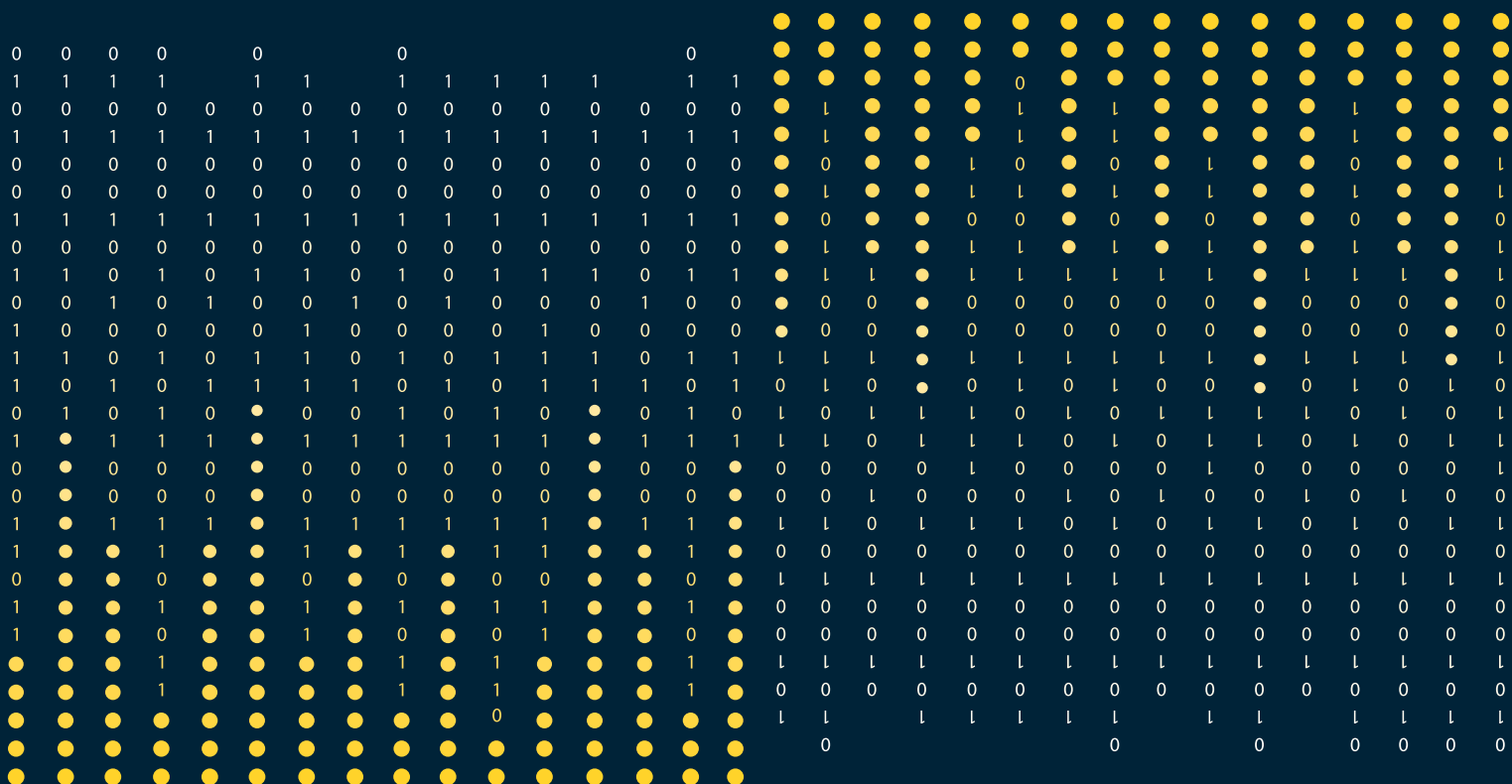


Annual Report 2024





Introduction

Cybercampus Sverige (hereinafter Cybercampus) came about in early 2021. The idea emerged to bridge the knowledge gap in digitalisation and cybersecurity, inspired by similar initiatives in Sweden and Europe. In early 2022, a joint planning project was launched by KTH Royal Institute of Technology, the Swedish Armed Forces, Research Institutes of Sweden (RISE), Karlstad University, The Swedish Civil Contingencies Agency (MSB), Saab, and Ericsson. The concept was presented in April 2022 at a cybersecurity symposium at KTH, in the presence of King Carl XVI Gustaf, Queen Silvia, and Crown Princess Victoria. A series of workshops and study visits, held through the summer of 2023, helped to anchor and further develop the concept.

