, state agencies and higher educational institutions. The ambition is to make Norway the most securely digitalized country in the world.

Security Delta (HSD), The Netherlands
Security Delta offers its more than 275 member companies, authorities and universities knowledge development, innovation support, commercial networks, recruitment channels and venture capital networks. Part of the Security Delta consists of HSD Campus, a physical meeting place for Dutch stakeholders in the field of cyber security. In comparison with, for example, the German CODE, Security Delta is more oriented towards the business and innovation sector.

Cyber Defence Research Institute, CODE, Germany
German efforts in cybersecurity and defence are spread over many different actors. With respect to research, the principal organizations are Cyber Defence Research Institute, CODE, at the University of the Federal Armed Forces; the Max-Planck Institute for Cyber Security and Privacy; the CISPA Helmholtz Center for Information Security; the KASTEL - Institute of Information Security and Dependability, and Fraunhofer ATHENE research centre for cybersecurity and privacy. Of these, we present CODE.

CODE was founded 2013 and connects competences in cybersecurity from research, the military, business, industry, as well as public agencies and organisations. Joint efforts in research, innovation and start-ups aim at promoting cybersecurity and digital sovereignty for the European Union. The institute has 250 employees with 13 professorships that conduct research of international excellence. It runs a data centre and is planning for the acquisition of a quantum computer.

Additional innovation activities in Germany are provided by the Bundeswehr Cyber Innovation Hub for supporting the digital transformation of the Bundeswehr, and the Agency for Innovation in Cybersecurity with the task of making research results applicable and practicable for real systems and situations.

Pôle d’Excellence Cyber, France
The Cyber Center of Excellence in Brittany provides both training and scientific research in cybersecurity. The centre has a broad member base from universities and Grandes Écoles, cyber research laboratories of CNRS and INRIA, and large industries along with entrepreneurial small and medium sized companies. A complementary Campus Cyber at La Défense in Paris was launched in 2021 with the ambition to promote French excellence in cybersecurity as an international hub for business development, innovation and entrepreneurship.

Other cyber security efforts

Helsinki-Aalto Institute for Cybersecurity, HAIC, Finland
HAIC is a joint initiative between Aalto University and the University of Helsinki for reinforced strengths through cooperation to develop a world-leading centre for research and education in cybersecurity.

NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, Estonia
CCDCOE covers areas of technology, strategy, operations and law for research, training and exercises in the field of cyber defence for its member nations and NATO. Sweden is a member of CCDCOE.

London Office for Rapid Cybersecurity Advancement, LORCA, United Kingdom
LORCA is a business accelerator for cyber security with technology and business experts as well as investors to grow the sector of cyber security business and to improve national cyber defence.

Outside Europe
Notable international centres outside Europe are the Chinese cybersecurity parks in Tianjin outside Beijing and in Wuhan; the Cyber NYC on Manhattan in New York, and the CyberSpark in Beersheva, Israel.

Common threads

A first common thread of the presented initiatives is the focus on innovation activities to bring new systems, solutions and work practices to companies, public organizations and state agencies. It is being addressed by co-location of all stakeholders, which is the second thread, for joint activities on a campus with professional administration and access to capital for new ventures. A third common thread is training of professional staff in cyber security. This relates to educating IT specialist as well as to adding security awareness and proficiency for other professions in areas such as health care, finance and retail. A fourth thread is national collaboration between researchers to address more challenging problems, to maintain costly research infrastructure, and to compete successfully in large European funding programs.

The mission and objectives

The mission for the proposed Cybercampus Sweden is to carry out agile and cutting-edge cybersecurity research, education and innovation vital for a resilient Sweden that go beyond what is possible for an individual university, institute, agency, or company.

The specific objectives of the campus include the following.

