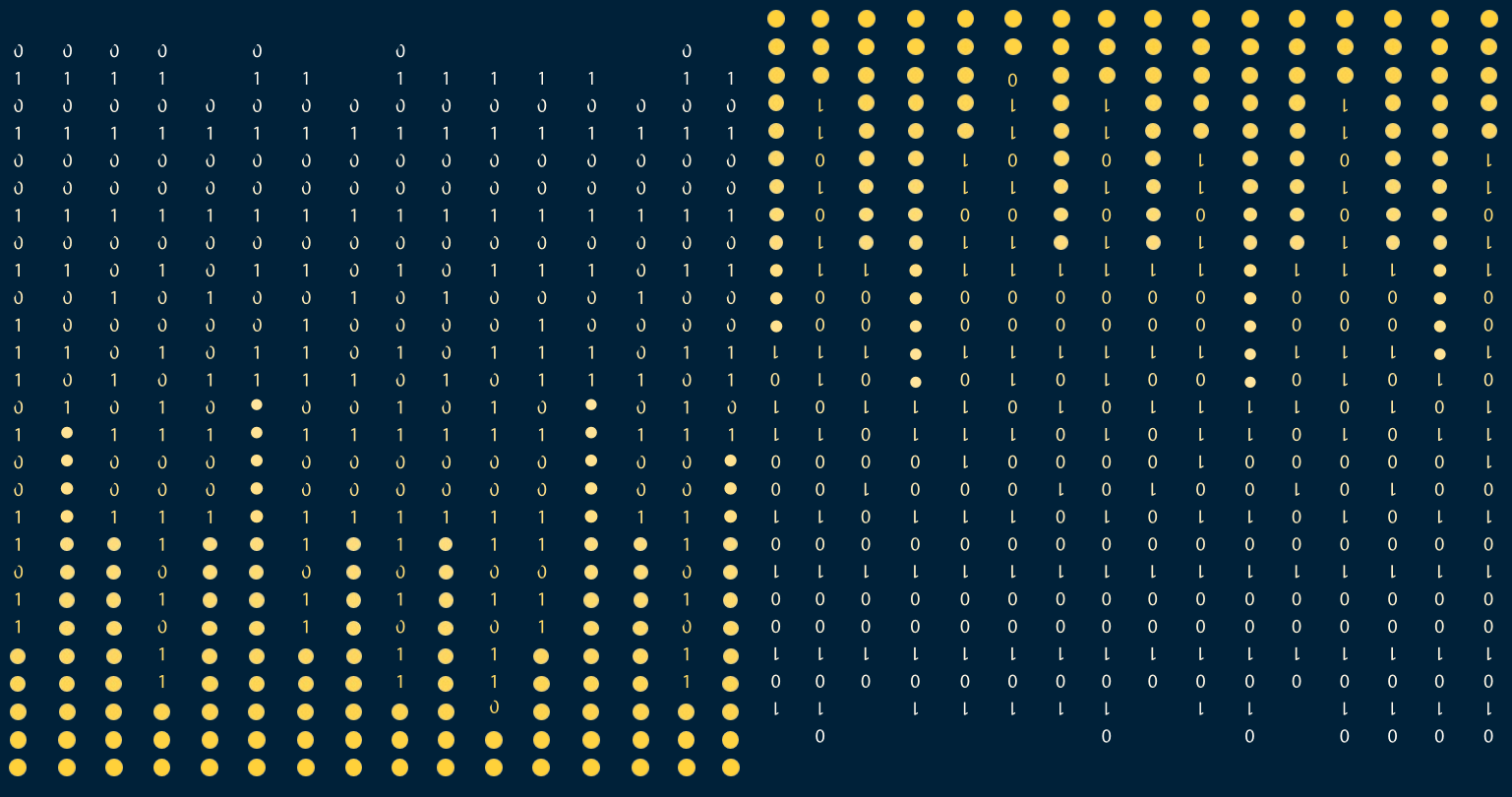
CYBERCAMPUS SVERIGE

Cybercampus Sverige

Strategies

Final draft
March 2025



CYBERCAMPUS SVERIGE

Table of contents

Cybercampus Sweden is a national initiative that conducts agile and cutting-edge research, innovation and education in cyber security and cyber defence.

www.cybercampus.se

Cybercampus Education

Improving cybersecurity in Sweden through education

A strategy for Cybercampus Sverige

Ambition

Skills and knowledge in cybersecurity for analysis, planning and execution require education and training. Cybercampus has the ambition to strengthen and complement existing educational offerings in Sweden and to drive development of education for professionals. Cybercampus education is grounded in ongoing research, both internationally and within the organisation nationally. Our education aims at transferring new results to practicable use as well as to raise competence for all needs.

This document provides a first strategy for establishing national collaboration regarding higher continuous education to meet the competence needs in the Swedish society. There are three audiences addressed: the public for their private lives and civic engagements, professionals in their work roles, and cybersecurity specialists for their specific needs.

Cybercampus serves also as a national collaboration hub for higher education in cybersecurity regarding educational resources, credit transfers, student exchanges, personnel and infrastructures.

General guidelines and rationales

The role of Cybercampus in education

The priority of Cybercampus is to strengthen and to complement existing educational programs at universities, university colleges, and higher vocational education providers to address the needs of professionals and prioritised categories of society.

Education for professionals should primarily be *contract education*, which has degrees of freedom not available for publicly grant-funded courses: absence of admission, no formal prerequisites, guaranteed availability, and freedom in scheduling and formats. Contract education is fully financed by the buyers and may award credits and grades.

All academic partners in Cybercampus provide *free-standing courses* that can be taken for free by admitted participants who meet the prerequisite qualifications. Cybercampus will provide a unified view of these courses with guidance to find matching courses for specific needs.

The strengthening of education at the partner institutions of higher education is through collaboration regarding sharing of course materials, credit transfer and

other means of forming a national curriculum in cybersecurity and to provide, operate and use common infrastructures for education.

Formats follow function

Professional upskilling needs education provided in situated, online and hybrid modes to be available as formal (for credits) or informal education (with other forms of recognition). Courses need to be of different sizes and formats to allow part-time studies. Informal activities will be given in the form of self-tests, challenges, seminars, discussions and consultations, and public lectures.

Cybercampus activities shall be characterised by high standards. All activities will be designed to be efficient for meeting the intended goals, and their quality will be evaluated and assured by Cybercampus in terms of contents, delivery and fulfilment of purpose.

Outreach activities will address society at large to provide actionable skills and applicable knowledge. We intend to build interest in vocational and academic studies and careers in cybersecurity by attractive youth activities.

Educational objectives and standards

The role of Cybercampus education is to meet higher educational goals: analysis, synthesis and evaluation. All courses should have high expectations on the participants when the education is formal: The study time should correspond to awarded credits and a passing grade should not be awarded without distinction in the work performed. High teaching standards shall be maintained in subject matter, exercises, and delivery, for all formats of education. The quality will be evaluated by Cybercampus.

Cybercampus is the primary point of contact for professional education and training in cybersecurity in Sweden and will provide contracts and agreements for education for all partner organisations. Contacts with teachers and staff should be professional and responsive.

Principles for funding of education and priorities

Funding for courses and infrastructure

We refer to the educational objects provided by Cybercampus as *courses*; courses may be bundled or stacked into programs. The formats of courses and programs are not given a priori or limited by precedence from regular grant-funded education.

The education provided by Cybercampus and its partners are:

Cybercampus courses that follow the educational strategy and priorities of Cybercampus. They are developed, funded, maintained and promoted by campus resources. The courses are available to all partners; rights and curation of material reside with Cybercampus, if not agreed otherwise.

Partner courses are developed, funded and maintained by each partner or group of partners. The courses can be shared within and promoted by Cybercampus. Rights and curation of material reside with the partners.

The development of campus courses and inclusion of partner courses are decided and regulated by the campus management. Cybercampus monitors that the quality of the courses is of a high standard according to an agreed framework.

Infrastructures for education will be supported by Cybercampus both financially and operationally when they provide services of shared interest among two or more partners. Examples include testing facilities, learning management systems and cyber ranges. Decisions on support depend on foreseen usage and an economic plan for a proposed platform.

Priorities and discussion

Among professionals needing training, there are distinct categories.

- Non-executive decision makers: board members and investors.
- Executive and legal officers and heads of government agencies.
- Professionals working with cybersecurity in non-technical roles.
- Cybersecurity specialist in need of continuous updates and training.
- Basic awareness and skills for all employees.

In addition to professionals, Cybercampus collaborates with state agencies and civic organisations to increase the competences of all members of society to withstand cybersecurity attacks and with education providers to support students to become professionals.

We make the following prioritisation *timewise* with respect to the resources of Cybercampus.

At first – urgency

Two prioritised activities target education for the *first and last categories* for the following reasons.

- We need societal and business leaders who are confident in addressing cybersecurity within their organisations. Their knowledge of cybersecurity

will lead to further development of Cybercampus activities in education, innovation and research.

- All members of an organisation are potential cybersecurity vulnerabilities. Workplaces must thus provide cybersecurity training to raise the lowest level in awareness and skills of everyone.

A third activity for the near-term addresses specialists and students: The establishment of a course catalogue over available freestanding and contract-education *partner courses* and programs for the needs of specialists and non-technical professionals. The catalogue is curated, and the courses are grouped into meaningful programs with tools for matching them to individual needs.