In the autumn of 2023, the Swedish government decided to fund the initiative from 2024. In February 2024, Cybercampus was inaugurated, and efforts since then have focused on establishing a stable structure for long-term operations and funding. So far, 24 organisations have expressed their intention to become formal partners, and our partnership model will be launched during the first half of 2025.

During its first year, Cybercampus – both independently and in collaboration with others – organised seminars, conferences, and cybersecurity competitions. Our events reached invited decision-makers and experts as well as a broader audience. Researchers and experts in cybersecurity, AI, information operations, and representatives from innovative companies have shared their knowledge. Cybercampus also supported initiatives such as the Swedish National Hacking Team, which has demonstrated success at the European level. At the end of 2024, we hosted the Minister for Foreign Affairs’ launch of Sweden’s international cyber and digitalisation strategy, and we also organised a partnership co-creation event.

While joint research, continuing education, and innovation efforts have kicked off, long-term planning continues. Our international

collaboration already includes partnerships with Nordic cybersecurity initiatives, the European Union Agency for Cybersecurity (ENISA), and exchanges with Germany, Belgium, and Estonia.

The growing cybersecurity skills gap, rapid technological development, societal digitalisation, a worsening global security situation, and cross-border IT crime all underline the need for secure digital infrastructures and services. As a unifying national force, Cybercampus creates optimal conditions for interdisciplinary knowledge sharing, innovation, and long-term competence development. The initiative has been shaped in collaboration with over 50 organisations and more than 160 experts through workshops, interviews, meetings, and discussions since 2022. With funding from Vinnova, Sweden’s innovation agency, and the Technology Industries of Sweden’s Advanced Digitalisation program, combined with strong support from decision-makers and the government, our vision is more than a groundbreaking idea – it already has tangible results to build upon.

Happy reading!



Photo: Christopher Andersson

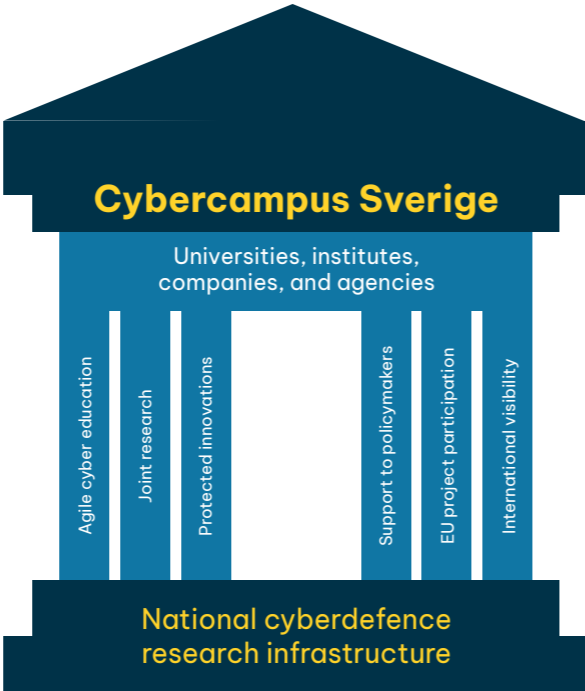
David Olgart
Director, Cybercampus Sverige
December 2024

Table of contents

Editorial	3
About Cybercampus Sverige	4
Highlights 2024	6
Education	8
Research	10
PhD Education and Graduate School	14
Innovation	15
Partnership Offer	17

About Cybercampus Sverige

Cybersecurity is crucial to Sweden’s digitalisation. Building and operating digital systems is challenging – it requires high expertise, national collaboration, and an interdisciplinary approach to protect our vulnerable systems and infrastructures.