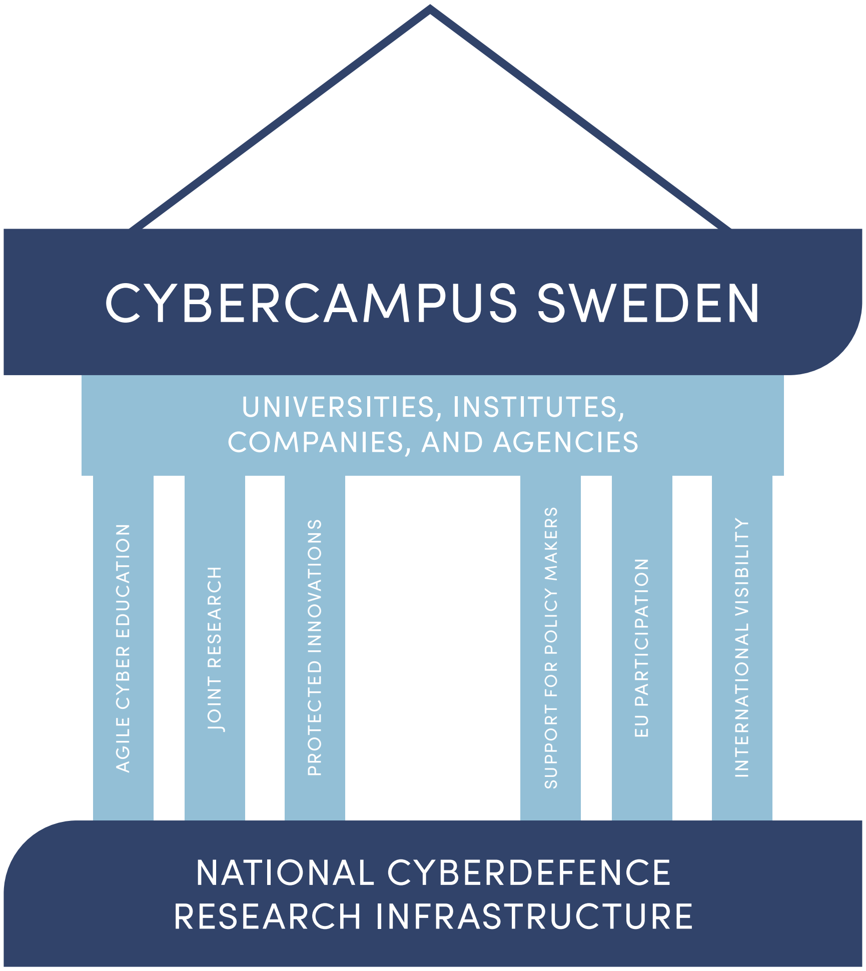
Agile cybersecurity education: There is an alarming imbalance between the cybersecurity workforce required in Sweden and the number of skilled graduates being produced by Swedish universities. There is also a gap between the needed cyber skillset and the contents of existing education programmes. Cybercampus Sweden aims to build capacity for work force training and to facilitate new cross-university cybersecurity programs, taking advantage of the specific teaching expertise from different universities. Bachelor-level programmes will provide a strong base with deep area expertise, and master-level and continuous education programmes will train the cybersecurity workforce needed in Swedish organizations.

Joint research: Swedish cyber security research is competitive, with strong research groups in universities such as KTH and research institutes as for instance RISE. However, a few research topics are dominant, whereas other highly important research areas are missing. Ongoing cybersecurity research is neither well-coordinated nor interdisciplinary. Cybercampus Sweden will thus identify, execute, and coordinate cross-university research on topics important for Swedish civil and military cyber defence as well as industrial competitiveness.

Protected innovation: Cybercampus Sweden will provide a common workplace for academia, government agencies, industry, and spin-offs. This constellation, when combined with coordinated educational programmes and interdisciplinary research initiatives, will form a strong cyber innovation environment in Sweden. Cybercampus will bridge open academic research and protection of innovations for defence and industry.

National research infrastructure: The campus aims to establish a unique national research infrastructure for cybersecurity. The national infrastructure will also provide synergies with existing research and innovation facilities such as CRATE at the Swedish Defence Research Agency (FOI) and the RISE Cyber Range.

Competent body of expertise for decision makers: The Campus will be able to provide timely, well-informed and organizationally neutral advice and expert opinions to decision makers on cybersecurity and cyber-defence related matters, including EU regulations, evaluation of national digital infrastructure, new national cybersecurity research and innovation programmes, and critical products and services being used in national infrastructures.


CYBERCAMPUS SWEDEN
UNIVERSITIES, INSTITUTES, COMPANIES, AND AGENCIES
AGILE CYBER EDUCATION
JOINT RESEARCH
PROTECTED INNOVATIONS
SUPPORT FOR POLICY MAKERS
EU PARTICIPATION
INTERNATIONAL VISIBILITY
NATIONAL CYBERDEFENCE RESEARCH INFRASTRUCTURE

Coordinated EU participation: EU runs several multi-billion-Euro programmes on digitalization and cybersecurity. There is a strong imbalance between Swedish contribution to EU programmes and the participation of Swedish organizations in these programmes. Such programs are out of reach for small research groups in universities; also, the efforts required to coordinate and apply for these programmes is usually beyond the expertise of a single organization. The proposed Cybercampus Sweden will have the required expertise to apply for and lead projects within these programmes.

International visibility: Cybercampus Sweden aims at boosting international visibility for Swedish researchers and innovators. The momentum provided by joint research, the availability of cybersecurity research infrastructure, and stronger national and international funding will allow Swedish cybersecurity to prosper. This, in turn, will attract international cyber experts to Sweden, further strengthening the Swedish cybersecurity ecosystem.