Intermediate concern – education in need of development

Non-technical work in cybersecurity requires in-depth understanding of a workplace and work practices to assess risks, commission work to mitigate them and to implement solutions. The need for training this category of professionals will be studied, and suitable educational activities will be developed.

Specialist training will develop by means of networking, online seminars and events to provide access to research and researchers at partner universities.

Outreach activities for improving competence for all members of society and civic organisations require resources and marketing of efforts beyond regular university education. Outreach will be addressed by appropriate campus events and cooperation with relevant stakeholders.

Not important or not urgent

Setting priorities also implies ranking activities low, either in importance, urgency, or both.

Focusing on education for professionals implies that Cybercampus will not address the capacity for, or volume of, grant-funded cybersecurity education in first and second cycles (for third cycle education see *Cybercampus PhD Graduate School – Plan & Strategy)*.

It is not the concern of Cybercampus to meet individual organisations' needs; only education that is demanded broadly and coheres with this strategy will be addressed.

Surveying the needs of cybersecurity competence in work life and society at large and to provide overviews of providers nationally and internationally is beyond the scope of the educational role of Cybercampus.

There will be expectations that cannot be met without deviating from the set strategy. The purpose of this plan is to communicate this clearly for contacts with

Cybercampus regarding education. We will engage in discussion regarding any choice stated herein.

Actions for addressing the priorities and initial steps

The general structure for developing campus courses and other educational components is based on collaboration among partners and based on *calls for application* regarding a foreseen need. The selected partners offer the developed education under the auspices of Cybercampus; other partners may use it freely or on reasonable terms.

The ambition is to provide an extensive set of courses (in the broad sense used herein). This set needs to be managed to serve the targeted groups specified above: Courses may be organised into proposed tracks leading to specific professional roles, and guidance provided in matching courses to needs by means of AI, diagnostic tests and informative material. Credits should be transferable among all partner institutions for the common set of courses.

All courses are promoted by Cybercampus information, events and activities.

To promote novelty in education, proposals and ideas will be tested in small workshops, fictitious offerings, surveys and by other means to receive feedback; some proposals will then be developed to become available educational products. Sharing experiences and workable practices is encouraged.

Cybercampus will provide teacher exchanges, education platforms for learning management and practical training, open educational resources of any form, software and equipment as well as time for collaboration and coordination. The balance of these activities constitutes an important continual task.

Cybercampus will rely on state agencies, business associations, direct contacts and other sources of information for assessing the needs of education, such as requests from potential buyers and other parties in need of education. The compiled and prioritised list of needs, with subjects and course formats, serves as a basis for calls for developing courses and other educational material, not as official public surveys.

Cybercampus Research

Research Plan and Collaboration Model

Cybercampus Sweden is a national initiative that conducts agile and cutting-edge research, innovation and education in cyber security and cyber defence.

www.cybercampus.se

Acknowledgements: This Research Plan and Collaboration Model is developed by RISE with valuable comments and feedback from the following organisations that we would like to thank very much: Chalmers University of Technology, Karlstad University, KTH, Jönköping University, Linköping University, University of Skövde, Uppsala University, Örebro University.

Abstract

Cybercampus Sverige is a Swedish national initiative that conducts agile and cutting-edge research, innovation and education in cybersecurity and cyber defence beyond what is possible for a single university, institute, government agency or company. *This Cybercampus Research Plan outlines the strategic approach to advancing cybersecurity research and collaboration in Sweden. To complement the existing research setup and project-based initiatives, as well as piggybacking on these initiatives, Cybercampus research will carry out mission-oriented research to address immediate cybersecurity challenges and foster groundbreaking innovations that have direct applications and use in Swedish society. The mission could be to build a new tool, technique, or service; however, it must be implementable in Sweden in the near future to strengthen Swedish cybersecurity capabilities and/or foster safe and secure digitalisation.*

Key research areas are chosen based on ensuring digital sovereignty, resilience, and usability in Sweden; proposals to include other research topics are welcome by the partner organisation as long as they fall within the aims of mission-oriented research that goes beyond what a single organisation can carry out or what is being funded by other sources. The plan also highlights the significance of cybersecurity for critical infrastructure sectors such as healthcare, energy, and telecommunications.

Cybercampus research activities are supported by long-term research engineers, senior researchers, professors, and PhD students. We will establish a national cybersecurity research graduate school that will support combined research students across Sweden, (co-)supervised by at least two partner universities, institutes, or industry partners. Cybercampus research activities will be aligned with national and EU priorities as well as current and upcoming cybersecurity regulations. A strong focus will be on collaboration with industry and the public sector to develop and implement effective cybersecurity solutions.

The ultimate goal is to establish Sweden as a leader in cybersecurity research, ensuring that its digital infrastructure is secure, resilient, and capable of withstanding both cyber threats and physical conflicts. This document serves as a comprehensive guide for fostering cybersecurity research, maintaining high research standards, and promoting the practical application of research findings in Swedish industry and public sectors. It is a living document and will be further developed based on input from Cybercampus stakeholders and collaboration partners and continuously updated to adequately address emerging cybersecurity challenges.

List of Abbreviations

CRATE	Cyber Range And Training Environment
EDF	European Defence Fund
ESA	European Space Agency
EU JU	Joint Undertakings JRC Strategic Research Plan
FHS	Försvarshögskolan, Swedish Defence University
FOI	Totalförsvarets forskningsinstitut, The Swedish Defence Research Agency
GDPR	General Data Protection Regulation
KKS	Stiftelsen för kunskaps- och kompetensutveckling, The Knowledge Foundation
NTN	Non-Terrestrial Network
OT	Operational Technology
PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
PET	Privacy-Enhancing Technologies
RISC-V	Reduced Instruction Set Computer five
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SoC	System-on-Chips
SSF	Stiftelsen för Strategisk Forskning, Swedish Foundation for Strategic Research
TEE	Trusted Execution Environment
VR	Vetenskapsrådet, Swedish Research Council
WASP	Wallenberg AI, Autonomous Systems and Software Program

Introduction

Cybersecurity research is increasingly becoming an important topic. Cybercampus Sverige's mission is to drive agile and cutting-edge joint research, innovation, and education in cybersecurity and cyber defence—far beyond what individual universities, institutes, companies, or government agencies can achieve on their own. By uniting forces across different disciplines and all sectors of society, Cybercampus addresses needs that no single actor in the cybersecurity field currently meets.

On the research side, this should be achieved through the cooperation of various excellent cybersecurity research groups in Sweden, each with complementary expertise in different cybersecurity domains. Nonetheless, although Sweden has research groups of very high international standards in many areas, some strategic cybersecurity research topics and areas are not well covered. At a workshop on "Research and Joint Research Infrastructure," organised by the Cybercampus planning group in January 2023, participants from academia, industry, and the public sector identified and discussed research areas that were already well covered in Sweden and those that still lacked sufficient focus.

We also aim to achieve the highest international standards in strategic cyber research and position Sweden as a leading cybersecurity research hub. This document also outlines the principles of research connected to Cybercampus Sverige. The purpose is to create a mutually beneficial and fruitful collaborative environment for students and researchers, whether they are physically located at the Cybercampus facility or regularly visiting and meeting there. By sharing workspace and cybersecurity infrastructure, Cybercampus partners can facilitate active research collaboration.

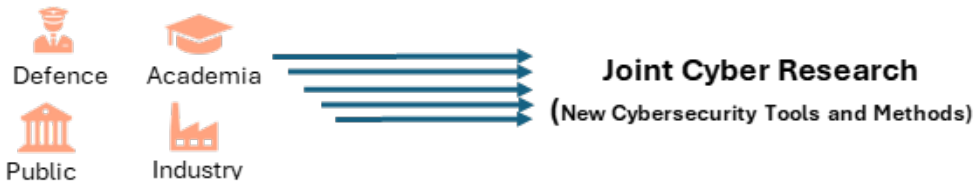


Figure 1: Bringing expertise from all sectors to carry out joint strategic cybersecurity research for Sweden.

Guiding principle for research in Cybercampus

In developing a comprehensive research roadmap for Cybercampus Sweden that aligns with its vision (national initiative that conducts agile and cutting-edge research, innovation and education in cybersecurity and cyber defence beyond what is possible for a single university, institute, government agency or company), it is crucial to consider that Cybercampus will complement the existing

cooperative, project-based, and individual research activities by carrying out mission-oriented research.

Mission-oriented research activities at Cybercampus begin with a clearly defined output that can be directly implemented in Sweden. For example, a mission could be to develop a sovereign and trustworthy cloud infrastructure in Sweden that can be used by Swedish organisations, such as healthcare providers for secure data storage and processing, as well as by other civil and military entities. To achieve this mission, cyber experts from various domains—including hardware, software, applications, and policy—will be needed, along with long-term research engineers and support staff to sustain and innovate upon the results beyond the project period. The ultimate goal would be to commercialise the results and establish a fully operational cloud solution through new spin-offs, startups, or Cybercampus industrial partners. To achieve a specific mission, we do not always rely solely on applied research or utilise fundamental research funded by other sources. Instead, conducting fundamental research in the campus may also be necessary when required.