Cybercampus’ mission is to drive groundbreaking research, innovation, and education in cybersecurity and cyber defense – far beyond what individual universities, institutes, companies, or government agencies can achieve on their own. By uniting forces across all sectors of society, we address needs that no single actor in the cybersecurity field currently meets.

Sweden has great potential to rapidly strengthen its cybersecurity. Research is conducted nationwide on technical solutions, legal frameworks, administration, and behavioural aspects of cybersecurity, among other areas. Our higher education institutions, both universities and university colleges, offer modern and high-quality education. With support for innovation, incubation, capital, and entrepreneurial expertise, all the necessary building blocks are in place. Cybercampus brings together this expertise and capacity.

However, we face challenges such as understaffing, a shortage of specialists, and disruptive workforce turnover. Growing demand is straining available resources, making it equally important to spark interest in cybersecurity among the general public. The Eurobarometer Cyberskills 2024 study shows that 56 percent of cybersecurity teams consist exclusively of men and that 32 percent of teams include at most one woman. To enhance decision-making and foster innovation, diversity is essential. In 2024, we networked with important organisations such as Women4Cyber and Security Divas, and we plan to participate in Introduce a Girl to Engineering Day (IGEDay) 2025.



Movitz Sunar is a former team member of Sweden’s National Hacking Team (SNHT), Project Manager at Kodsport Sverige and project manager for the Security Swedish Championship. Movitz has a strong interest in policy issues within cybersecurity and aims to enhance Sweden’s capabilities in the cyber domain.

How do we engage young people in cybersecurity?
We should create role models that inspire and normalise ethical hacking. Sweden also needs to reach young people earlier and on a larger scale to generate the best offensive and defensive skills. To inspire, a concentrated effort is required at an early age.

What do you expect from Cybercampus?
At Kodsport Sweden, we look forward to a continued good collaboration with Cybercampus, which is currently doing a great job supporting several organizations with networking, administrative support, and expertise. We expect this important work to continue.



The panel discussing the future cyber workforce at the inauguration of Cybercampus, Anne-Marie Eklund Löwinder, Eva Fogelström, Kristina Bjerka, Anastasiya Kornitska.

Highlights 2024



Photo: Sanna Johannesson, Blackbox Videoproduktion AB

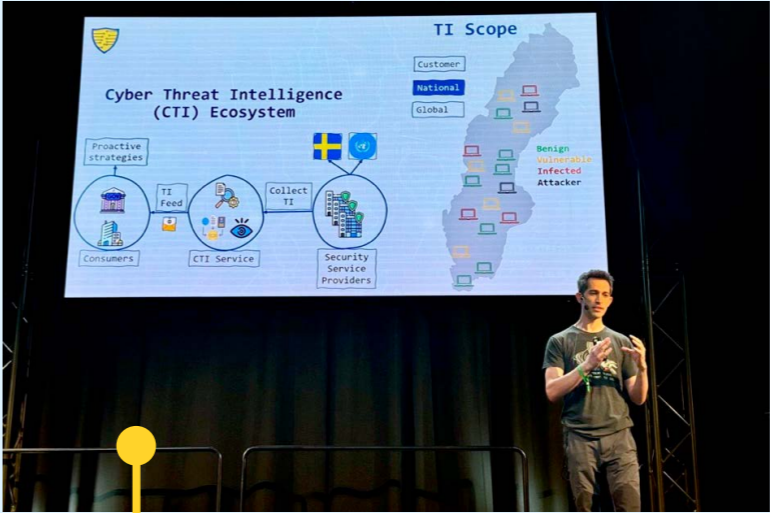
In February, Cybercampus was formally launched at a ceremony at the new headquarters in Stockholm. The inauguration featured a full-day program focused on Cybercampus’ mission to contribute to a safer and digitally resilient future for Sweden. The day began with a ceremony that included presentations and speeches by, among others, the Director of Cybercampus Sverige, David Olgart, KTH President Anders Söderholm, Minister for Civil Defence Carl-Oskar Bohlin and Minister for Education Mats Persson. After the ceremony, the 180 guests visited the exhibition on cybersecurity education in Sweden and attended workshops on research and education.