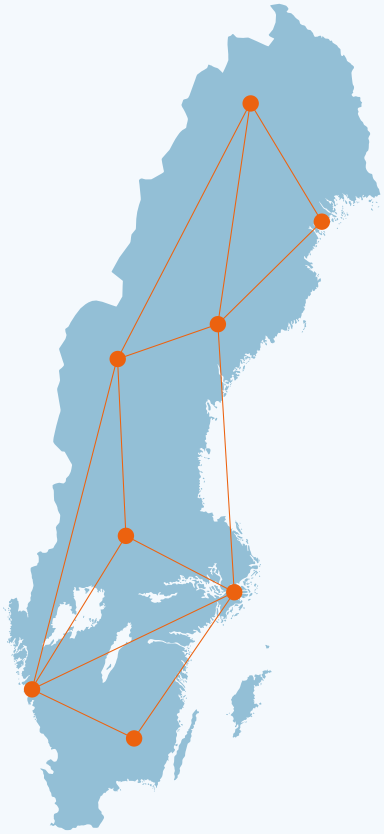
Organization and location

Large-scale national research infrastructure benefits from being conducted in collaboration between several higher education institutions and other actors.

One successful example is SciLifeLab which has four founding universities: KTH Royal Institute of Technology (the prinicipal university), Uppsala University, Karolinska Institute and Stockholm University. Founded in 2009 SciLifeLab was has proven to be a common infrastructure for all universities in life sciences in Sweden. SciLifeLab also works with data management, infrastructure education and translational innovations. Other sectors, such as healthcare and industry, also use the SciLifeLab infrastructure. As a result, integrated collaboration structures for infrastructure, research, data management and education are enabled. The strength of this national research infrastructure was particularly evidenced during the pandemic.

Cybercampus Sweden is therefore proposed to be organized as a national collaboration between several universities, research institutes, government agencies and companies across Sweden. The workforce will be constituted of a mix of faculty from participating universities, employees of institutes as well as dedicated Campus staff and representatives from companies and agencies.

The physical space of the campus will offer an inspiring workspace for the employees as well as a dynamic and neutral meeting place for all stakeholders from both the private and public sectors. Maintained national research infrastructures will be open for all participating Swedish researchers.



To allow research and innovation on subjects of national security as well as on sensitive corporate matters, both physical and information security will be prioritized in the organizational structure and physical office planning. Provisions to allow compartmentalization will be used to restrict interaction, when necessary, while maintaining an open and collaborative environment when possible.

Action plan

Below is the list of actions by the Government and by the Campus to start the operation of the campus.

Actions by the Government

- Establish Cybercampus Sweden and allocate long-term funding to it.
- Appoint a national board that governs the campus, with representatives from the host universities, research institutes, government agencies, and the private sector.
- Appoint a National Cybercampus Committee representing other Swedish universities and stakeholders contributing with a national perspective to the operations.

Actions internal to the Campus

- Develop a plan for the establishment of the Campus.
- Recruit staff to the Campus management team.
- Secure a physical location for the Campus.
- Develop a strategic research agenda for strengthened national cyber defence and cybersecurity posture.
- Develop Cybercampus Sweden's educational program.
- Develop a detailed plan for the national infrastructure – technologies, dedicated expertise and meeting facilities – within the campus for all cyber defence and cybersecurity researchers and innovators throughout Sweden.
- Establish an international advisory board to ensure that the campus evolves in accordance with international trends and developments.

About the signers

KTH Royal Institute of Technology
KTH is Sweden's largest and most productive university with respect to cyber security research. We develop new knowledge to strengthen Swedish cyber security for the rapid digitalization of society. The KTH Center for Cyber Defence and Information Security, CDIS, is a research and education collaboration between KTH, the Swedish Armed Forces, the Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment (FRA), the Swedish Defence Research Agency (FOI), and the Swedish Defence University (FHS). The research conducted results in novel information security methods and tools, as well as cyber defence applications. The research conducted results in novel information security methods and tools, as well as cyber defence applications. CDIS facilitates the transfer of knowledge to related organizations and partners, while KTH also assists the Swedish Armed Forces with courses to train cyber soldiers, based on the latest state-of-the-art research.

RISE Research Institutes of Sweden
RISE is the largest Government-owned research institute, headquartered in Gothenburg and present in all major cities in Sweden. RISE has a strong focus on cybersecurity, having over 30 researchers. In addition to conducting basic and applied cybersecurity research, RISE is participating in strategic Swedish and EU initiatives in close collaboration with industry. Among other activities, RISE is leading the National Cybersecurity Innovation Node (cybernode.se), hosts a cybersecurity test and demo arena (RISE Cyber Range), and a partner and management board member of the CONCORDIA EU Cybersecurity Network of Excellence.

Swedish Armed Forces
The Swedish Armed Forces defend Sweden, the country's freedom and protect our right to live the way we choose. The Swedish Armed Forces grow, strengthen their capabilities and develop the defence forces of tomorrow. Access to cutting-edge knowledge at the forefront of research is paramount for capability development of the Swedish Armed Forces, not least regarding cyber defence and information security. Capability development of the Swedish Armed Forces is carried out together with national and international partners.

Contact

Pontus Johnson
Director of
CDIS,
KTH
pontusj@kth.se

Shahid Raza
Director of
Cybersecurity Unit,
RISE
shahid.raza@ri.se

David Olgart,
Coordinator R&T
Cyberdefence,
Swedish Armed Forces
david.olgart@mil.se