Due to the lack of long-term funding and working models, such mission-oriented research is difficult to conduct within a single Swedish university or institute. Cybercampus will utilise, whenever and wherever possible, the outcomes of existing and upcoming research projects in Sweden funded by various Swedish funding organisations. On a limited basis, Cybercampus also aims to carry out cutting-edge, long-term basic research, mainly co-funded by partners from academia and industry. This approach allows Cybercampus to remain responsive to emerging threats and opportunities while fostering collaboration and excellence in cybersecurity research.

There are several challenges to cybersecurity research in Sweden. The current research is not sufficiently coordinated, nor is it interdisciplinary. As Cybercampus has identified in several workshops and meetings, there are a few research topics that are dominant whereas other highly important areas are missing. Cybercampus Sweden aims to identify and execute cross-organisation research and provide an environment to conduct both cyber defence and cybersecurity research which is directly applicable to Swedish civil/military cyber defence and industrial competitiveness.

Key Cybersecurity Research Needs in Sweden

Cybercampus will cater to Swedish cybersecurity research needs through a joint interdisciplinary approach. **I**n cybersecurity research, the convergence of technology, policy, law, ethics, human factors, and organisational considerations is crucial for developing comprehensive security solutions. As the Cybercampus mission is to have implementable results in Swedish, *these horizonal interdisciplinary aspects are central to the deployment of outcomes in Sweden*.

Digital sovereignty is of paramount importance for Sweden as it ensures the nation's control over its digital infrastructure, data, and technological innovations. In an increasingly interconnected world, maintaining digital sovereignty protects against external threats, secures sensitive information, and promotes economic stability. By investing in robust cybersecurity research, Cybercampus aims to develop cutting-edge technologies and strategies that safeguard its digital autonomy. This research not only fortifies national security but also fosters innovation and competitiveness in the global market. It is essential for Swedish cybersecurity research to contribute to digital sovereignty, ensuring that Sweden remains resilient against cyber threats and maintains control over its digital future.

For contributing to this end, ten cybersecurity research themes that Cybercampus will address are presented below. These *mission-oriented themes* are highlighted based on recent Swedish and European cybersecurity reports, strategies and policies as well as possibilities to co-fund them through the new national and international funding calls. All these themes must at the end propose projects are follow the mission-oriented research principle highlighted above. A proposal by Cybercampus partner organisation to include other themes that following the mission-oriented research principle are very welcomed. However, research activities where the end beneficiaries of results are not in Sweden will not have high priority as we have limited resources in the campus and the focus will be on strengthening Swedish cyber capabilities. It is important to note that all ten proposed themes require research contributions from various domains and disciplines. Therefore, they must be addressed through joint research cooperation among cybersecurity researchers from different Cybercampus partner organisations, bringing together expertise from multiple fields. This includes researchers specialising in hardware security, software security, network security, cryptography, data privacy, human factors, cybersecurity law, and other relevant areas (see also the discussion on the “Horizontal Interdisciplinary Approach” below).

The themes presented below ensure that Sweden places well in the context of cybersecurity in European research work programmes, where Horizon Europe [i], DIGITAL Europe [ii], and European Defence Fund EDF [iii] are the most prominent on the topic. However, cybersecurity spans the whole maturity scale from Pillar I with fundamental and excellent research in ERC [iv] and Marie Sklodowska-Curie Actions MSCA [v] to the more applied types of research funded in Pillar III by the European Innovation Council EIC [vi]. Topical calls in Pillar II [vii] often express needs for cybersecurity expertise and these are also monitored by Cybercampus.

Socio-Technical Practices and Approaches

Organisations in real-world situations face challenges, which need to be addressed by socio-technical practices and approaches, including, but not limited to,

challenges related to information security management, cybersecurity culture, human aspects, ethics, privacy, and legal aspects. Information security management is essential for protecting sensitive data, ensuring regulatory compliance, and maintaining business continuity. It is also part of fostering an information security culture, helping to mitigate risks from evolving cyber threats. The challenges in this topic cover a broad spectrum, from managerial challenges concerning, for example, upper management awareness and responsibilities for designing and maintaining the necessary policy documents to challenges related to risk management. In risk management, open issues include decreasing subjectivity in decisions, risk modelling, and compliance. In designing and maintaining the necessary policy documents, there is a need to research how to effectively design actionable advice to guide employees and users in their daily tasks of handling digital systems and completing their assignments. Furthermore, challenges associated with the critical area of resilience, such as continuity planning and incident response, have traditionally received too little attention in research.

Another critical research challenge in cybersecurity is addressing the fact that most cybersecurity incidents stem from how digital systems are used, the so-called human factor of cybersecurity. The human factor area is multi-faceted and includes, for instance, authentication practises, social engineering and system configuration. Research and practice show that incidents that can be traced back to the human aspects happen for various reasons, including user mistakes, unclear communication of rules and procedures, complex digital systems, and/or lack of a culture where cybersecurity is promoted. In essence, organisations must develop a sound cybersecurity culture where security is high on the agenda for every organisation member. Developing a cybersecurity culture is highly dependent on national and organisational culture and the values and perceptions of the people in the organisation, stressing the need for cybersecurity culture to be researched within a Swedish context. To that end, research is needed on building cybersecurity in Swedish organisations. Project examples include implementing effective awareness-raising programs contributing to a more robust cybersecurity culture.

Secure Cloud and Edge Processing

In today's connected and digitalised world, a secure cloud is essential for safeguarding sensitive data, ensuring privacy, and maintaining the integrity of digital operations. Trusting public cloud providers can be challenging due to the potential risk of insider attacks, where employees or contractors within the provider’s organisation could misuse their access to exploit or compromise customer data. Public clouds are also susceptible to espionage and governmental access. Governments may exert legal pressure on cloud providers to disclose data through mechanisms such as surveillance laws like the USA PATRIOT Act [viii] or the CLOUD Act [ix]. Additionally, espionage activities, whether conducted by state-sponsored actors or malicious entities, can target public cloud infrastructures to gain unauthorised access to sensitive information. These concerns underscore the importance of implementing strong encryption, data sovereignty measures,

privacy-enhancing technologies and stringent security protocols to protect data stored in public clouds from unauthorised access and surveillance.

Cybercampus aims to build practical cloud technology where it is possible to store and process sensitive data without needing to trust the cloud providers. To this end, we will exploit technologies such as confidential computing and fully (hybrid) homomorphic encryption techniques or secret sharing protocols. Additionally, we will work on eliminating the risk of hardware backdoors and espionage and will develop a cloud solution built on the open hardware architecture such as RISC-V [x] and open-source software stack. Moreover, usability of the configuration of secure cloud solutions needs to be addressed, which may require not only technical but also legal and management expertise.

Open-Source Software and Hardware

Open hardware platforms like RISC-V are becoming increasingly vital for the European Union's digital sovereignty, enabling independence from proprietary technologies. While the security guidelines of RISC-V are still under development, providing RISC-V users with an effective plug-and-play solution to strengthen the security of System-on-Chips (SoC) is critical. Though software security remains a paramount concern, placing trust in an entire codebase that includes millions of lines of code and third-party libraries is not feasible due to potential vulnerabilities. As such, the isolation of the most critical software operations from the rest of the technology stack is inevitable. Trusted Execution Environments (TEEs) is instrumental in achieving this isolation, providing a secure area for sensitive processes. Our research will focus on the integration of open-source hardware and software that support isolated trusted execution. We will also examine the use of software fuzzing as a method to enhance the security of future networks, including IoT devices. Furthermore, formal verification techniques for the small codebase that ends up in TEE are necessary. Cybercampus will also facilitate the deployment of these secure open hardware and software solutions in Swedish critical national services to ensure a robust and secure digital infrastructure.

Trustworthy AI

Numerous research efforts are being carried out using AI to solve important cybersecurity problems, such as developing better intrusion detection mechanisms. Researching such AI-powered techniques to anticipate, detect, and mitigate malicious activities is crucial. Though these AI-powered defence strategies are essential for combating the sophisticated and evolving nature of cyber threats, AI and machine learning techniques themselves are susceptible to various cyber-attacks, which can undermine their effectiveness and reliability. More generally, AI raises cybersecurity, privacy, ethical and broader societal issues. Therefore, it is also of key importance to develop AI solutions that comply with the Ethics Guidelines for Trustworthy AI promoted by the EU Commission [xi] and with the AI act’s comprehensive rules for trustworthy AI [xii].

Particularly, adversarial attacks involve manipulating input data to deceive AI models into making incorrect predictions or classifications. Attackers can also use inversion or membership inference attacks to gain access to the model and reconstruct sensitive training data or carry out poisoning attacks by inserting malicious data into the training set. The applicability of such attacks is even more pronounced in novel machine learning techniques such as federated learning and transfer learning. Cybercampus is committed to working on trustworthy AI with the aim of identifying and securing machine learning techniques that have the potential for use in Swedish industry and the public sector. Cybercampus plans to build a testbed for adversarial AI testing, open to our partners, ensuring robust security measures to protect AI systems from exploitation and guaranteeing that AI-powered defences remain resilient and trustworthy. Moreover, it will research how trustworthy AI principles that can be in conflict with each other (including security, accountability, transparency, fairness, data minimisation or safe) can be adequately achieved in combination through configuring suitable trade-offs per context, and how a fundamental rights assessment required by the AI act for high-risk AI system could consider such value conflicts and assist with finding suitable trade-offs.