February – Cybercampus inauguration

April – Cybernode Round Table discussions

May – SWITS Conference

June – Midnight Sun CTF



In June, Midnight Sun was organised by Cparta, together with Cybercampus, Saab, SEB, and others. Midnight Sun is one of the world’s top-ranked Capture-the-Flag competitions and a three-day conference featuring seminars, panels, and workshops. This year’s theme was “Cyber Conflicts: The Tools and Techniques of Tomorrow” and the discussions focused on offensive security, advanced exploitation methods, reverse engineering, vulnerability detection, and various cyber strategies. Pictured: Dr. Emre Sören, Cybercampus.



Photo: Sanna Johannesson, Blackbox Videoproduktion AB

In December, Cybercampus hosted the launch of Sweden’s foreign and security policy strategy for cyber and digital issues. The emergence of new strategic, digital technologies contributes to new possibilities for economic growth and development but also create challenges in security policy. The Government’s strategy aims to strengthen Sweden’s role and promote Swedish interests in the global digital landscape. Pictured: Minister for Foreign Affairs of Sweden, Maria Malmer Stenergard.

September – ENISA Conference, Research workshop, Launch of Cyberlyftet

October – Cyberlov, MSB Cybersecurity conference

November – Säkerhets-SM

December – Launch of strategy for cyber and digital issues, Partnership co-creation event

Education

Swift action is needed to meet the urgent skills demand in cybersecurity across both the private and public sectors. The most pressing need is to provide professional training for specialists as well as courses for other roles that require greater cybersecurity responsibility. Training must be flexible – often offered part-time – to suit working professionals.

Through agile work processes, we adapt existing courses to meet professional needs while identifying gaps that require new programs, courses, tests, and exercises. Cybercampus is a network that spans higher education institutions and university colleges. We also collaborate with the public sector and the business community to offer an attractive catalogue of courses.

“Cybercampus is conducting a thorough effort to ensure cybersecurity competence for Sweden.”

We contribute to strengthening cybersecurity expertise in Sweden through collaboration between academia, industry, and the public sector. Our partners include MSB and the Swedish Coordination Centre for Cybersecurity Research and Innovation (NCC-SE), which provides us with international links to the European Competence Centre for Cybersecurity (ECCC). We also cooperate with ENISA and recently participated at the Cybersecurity Skills Framework conference in Budapest. Cybercampus is a member of the Nordic-Baltic think tank Cyber Bridge Forum, funded by the Nordic Council of Ministers. Our training offerings are designed primarily for professionals in both the public and private sectors. In the spring of 2024, we took part in writing a successful proposal to

the EU Digital Europe call Cybersecurity Skills Academy, together with 16 partners in ten EU countries. The project – aimed at sharing and developing cybersecurity education targeted towards professionals in small and medium enterprises and the public sector – will start in January 2025.



The European Network and Information Security Agency (ENISA), launched in 2004, aims to develop research, innovative solutions and connect academics with industry. Cybercampus attended the annual ENISA conference in Budapest. As always, EU initiatives give international perspectives and the chance to learn from other nations' success stories and challenges.

“Our training offerings are designed primarily for professionals in both the public and private sectors.”



Photo: Fredrik Persson

In partnership with RISE, we have launched the introductory program Cyberlyftet, which has already attracted thousands of participants. A course targeted at managers and decision-makers is also under development. To promote long-term competence development, we work with various stakeholders to inspire young people to pursue a career in cybersecurity. Throughout the year, we hosted initiatives such as Cyberlov and the Säkerhets-SM competitions at our facilities.



Cyberlyftet provides a basic understanding of how to protect digital systems, networks, and data against cyber threats. Through a number of chapters and practical exercises, users learn how to identify and deal with various cyber threats. Cyberlyftet is a free online course which requires no previous experience and is available to anyone interested in developing their cybersecurity skills. RISE did an incredible job creating this and we are proud to work with them.



Karin Omsén, Rector, Yrgo, higher vocational education and training

How can Cybercampus collaborate with vocational colleges?