Trustworthy IoT

Though extensive research is being conducted on securing IoT devices, the actual enforcement of security and privacy solutions in real-world deployments remains challenging. It is of utmost importance that IoT devices used in Swedish critical infrastructure have a guaranteed level of security. Moreover, IoT devices used for personal purpose should comply with privacy standards. To address this, we will closely align with new EU regulations such as the EU Cybersecurity Act [xiii], the Cyber Resilience Act [xiv], GDPR [xv], and NIS2 [xvi]. We will develop automated assurance and certification mechanisms that ensure not only the authenticity of devices but also the security of the device software stack. This interdisciplinary research will combine expertise from law, policy, cybersecurity, and IoT hardware and software. We will leverage existing research on IoT security protocols, address important gaps, and primarily focus on creating IoT certification mechanisms. These assurance mechanisms should meet the constraints of IoT resources and can be carried out automatically and continuously after each software update or at regular intervals specified by the deployment policy. The ultimate goal is to assign a cybersecurity seal, similar to a safety seal, to IoT devices, which can be easily verified when interacting with the device.

Cybersecurity for Industry 5.0

The incorporation of IT, OT (Operational Technology), IoT, and humans-in-the-loop is a cornerstone of Industry 5.0, where advanced technologies such as cloud computing and AI integrate seamlessly to create intelligent, adaptive, and efficient industrial environments. This convergence enhances productivity, optimises operations, and enables innovative solutions, but it also introduces new cybersecurity challenges. As the boundaries between IT, OT, and IoT blur, a comprehensive cybersecurity strategy must be implemented to safeguard the

entire ecosystem. At Cybercampus, we aim to leverage research in cloud, IoT, and secure AI to develop robust cybersecurity solutions for industrial environments, bringing together control engineers and cyber experts. We plan to build a real Industry 5.0 testbed in Cybercampus with industrial partners, using open-source solutions wherever possible to demonstrate these cybersecurity technologies in action. The ultimate goal is to offer these ready-made cybersecurity solutions to the industry, ensuring they are easy to deploy in real industrial environments in Sweden.

Intelligent and Controlled Network Infrastructure

Cybersecurity research is crucial for ensuring controlled network data flows in Sweden, leveraging technologies such as Software-Defined Networking (SDN) and path-aware networking. These advanced networking paradigms enable precise control over data traffic, allowing dynamic and secure routing of information. By implementing robust SDN and path-aware solutions, Sweden can ensure that critical data remains within national borders, thereby upholding digital sovereignty, especially in the event of national disasters or war. This capability is vital for protecting sensitive information from foreign access and ensuring the operational integrity of local digital infrastructure. Moreover, in the event of war or other national emergencies, controlled network flows can guarantee the continued functionality of essential services and communication networks. Through dedicated cybersecurity research in Sweden, Cybercampus aims to build resilient, secure, and sovereign digital infrastructures that are prepared to withstand both cyber threats and physical conflicts. As a first step, we aim to build such an infrastructure among partner universities as a testbed, showcasing secure interconnections among organisations in Sweden with guaranteed network flow.

Vulnerability Analysis

Despite cybersecurity vulnerabilities being a long-standing area of study, continued research remains critical as our reliance on digital technologies deepens, leaving us vulnerable to increasingly sophisticated cyber threats. Such research is pivotal for fortifying new technologies, particularly IoT devices, which often have insufficient security measures. Swedish researchers in industry and academia have a rich history of researching vulnerabilities, uncovering numerous security gaps and crafting specialised methodologies for vulnerability assessment. The focus of this research is on examining vulnerabilities in IoT, cloud computing, and Operational Technology (OT) that are integral to national essential services, including energy, transportation, healthcare, finance, and industrial sectors. This work will also leverage artificial intelligence and machine learning to enhance vulnerability analysis and digital investigations, including forensic inquiries. An example investigation that Cybercampus plans to carry out is to examine the security of all home router brands being used in Sweden and identify vulnerabilities. By identifying these vulnerabilities, we can provide actionable insights and recommendations to improve the security of home networks, thereby enhancing the overall cybersecurity posture of Swedish digital infrastructure.

Automating Cybersecurity

One of the critical research challenges in cybersecurity is addressing the fact that humans are often the weakest link in the security chain. Human errors, such as weak password practices, falling for phishing attacks, and misconfiguring systems, can lead to significant security breaches. To enhance future security, Cybercampus aims to develop systems that minimises the reliance on human behaviour and interaction for security measures. Automated authentication mechanisms that eliminate the need for passwords and reduce dependence on human knowledge are essential. These systems could leverage biometric data, behavioural analysis, and advanced applied cryptographic methods to provide seamless and secure access with minimal human intervention. By minimising the human factor in cybersecurity, we can create more robust and resilient digital systems that are less susceptible to exploitation due to human errors. Still, even if security is automated, human factors need to be researched related to error situations (e.g. in case of false negatives of certificate errors), when human need anyhow be involved to deal with the errors.

(Semi-)automation of security and privacy decisions by users can also be achieved by AI-based personalised security and privacy assistants that could accurately predict the users' preferences for setting permissions. Nonetheless, in addition to technical approaches, also the compliance with legal requirements and human factors for AI-based (automated) decision making need not be considered. Especially, human oversight for keeping the humans in the loop is required by the AI act for high-risk AI systems, and according to the GDPR consent decisions by data subjects require affirmative actions. How humans can best be engaged for making informed and adequate decisions in these situations constitutes another research challenge that Cybercampus will address.

6G and Cybersecurity

One significant shift from 5G to 6G is the seamless integration of Non-Terrestrial Networks (NTNs) into the telecom infrastructure. The rise of accessible and affordable satellite technologies is paving the way for their widespread adoption across various sectors, fostering a massive convergence of devices and services from personal communication to the management of critical infrastructure. Current research prioritises novel 6G use cases, requirements, and high-level architectures. However, there is scant research focused on creating innovative solutions for secure 6G satellite communications. Sweden holds a strategic position to spearhead the development of 6G protocols, their standardisation, and early implementation. This initiative aims to pioneer new cybersecurity technologies for the automated, intelligent, and seamless amalgamation of NTNs with telecom networks. Cybercampus partners, with its long-standing engagement in numerous telecom security projects and space science projects (funded by ESA), will steer this task. Collaborating with industry, including those from space industry, we aim to formulate and standardise novel cybersecurity protocols specifically for 6G satellite communications.

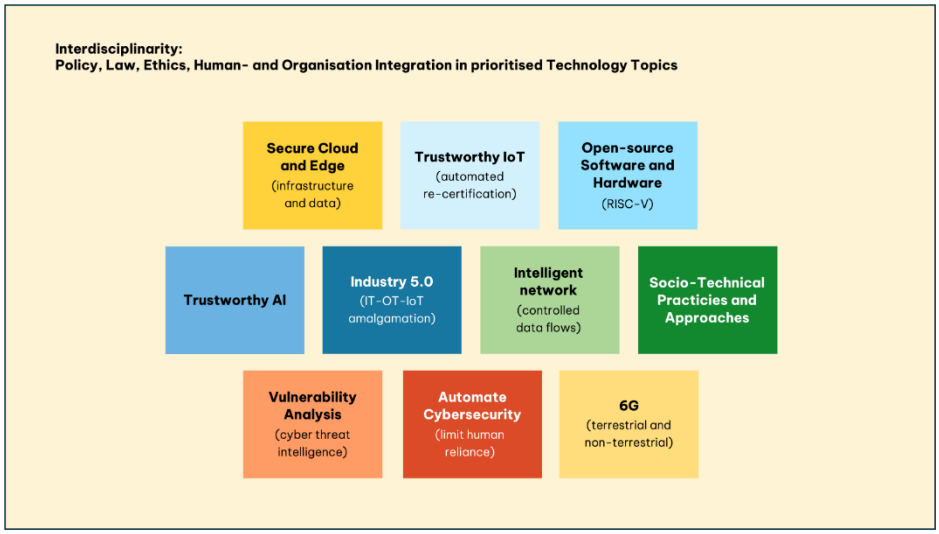


Figure 2: Key mission-oriented high-level research themes for Sweden.

Cybercampus Collaboration Model and Activities

Research Staff

In the long term, Cybercampus aims to strengthen its research team with professors (Assistant/Associate/Full), senior researchers, postdocs, industrial PhD students, and regular PhD students, among others. However, due to limited resources, Cybercampus will initially focus on building a research environment that extends beyond a single university or organisation.

We will start by establishing a cybersecurity graduate school consisting of PhD students. A detailed plan outlining the graduate school's structure and activities—including research, education, mobility, and networking—is provided in the supporting document [REF]. In the first cohort of the graduate school in 2025, we plan to *hire 10 PhD students*. The graduate school will also provide travel grants for PhD students and supervisors, enabling them to visit the campus regularly and foster a focused collaborative environment.

The graduate school will be complemented by hiring senior researchers and postdocs at Cybercampus. This will accelerate cutting-edge research and enable more focused implementation of results in Sweden. Initially, in 2025, we plan to *hire 5 postdocs*.

Supporting Research Staff

The research environment at Cybercampus will also be supported by *long-term research engineers*, who will assist with software development and testing,

conducting experiments, maintaining open-source software repositories, and building and managing datasets, among other research support activities. These roles are essential to ensure continuity in research efforts, preventing work from being halted when a single project ends or when a PhD student or postdoc completes their tenure. To achieve this during 2025-2026, we plan to hire *two research engineers*.

Securing external funding from national and, primarily, international sources is crucial for Cybercampus research activities. Initially, we will focus on applying for EU Horizon Europe, MSCA, and EDF projects. To support this effort, we will allocate base funding for *1–2 full-time EU project coordinators* at Cybercampus.

Visibility and Internationalisation of Cybercampus Research

In order to attract top international talent (PhD students, postdocs, etc.), it is important that Cybercampus Sweden is seen as one of the main choices and a competitive place to carry out cybersecurity research. To achieve this, Cybercampus plans to: (i) host international cybersecurity academic conferences; (ii) offer short-term mobility grants to top international professors and researchers; and (iii) send Cybercampus research staff for short-term international exposure to world-class academic and industrial institutes. To disseminate Cybercampus research to a wider community in Sweden, we plan to organise an annual Cybercampus Research Conference.

Initially, 2025–2026, we plan to: offer *five incoming mobility grants* for international researchers to come to Cybercampus, offer *five outgoing mobility grants* for Cybercampus researchers to gain international exposures, and organise one annual trip for Cybercampus senior research staff to develop international cooperation. A mobility period could be 1-2 weeks.

Research Infrastructure

Cybercampus Sweden will create a network of large-scale cybersecurity research infrastructure that no single entity can build and maintain and make it available to multiple organisations. During 2025, we will study the currently available national infrastructure and investigate the possibility of offering access to cybersecurity partners. Cybercampus has already established a hacking lab and made it available to Cybercampus partners. The national cybercampus infrastructure will provide synergies with existing research and innovation facilities such as CRATE at the Swedish Defence Research Agency (FOI) and the RISE Cyber Range. Access to digital infrastructure owned by a single organisation is challenging and incurs costs that are hard to bear for individual research and academic entities. Cybercampus aims to eliminate the technical, legal, and economic hurdles and enable harmonised access for its partners.

Activity	Initial Staff (2025-2026)
PhD Students	10
Postdocs	6
Long-term Research engineer	2
EU grant coordinator	1-2
Infrastructure coordination and support	1

Long-Term Research

Long-term cybersecurity research is inevitable for Sweden due to the rapidly evolving nature of cyber threats and the increasing reliance on digital infrastructure in all aspects of society. Long-term research enables the development of advanced security solutions that can anticipate and counteract future threats, ensuring the ongoing protection of critical infrastructure, national security, and economic stability. It also helps to build a skilled workforce, establishes Sweden's leadership in the global cybersecurity landscape, and fosters innovations. Such long-term research is already funded by other Swedish and EU funding organisations.

Cybercampus plans to liaise with national funding bodies to fund long-term cybersecurity research in Sweden. We will establish closer interaction with industry, the public sector, and defence to fund basic exploratory research. Such externally funded long-term research activities could receive *20% co-funding from the Cybercampus* base funding, where needed.

Co-funding future Research Funding Opportunities

Cybersecurity research is funded through several sources and funding agencies nationally and internationally. Given the urgent need of increased cybersecurity, many funding agencies now have calls on cybersecurity topics and themes. In Sweden, a common model is that academia and industry share the responsibility for reaching a 50% co-funding of the total budget at project level. In Horizon Europe calls, the situation is different and 100% funding is more common. However, many of the cybersecurity calls are in the Digital Europe program where the total funding level is 50%. Also, the Eureka Clusters Programme (ECP) calls require co-funding. Cybercampus will analyse, support the application process, and co-fund calls that complement its mission-oriented research, either by filling a specific gap with foundational research or by supporting the implementation of a mission in a specific use case.

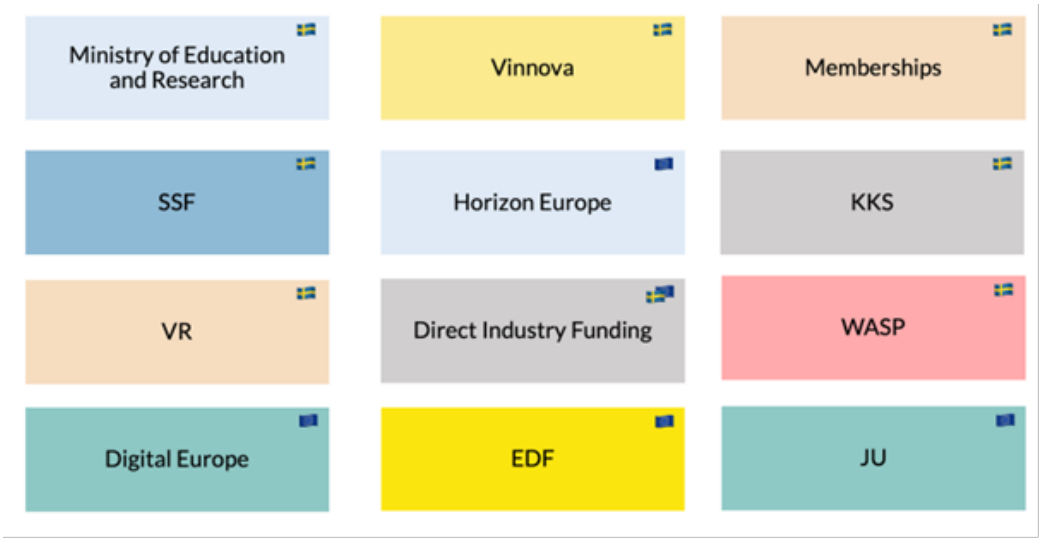


Figure 3: Significant funding sources for cybersecurity research in Sweden.

Cybercampus PhD Graduate School – Plan & Strategy

Vision

Cybercampus will engage in research education and will establish a National Cybercampus Graduate School for education and training of future cybersecurity experts.

This new graduate school will contribute to the overall vision:

> Cybercampus Sweden carries out cutting-edge cybersecurity **research education** that **goes beyond what is possible for an individual university**.

Background and motivation

Cybersecurity has to be assured cross-domain – it needs to be implemented and enforced in software, hardware and at network and application levels. Cybersecurity experts therefore require cybersecurity expertise in different technical domains. In addition, cybersecurity experts do not only have to possess technical cybersecurity knowledge, but they should also have an understanding of legal, organisational and human aspects of cybersecurity, especially if considering that the majority of security breaches are occurring due to human factors[1]. Additionally, even though the core of many of the research challenges that Cybercampus will address (as described in the Cybercampus research plan) are technical in nature, the Cybercampus graduate school should not only offer research education in technical cybersecurity aspects but should also teach and train interdisciplinary cybersecurity skills. Moreover, the graduate school should also teach and train future cybersecurity experts from non-technical disciplines, coming e.g. from information systems, social sciences, or law.

Thus, a cooperation of cybersecurity experts and researchers across technical domains and also across disciplines can contribute to an excellent and cutting-edge cybersecurity research education. Therefore, a cooperation of cybersecurity researchers across Swedish universities and departments, is essential and envisioned for providing a high-quality cybersecurity PhD education by Cybercampus Sweden.

For achieving this vision and cooperation, we can partly build on the well-established Swedish IT-Security Network (SWITS[2]) for PhD students and researchers, founded in 2001 and coordinated by Karlstad University (KAU). SWITS is an informal cooperation network for Swedish cybersecurity PhD students, and supervisors, which has received funding from MSB and comprises PhD students and researchers from more than 20 Swedish Universities and

research labs, and has successfully connected different cybersecurity PhD students, researchers and research groups in Sweden.

Despite the cybersecurity skills gap in Sweden and world-wide, the first cybersecurity graduate schools in Sweden were only established in the past 2 years. This includes the KKS-funded and newly established Swedish industrial graduate school on Cybersecurity (SIGS-CyberSec[3]) that funds industrial PhD students, coordinated by KAU, as well as a Graduate School on Cybersecurity that is currently established at Uppsala University[4]. Also, WASP (Wallenberg AI, Autonomous Systems and Software Program) is operating a graduate school[5], however focused on AI and Data Science, but has recently started to fund cybersecurity research projects and PhD students. A limitation of all existing graduate schools is, however, that these schools are restricted to a subset of Swedish universities and organisations. Hence, these graduate schools are not able to build on the complete potential and cybersecurity expertise that is existing in Sweden at different Universities and research labs.

National Swedish PhD Graduate School by Cybercampus – Goals and Approaches

Cybercampus will establish the first National Swedish Graduate School with co-funded PhD positions, which will be open to all Cybercampus partner organisations. All Swedish universities and research labs that conduct Cybersecurity research will be invited to join Cybercampus as a partner organisation. The Cybercampus graduate school will be designed to be inclusive and will also offer PhD students from non-Cybercampus partner organisations to participate in its courses, seminars and other activities.

The Cybercampus graduate school will be based on the following sub-goals, principles and approaches:

1. **Achieving EXCELLENCE THROUGH COOPERATION**

As outlined above, cooperation across universities / organisations in PhD research and research education will be key for achieving excellence. Therefore, Cybercampus will support:

- **PhD projects, co-supervised** by Cybercampus partners – PhD projects should be co-supervised by cybersecurity researchers with complementing expertise coming from different research groups / universities/ research labs. Cybercampus will co-fund PhD students, who will each be employed and/or enrolled by different Cybercampus partners (universities, or research labs, industry).