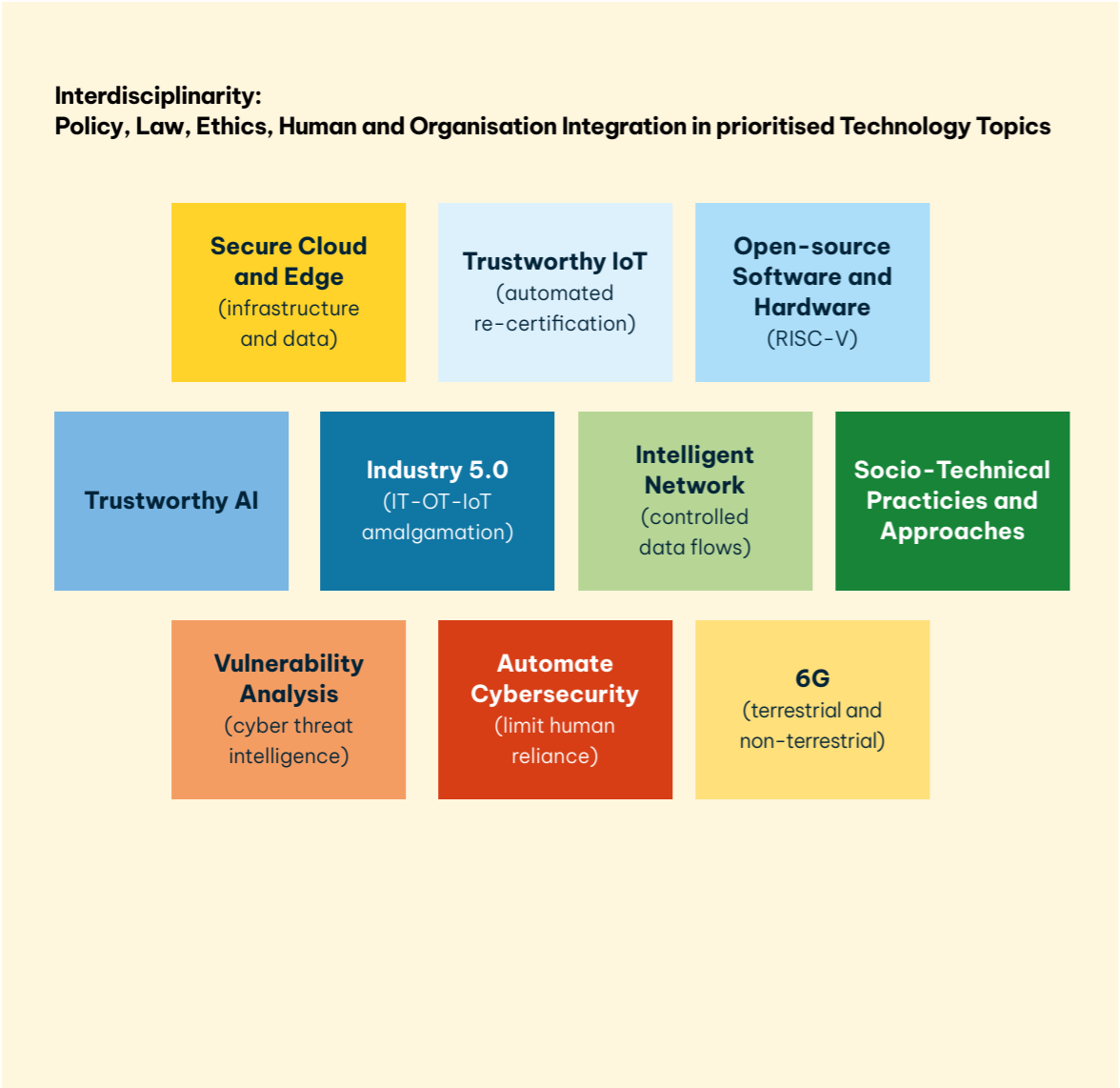
Cybercampus and Sweden's vocational colleges can collaborate in several areas. Since the role of the vocational colleges is to create and run agile education in close collaboration with employers, collaboration with Cybercampus helps to ensure that the education is relevant, and that Sweden gains the competence required to meet the cyber challenges of the future at all levels. Cybercampus will also coordinate and make visible all educational options nationally, a huge showcase for all providers of higher vocational education and for current educational offerings.