- **Joint working and meeting space & research infrastructure** at Cybercampus premises – While PhD students should be enrolled at

different Swedish universities, it will also be promoted that they will regularly visit Cybercampus for meetings, for PhD networking events and courses, or, if possible, that they come for long-term visits (secondments) to Cybercampus for enabling joint research cooperation with other Cybercampus researchers and PhD students. Alternatively, they could have their main working place at Cybercampus (see also below). A joint working and meeting space for PhD students at the Cybercampus premises will therefore be created, in addition to flex-office spaces for their supervisors. Being present at Cybercampus is also beneficial for utilising the joint research infrastructure, such as the hacking lab at Cybercampus with support of the research engineers.

- **Hybrid set-up with supported visits and secondments.** For promoting cooperation, the PhD students will be encouraged to spend a considerable amount of time at Cybercampus (and/or at other Cybercampus partner sites) for shorter or longer research visits while also being connected with their home universities. For enabling this, a hybrid setup with secondments, an instrument common in Marie Skłodowska-Curie Action (MSCA) doctoral networks, will be supported. As with MSCA, mobility grants supporting double household costs for the duration of secondments, will be paid by Cybercampus. Moreover, PhD students (and their supervisors) that are not located in Stockholm are specifically expected to also regularly visit Cybercampus and should, if possible, plan to stay parts of their secondments at Cybercampus together with other PhD students that work on a related research theme for enabling synergies between their PhD projects and joint work.

  We are envisioning a hybrid setup, where some PhD students either have their working place at Cybercampus or are located at the home universities where they are enrolled, or other Cybercampus partner organisations, where they are employed. (Please note that the percentages mentioned below are suggestions that have been discussed with other with SWITS partner organisations – final figures will need to be decided by the General Assembly).

  A PhD student position located at Cybercampus (even if enrolled at other universities than KTH) could be mostly funded by Cybercampus, e.g. with 70+% of the salary costs, while remaining salary costs should be covered by the home university. Besides, there will be mobility funding for visiting their home universities or organisations of their (co-) supervisors for longer secondments (e.g. for 1-2 months per year – 4-8 months in total) and regular research visits (e.g. for 1-2 visits per month). These PhD students can benefit better from the joint infrastructure and also contribute with up to 20% administrative of educational Cybercampus work as part of their administrative duties (which is motivating a higher Cybercampus funding than for PhD positions at other places). Especially, PhD students located in Stockholm (e.g. working for KTH, RISE, FHS, or SU)

should preferably have Cybercampus as their working address and location for promoting cooperation.

- PhD students that are employed and have their working addresses at other Cybercampus partner organisations will receive slightly less funding by Cybercampus, e.g. 60% of their salary costs plus mobility grants, while the employing Cybercampus partner should cover the remaining salary costs. The mobility grants should enable them to spend also a considerable time at Cybercampus (e.g. funding for at least 1-2 months per year – 4-8 months in total) or at cooperation partners including the co-supervisors' organisations and to regularly visit Cybercampus (funding for at least 1-2 visit per month). These PhD students located at other partner organisations could still conduct up to 20% institutional duties for Cybercampus with funding from Cybercampus for these duties (in addition to the 60% funding of salary costs). This could entail that they are spending more time at Cybercampus and /or that they are involved online for contributing to Cybercampus' activities, such as for instance education or infrastructure development.

- **Cooperation in PhD education** – All Cybercampus partners that are employing co-funded PhD positions should also develop and offer new PhD courses or at least develop course elements or hold seminars for Cybercampus PhD students and other cybersecurity PhD students in Sweden (as part of their co-funding efforts for Cybercampus partnerships). Hence, Cybercampus partners should not only co-fund PhD positions through covering parts of the salary costs but should also co-fund and support the graduate school through an active engagement in the PhD courses that will be offered.

- **Cooperation in PhD research** – PhD students should cooperate on related PhD topics. Currently, the draft Cybercampus research plan defines 10 research areas of importance for Sweden. For enabling cooperation, 2 – 3 research areas with highest priority should be identified, on which the (planned) 10 Cybercampus PhD students, who will be hired and enrolled in a first round, should jointly cooperate (to prevent that 10 PhD students are hired for 10 different and disjoint topics).

2. **Offering CROSS-DOMAIN & INTERDISCIPLINARY EDUCATION, Open for all PhD students in Sweden**

For training and educating future PhD students, the graduate school will develop and offer a range of cybersecurity seminars, courses that teach topics across domains. Research and PhD education in Cybercampus will address various technical cybersecurity challenges, as well as interdisciplinary cybersecurity aspects (legal, social, organisational). These are regarded as important for

educating cybersecurity experts and will therefore also be taught in the graduate school involving e.g. lectures from information systems / social science and law. All seminar and course offerings shall be open for all PhD students in Sweden, independent of whether their home universities are Cybercampus partners or not – hence, in contrast to existing graduate schools, Cybercampus will take an inclusive approach.

In particular, Cybercampus will organise the following type of offerings:

- Joint broadening and deepening **cybersecurity PhD courses** – which will be newly developed and offered to all PhD students in Sweden. PhD students that are officially part of the Cybercampus graduate school should jointly attend also a number of mandatory Cybersecurity courses (to be developed) that will address cybersecurity topics of high relevance for the prioritised research area and should in total comprise around 15 credits points – joint courses will also promote communication and cooperation among Cybercampus PhD students. (We intend to limit the number of mandatory PhD course points to 15 credits, as requiring more mandatory course points, as e.g. the WASP PhD school does, may restrict the student's freedom in choosing other courses of interest/need).

The Cybercampus graduate school also plans to include the course offerings that have already been developed for the SIGS-CyberSec graduate school (and the Uppsala graduate school).

- Regular **research seminars** & **annual SWITS seminar** – Cybercampus will regularly offer research seminars at Cybercampus or other places, and in hybrid form.

Moreover, it will support the SWITS network, which will in future be funded and organised via Cybercampus and it will continue to organise annual SWITS seminars, which will be open for all Cybersecurity PhD students and researchers in Sweden.

3. **Support INTERNATIONALISATION**

The Cybercampus graduate school will also support internationalisation by establishing international cooperation involving PhD students. To this end, it will organise and fund (individual or joint) exchange visits to other European Cybersecurity excellence centres hosting graduate schools (e.g. at Athene in Germany or the Swiss Excellence Centre) and will support secondments at international partners.

Cybercampus partnership engagement in the National graduate School:

While the educational offerings and SWITS activities are planned to be open to all Cybersecurity PhD students in Sweden, the graduate school also includes some offerings that are exclusive for Cybercampus partner organisations.

Cybercampus partners are expected to co-fund Cybercampus (1 MSEK per year) activities and these offerings will also largely require parts of this co-funding by the partner organisations.

The funded exclusive offerings by Cybercampus for its partners include:

- Co-funded PhD positions – Cybercampus will cover the travel and mobility costs and the majority of salary costs – we envision at least 70% of the PhD student salary costs for PhD students place at Cybercampus, and 50-60% of the salary costs for PhD students that have their working place at other partner organisations. Moreover, it funds the mobility grants for secondments and site visits mentioned above.

- Offering of working and meeting space at Cybercampus for PhD students plus flex-office space for supervisors and visiting PhD students

- Support for using the joint technical research infrastructure and assistance by research engineers and software developers

- Organisational support for establishing exchanges, secondments and cooperation

- Seminars with regular follow-ups and feedback on PhD projects by peers and other senior advisors

- PhD education and courses that are specifically designed for prioritised research themes that the PhD students will address

- Organised international research visits and trips, sponsored social activities and (in future) summer schools

- Opportunity to meet international cybersecurity experts that are invited at Cybercampus

What the universities / partners are expected to co-fund /contribute with for building up and running the graduate school:

- Partners hiring the PhD students are expected to cover the remaining salary costs – this co-funding can come from the university's own research resources or via matching/complementing research funding

- Supervision costs (at least 5% of the main supervisor's time and 8% supervision time in total)
- Office space costs at home university, publication costs.
- Course development costs for at least one PhD course, or parts of one PhD course, or seminar/lecture series
- Regular visits by supervisors to Cybercampus or to cooperation partners
- ….

Criteria for assigning PhD students to partners/main supervisors:

While Cybercampus should offer an inclusive research school, the funding for the PhD positions should not simply be equally distributed to all Universities and partners (and the Cybercampus funding would also volume-wise not allow to co-fund PhD positions at all Swedish universities either).

For achieving the main objective of **cutting-edge and outstanding research and research education**, the following criteria related to experiences, expertise and excellence, should be primarily considered when making a prioritisation of this first round of PhD student recruitments for establishing the graduate school. For a future second round of PhD student enrolments, other criteria could be applied for supporting main supervision by less experienced senior researchers, who need to gain supervision experiences for their competence development and/or for supporting new or smaller cybersecurity research groups that need to grow or are just starting PhD programs.

Partners/main supervisors should be prioritised in the first round according to the following criteria:

- Signed partnership agreement with guaranteed co-funding (of at least 1 MSEK per year, covering also parts of the costs for the PhD position)
- Main supervisors with excellent research track records in the prioritised research fields
- Very well-established research environments with a long track record for Cybersecurity research (with preferably at least 2 Docents or Professors in Cybersecurity)
- The universities, where the students should be enrolled, should also have a well-established PhD program for cybersecurity students in place

- Main supervisors with sufficient committed time/capacity (they should in total not supervise more than 5 PhD students). They should also commit to contribute with developing courses or course elements and travelling regularly to Cybercampus or other partners, help to organise PhD activities and study trips, …

- Experience in PhD supervision (preferably Professors / Docents having already supervised PhD students until graduation) research

- Excellent PhD supervision team with co-supervisors from other Universities or from other disciplines with complementing expertise

- Previous engagement for Cybercampus

- A research topic is briefly outlined by the supervisor(s) within the prioritised research areas or Cybercampus with potential high scientific and societal impact for Sweden

- ….