What are your expectations of Cybercampus Sweden?

My hope and expectations are that Cybercampus, together with us education providers, will succeed in helping to close the large skills gap that exists in the field of cybersecurity and that the availability of well-educated staff will quickly increase. The vocational colleges intend to work closely together with Cybercampus so that we can jointly ensure the right skills at the right time across the country.

Research

Our research activities are still in the early stages. Through meetings with academic partners, we have produced a first version of our research plan with prioritised key topics, following several workshops and extensive feedback. The Cybercampus graduate school is taking shape with principles of co-supervision, exchange, and joint mobility.



“The risk of data poisoning techniques targeting AI-driven tools –and, by extension, people– will increase.”

Asreen Rostami is a senior Human-Computer Interaction (HCI) researcher at RISE Research Institutes of Sweden and an affiliated researcher at Stockholm University. She leads the Human-Centred Cybersecurity research focus at RISE.

Which trends do you see as relevant in cybersecurity in the next 5-10 years?

As AI takes more presence, the risk of data poisoning techniques targeting AI-driven tools –and, by extension, people– will increase. Detecting such attacks will become increasingly difficult, raising the threat of more complex supply chain vulnerabilities.

What are your expectations on Cybercampus going forward?

To expand the scope beyond technical research and development and create more opportunities for the inclusion of other societal actors to exchange knowledge and learn from one another.



Joakim Kävrestad is a lecturer in computer science and has taught and researched cybersecurity for over 10 years. His main focus is human aspects of cybersecurity.

What do you consider important in cybersecurity that is easily forgotten?

I think we often forget that the digital world exists for people and companies and not the other way around. In the security world, this means that we must adapt security to users instead of, as is currently the case, trying to do the opposite.

What are your expectations for Cybercampus?

That Cybercampus will be able to unite Swedish education, research, and innovation with the result that we can be more efficient by collaborating in one venue instead of multiple.

“I think we often forget that the digital world exists for people and companies and not the other way around.”

The Research Plan was presented at the SWITS conference at Lund University in May and has been further developed with input from several universities. It is clear that our research must be interdisciplinary – integrating law, ethics, psychology, and sociology – so that technical innovations can be implemented in practice with sound theoretical understanding and ethical responsibility. Once our partnership agreements are in place, we will enter the practical phase of research.