Criteria for assigning secondary (co-)supervisors:

- 2 co-supervisors should be assigned – at least one of them should come from another partner organisation or department than the one of the main supervisors. Co-supervision can also strengthen the interdisciplinarity if supervisors come from different areas.

- Signed partnership agreements with the organisations of the co-supervisors. (One of the two co-supervisors can also be from an international partner (e.g. University in another country) – then this requirement for a partnership agreement does not apply).

- Important complementing expertise of high relevance for the PhD project. Interdisciplinary complementing expertise is especially welcome.

Who decides about PhD student assignment and enrolment?

- All partner organisations can apply for employing co-funded positions, stating also a suggested supervising team, research area and outlining the PhD topic. They should also specify how they can contribute to the PhD graduate school curriculum – the application should be easily filed (no detailed/lengthy research proposal required).

- An assignment will be done according to the criteria by Cybercampus. The evaluation of applications and proposed assignments will be done by the Head of the Graduate School, the Research Director, the Deputy Director, and the Research Coordinator of Cybercampus on behalf of the Cybercampus Management Board. Possibly further external experts can be involved.

Cybercampus Sverige Innovation Strategy 2025-2027

Executive Summary

This document presents the Innovation Strategy for Cybercampus Sverige for 2025-2027. The main objective is to establish a national cybersecurity innovation platform and promote a culture of continuous business innovation. The aim is to ensure a high level of cybersecurity in Sweden through collaborative partner-based innovation, startup incubation, and acceleration.

Introduction

Cybercampus' mission is to drive agile and cutting-edge joint research, innovation, and education in cybersecurity and cyber defence, far beyond what individual universities, institutes, companies, or government agencies can achieve on their own. By uniting forces across different disciplines and all sectors of society, Cybercampus addresses needs that no single actor in the cybersecurity field currently meets.

This Innovation Strategy outlines the vision, mission, strategic objectives, and framework for the innovation operations of Cybercampus.

Innovation can involve creating value from new knowledge, new technology, or implementing existing solutions in a new way (e.g., Product-as-a-Service, outsourcing) or in a different context (e.g., from private to public sector, from civil to military use, or vice versa).

Most innovation occurs within existing organisations in both the private and public sectors. Not all innovation will result in new offerings to customers or stakeholders, but it will still create value for the organisation by increasing efficiency or enabling compliance. For Cybercampus, it is crucial to enable and support our partners' innovation ambitions related to cybersecurity.

In recent years, there has been increased attention on innovation through the incubation of new companies, known as startups. The Swedish ecosystem for startups has enabled quite a success over the last decades, attracting increased attention from international venture capital. For Cybercampus, it is important to ensure this success extends to cybersecurity startups as well through collaboration with and by strengthening and complementing already ongoing activities.

This Innovation Strategy has been developed by Cybercampus' Innovation pillar staff building on material from the workshops in the planning phase of Cybercampus and the results of the two partnership co-creation events in December 2024 and February 2025.

The Innovation Strategy itself has been approved by the Cybercampus Management Team and is to be confirmed at the General Assembly during spring 2025.

Vision and Mission for Cybercampus Innovation

Vision

To be the leading entity in Sweden for partners seeking support in their cybersecurity innovation ambitions and to serve as the nation's unifying force for supporting new businesses, funders, and investors in cybersecurity.

Mission

The primary mission is to deliver solutions and support that catalyse impactful cybersecurity innovation, meeting the evolving needs of our partners by leveraging technology, creativity, and expertise, particularly through Cybercampus' Research and Education pillars.

The mission also includes collecting Sweden's opportunities for cybersecurity startups complemented with any critical missing parts to enable a full nationwide incubation support (Detailed in Section 5.3 Incubation and Acceleration.)

Strategic Objectives

The strategic objectives of **Cybercampus** are to:

- **Become Sweden's coordinating entity for cybersecurity innovation:** Establish a robust structure, methodologies, and representation to align with the expectations of Cybercampus stakeholders, both nationally and internationally, including prospective partners.

- **Drive Innovation from Mission-Oriented Research**: Organise activities and support related to results from activities in the research pillar to catalyse partners' innovation and startup incubation.

- **Partner-Centric Approach**: Focus on understanding and meeting the needs of Cybercampus partners to build long-term relationships and ensure partner satisfaction.

- **Increase Flow and Volume of Cybersecurity-Related Innovation:** Implement activities for Cybercampus partners to generate ideas and catalyse impactful cybersecurity innovation collaborations that can generate values for our partners.

- **Increase Cybersecurity-Related Startup Flow**: Boost incubation by activities and attractive support.

- **Improve Success Rate for Cybersecurity-Related Startups**: Build networks of relevant actors for support and financing for growth.

- **Increase the Cybersecurity Knowledge in Swedish Education for Innovation and Entrepreneurship**: Identify and offer relevant courses or content to such education programs.

- **Increase Innovation and Entrepreneurship Abilities in Cybersecurity Education**: Identify and offer relevant courses or content to such education programs.

Innovation Framework

An effective innovation framework is essential for supporting idea generation, catalysing collaborations, and fostering incubation and acceleration of startups.

This framework will encompass several key components:

Idea Generation and Management

A structured process for collecting and nurturing innovative ideas is crucial and is how Cybercampus will manage idea generation for cybersecurity-related innovation. This includes the following activities:

- **Innovation Catalysts**: Organise activities where creative thinking is encouraged, and new ideas can be shared, refined and tested.

- **Collaborative Platforms**: Implement physical and/or virtual arenas and events to facilitate idea sharing and collaboration among partners.

- **Hackathons and Competitions**: Organise events that stimulate innovative thinking and problem-solving in high-priority areas.

The prioritisation of the idea generation activities will primarily be determined by the degree of engagement from the Partners

Research-Based Innovation

Existing cybersecurity research is of particular interest for catalysing innovation. Cybercampus will actively work to bridge the gap between research and impactful implementation in Cybercampus partners' businesses. This will be done by identifying and encouraging application and commercialisation of research. This, in turn, implies identifying and encouraging researchers, to engage in innovation, either in collaboration with Cybercampus partners or for direct commercialisation in a startup.

Note that Cybercampus mission-oriented research is expected be a major source of this kind of research-based innovation. Partners might implement results from

Cybercampus research in their own businesses. Cybercampus will also work actively to catalyse commercialisation and incubation of its research results.

Some research results may be too far from application to inspire innovation. Cybercampus will actively encourage and coach researchers to bring their results closer to application and innovation. An investigation of funding opportunities for such work will be initiated to help eliminate lack of financing as an obstacle.

Partner-Based Innovation

Exchange of ideas between Cybercampus partners is another impactful driver of innovation to be considered. This has been successfully exercised in thematic co-creation events in which as many perspectives as possible are represented and considered. These have already generated new ideas and innovation initiatives. Such thematic co-creation events are one of the initiatives Cybercampus will use to drive partner-based innovation.

Another initiative to drive innovation is to have partners present their cybersecurity-related innovation ideas and/or needs to each other in innovation brokerage and matchmaking events aimed at shaping partner collaborations to meet existing partner needs or even to create joint ventures as spinoffs of collaboration.

Challenge-Driven Innovation

Another way to drive innovation is inviting partners to present cybersecurity-related challenges. Some challenges can be suitable for student or master thesis projects.

A general tool for partners to present such challenges and opportunities to students has been well received at individual Swedish universities. Cybercampus' ambition is to provide this kind of tool for all cybersecurity students in Sweden with cybersecurity-related challenges from all interested Cybercampus partners.

Innovation competitions for entrepreneurial teams are known to increase the number of startups. These can be based on challenges from sponsoring partners while hosted by Cybercampus. Cybercampus can also assist partners in hosting and/or attracting teams for cybersecurity-related hackathons.

Management of Innovation Ideas and Proposals

Given the diverse innovation expectations and needs of Cybercampus' partners, idea-generation activities will prioritise fostering a high volume of creative ideas and proposals over focusing solely on quality or depth. A substantial flow of creative ideas often leads to the emergence of even more innovative concepts. The greater the number of ideas, the higher the likelihood that partners will encounter something relevant or intriguing. The ambition of Cybercampus will be to facilitate various arenas and activities for idea generation designed to enable and stimulate a significant flow of ideas and proposals.

To identify the ideas with the best potential for success and impact, it is important to have opportunities to test numerous concepts, understanding that many may fail but will do so swiftly. Cybercampus will encourage the initiation of multiple short-term collaborations to rapidly test ideas that have garnered interest from partners.

Given that timing is a significant challenge in the commercialisation of ideas, Cybercampus will oversee the management of innovation ideas and proposals over time. It is likely that some ideas will exhibit high potential but may be premature for commercialisation or other impactful implementations. Therefore, Cybercampus will systematically collect and manage these proposals. Subsequently, on Cybercampus' initiative, previously rejected proposals with high potential will be periodically reviewed and re-presented to partners.

In summary, Cybercampus intends to implement innovation idea management that encourages idea generation, facilitates collaborations and incubations, promotes rapid testing, and manages ideas and proposals over time.

Collaboration and Networking

Building strong networks and partnerships is essential for successful innovation. Strategies include:

- **Engage the Cybercampus Network of Partners**: Actively involve the Cybercampus network of partners in various initiatives.
- **Engage National Cybersecurity Communities**: Connect with national cybersecurity communities to leverage their expertise and resources.
- **Research/Innovation Consortia**: Form consortia focused on specific innovation challenges to pool knowledge, enable synergies, and drive results.
- **Public-Private Partnerships**: Foster collaborations between partners from both public and private sectors, typically involving experts and researchers from academia, institutes and industry to leverage diverse expertise and resources.
- **Innovation Procurement in the Public Sector**: Develop and test prototypes for innovation in collaboration with private actors, including startups.

Many of Cybercampus’ intended partners are already active in different kinds of collaborations, some of which are facilitated by Cybercampus. Cybercampus will continue to catalyse, facilitate and support these collaborations. All Cybercampus partners will regularly be invited to various networking events including

conferences and idea generation initiatives. The idea generation initiatives above in Idea Generation and Management will be used to catalyse new collaborations for innovation by pitching of ideas and matchmaking for partner collaboration.

There are many other initiatives for innovation in Sweden, some of which are focused on cybersecurity. The Cybernode, run by RISE for NCC-SE, is one of the most important ones. It has groups focusing on various themes and aspects of cybersecurity by engaging the cybersecurity community nationwide. Those thematic groups play a central role for idea generation and support ensuring that innovations address real-world needs and gain wider acceptance. Collaboration with the Cybernode is highly prioritised by Cybercampus.

For innovation in organisations in the public sector there is an opportunity to develop and test prototypes for innovation together with private actors, including startups. This is called Innovation Procurement and has recently been successfully implemented in projects co-funded by Vinnova. The lessons learned from those projects will be used to support partners from public sector in their innovation collaborations facilitated by Cybercampus.

Wherever there is an identified opportunity for innovation collaboration between partners Cybercampus will support the creation of consortia for that collaboration if needed. Some of Cybercampus' partners are likely to more often take on the task of coordinating or managing such consortia given their long experiences of such roles.

Incubation and Acceleration

Cybercampus initiatives for start and growth of startups include:

- **Stimulating the Formation of Entrepreneurial Cybersecurity Startup Teams**: Encourage the creation of new cybersecurity startup teams.
- **Building on Existing Startup Support Networks**: Create partnerships to support innovation efforts nationwide.
- **Mentorship Programs**: Connect startup teams with cybersecurity experts and experienced business mentors who can provide guidance and support.
- **Funding Access**: Help startups secure the necessary funding through grants, investments, and partnerships.

Since Cybercampus has a nationwide responsibility, these initiatives will need to be valid across Sweden. Sweden has a well-functioning ecosystem for tech startups

in general with nationwide incubation support, funding and even early investments. The latter at least in parts of Sweden. Some of Cybercampus' partners have more experience of supporting cybersecurity-related startup teams.

University partners have innovation offices with incubation support. Some of them have related acceleration activities, like LEAD, in collaboration with Linköping University. LEAD is also the partner appointed from Sweden for NATO's DIANA, an accelerator to find and accelerate dual-use innovation capacity across the alliance.

Other incubators and accelerators, like for example STING or Digital Well Ventures, with experiences from supporting cybersecurity-related startups are also important to connect with. Cybercampus will build on the existing initiatives for incubation and acceleration of cybersecurity-related startups with the goal to ensure startup support all the way from forming entrepreneurial teams, over incubation and funding to first rounds for financing with venture capital. As this already exist at some locations, the challenge will be to provide similar support nationwide.

Innovation Competitions for entrepreneurial teams are known to increase the number of startups by offering attractive prizes and opportunities to showcase to potential customers or partners. There are related examples in Sweden, such as MobilityXlab's international challenges for mobility startups. There are also international examples of cybersecurity startup competitions worth studying. Hosting a Cybersecurity Innovation Challenge might boost the number of startups in Sweden. Cybercampus will investigate organising such an event to benefit the Swedish startup community.

Cybercampus will support Swedish cybersecurity startups by reducing obstacles, offering resources, fostering collaborations, informing about funding, and provide ing office space. Cybercampus will act as a central hub for support and coordinate efforts within the Swedish startup ecosystem to boost the success of these startups.

If support is insufficient, Cybercampus will help bridge the gaps. Cybersecurity experts hosted at Cybercampus provide technical advice and associated experienced entrepreneurs offer business guidance. If sufficient startup mentoring is lacking, Cybercampus will address this need as well.

Cybercampus will connect startups with investors, attracting early-stage backers and venture capital. By fostering relationships with Swedish cybersecurity startups, Cybercampus aims to boost investor interest in these ventures.

Cybercampus first steps related to Sweden's opportunities for cybersecurity startups will be to reach out to actors all over Sweden already engaged in incubation and acceleration of cybersecurity-related startups to identify synergies and opportunities.

Education and Innovation for Cybersecurity

Sweden has education programs centred on innovation and entrepreneurship. Students in these programs often become entrepreneurs or intrapreneurs, enhancing cybersecurity awareness. Cybercampus will explore opportunities for adding cybersecurity courses to these innovation and entrepreneurship programs. Cybersecurity students may foster innovation by becoming more entrepreneurial. Cybercampus will explore opportunities to add innovation and entrepreneurship courses to cybersecurity programs. Cybercampus, along with its education partners, will explore these opportunities during 2025/2026, aiming for implementation by 2027/2028.

Collaboration and Partnerships

Organisations in Sweden and abroad can significantly contribute to Cybercampus Innovation. The Swedish Cybernode, see above, is of primary interest for deeper innovation collaboration.

Cybercampus aims to collaborate with all Swedish incubation, acceleration, funding, and financing actors relevant to cybersecurity startups.

The European Digital Innovation Hub (EDIH) Sweden Secure Tech Hub helps Swedish organisations improve their cybersecurity. All EDIH entities in the EU, including Sweden, support digital innovation in SMEs and the public sector, requiring cybersecurity. The EDIH Health Data Sweden has already indicated interest in collaboration with Cybercampus. Cybercampus will explore partnerships with these EDIH entities to boost cybersecurity innovation.

IPR regulation

Each innovation collaboration may create copyrightable software, novel designs, or patentable inventions. Intellectual property rights for these results should be individually regulated and agreed upon, unless covered by the Cybercampus Framework Agreement.

Management, Monitoring and Evaluation

The General Assembly decides at least every third year on the Innovation Strategy.

The Director of Cybercampus through the Head of Innovation is responsible for the implementation of Cybercampus Innovation Strategy and related operations with support from an Innovation Lead, Project Manager Innovation, or Business

Development Manager for Innovation and the Cybercampus team for events and communication. Head of Innovation reports to the Cybercampus Director.

Implementation Considerations

The success of this Innovation Strategy depends largely on the involvement of Cybercampus partners. Some activities require collaboration, while others can be started independently. The following prioritised activities reflect this approach:

Framework implementation

Idea Generation and Management

Research-based Innovation

Cybercampus will invite and stimulate researchers and PhD students to present cybersecurity-related proposals for impactful implementation in industry or public sector including civil and military defence. A pitching event for this would preferably be coordinated with a relevant conference or similar national event attracting both researchers and potential partners. With sufficient interest from researchers this could be arranged in 2025.

Partner-based Innovation

Once Cybercampus attracts enough relevant partners, partner-based innovation can begin. Cybercampus will invite partners to share opportunities and needs, fostering innovation collaborations. Small cybersecurity companies will likely offer opportunities, while industry or public sector partners may present needs. All opportunities for collaboration will be promoted.

Challenge-Driven Innovation

Before partners can offer challenges, Cybercampus can provide a general cybersecurity challenge. Cybercampus will explore organising a Swedish prize for cybersecurity innovation by 2025.

Cybercampus will also investigate how to provide a tool for partners to present cybersecurity challenges for students nationwide by winter 2025/2026.

Collaboration and Networking

Networking with all relevant Swedish actors engaged in cybersecurity-related innovation has been initiated and is of highest importance for Cybercampus. It will be continuously developed and maintained. It includes both actors engaged in partners' innovation as well as the startup ecosystem.

Cybercampus will actively foster collaboration and undertake initiatives to advance cybersecurity innovation. This includes operational cooperation with Cybernode and support for the formation of consortia aimed at addressing specific national interests. Collaborative efforts involving partners will be given priority.

To attract partners from the public sector, Cybercampus will explore appropriate forms of innovation for the public sector, including innovation procurement.

Innovation-stimulating and catalysing networking activities will be implemented in collaboration with committed partners. For instance, a co-creation or matchmaking event can be organised given sufficient engagement from the partners.

Incubation and Acceleration

Cybercampus will actively engage with cybersecurity startup incubators, accelerators and financiers across Sweden to coordinate efforts, identify synergies and build a comprehensive national support system.

Education and Innovation for Cybersecurity

The initiatives outlined in this Innovation Strategy pertaining to Education will be executed in conjunction with the implementation of the Education Strategy.

Collaboration and Partnerships

Cybercampus will prioritise partnerships and collaborations within Sweden, focusing on the implementation of the Innovation Framework as outlined above.

International partnerships and collaborations will be considered based on opportunities in collaboration with Cybercampus partners in Sweden.