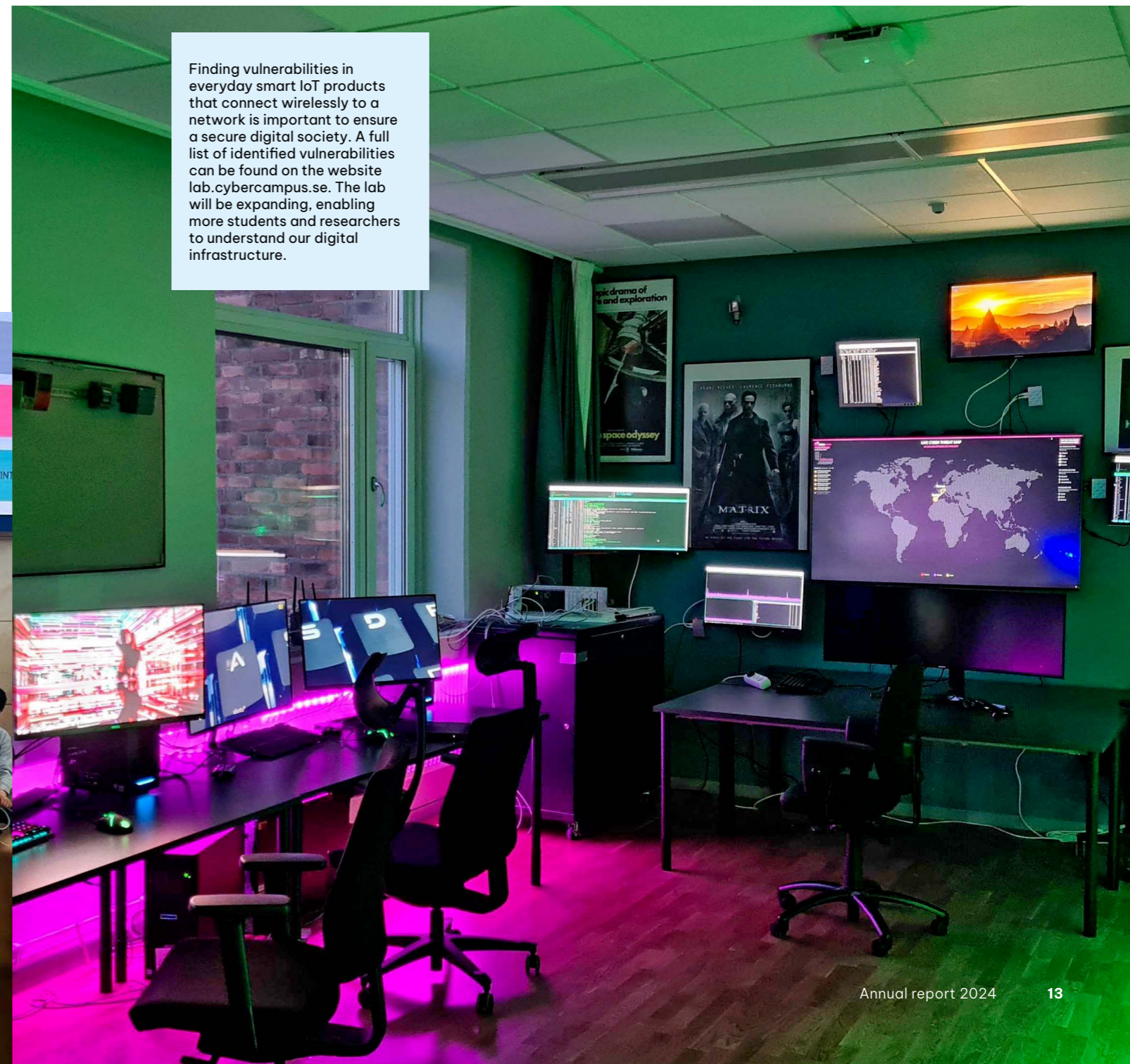
”It is clear that our research must be interdisciplinary – integrating law, ethics, psychology, and sociology – so that technical innovations can be implemented in practice with sound theoretical understanding and ethical responsibility.”

At the inauguration, we also presented the vision for our graduate school, based on a hybrid model where PhD students work either at Cybercampus or at their home institutions. We are currently designing principles for co-financing, co-supervision, and exchanges to strengthen collaboration between doctoral candidates and supervisors.

The Swedish IT Security Network for PhD students (SWITS) – a network for PhD students and supervisors coordinated by Karlstad University since 2001 – has been an important partner and starting point. At SWITS 2024 in Lund, its 24th edition, we were one of the hosts with over 95 participants from 15 universities. The next SWITS seminar will be held at Cybercampus in June 2025.

Our hacking laboratory at Cybercampus conducts world-class penetration testing and research. In the lab, we explore large language models (LLM), search for vulnerabilities in connected vehicles, and perform digital forensics, to name a few activities. The laboratory also serves as a demonstration venue for presenting research outcomes in practice. An EU grant application on LLM-assisted IoT vulnerability research has been

submitted. With generative AI as a central part of our operations – aligned with the AI Commission’s roadmap for Sweden – dedicated cloud resources are required for our studies. We are recruiting PhD candidates and researchers to meet future needs. Cybercampus has also recruited experts in coordinating future cybersecurity proposals and projects within Sweden, EU and NATO.



PhD Education and Graduate School

Cybercampus will establish a National Cybercampus Graduate School for the education and training of future cybersecurity experts. This new graduate school will contribute to the vision of carrying out cutting-edge cybersecurity research education beyond what is possible for an individual university.

Cooperation between cybersecurity experts and researchers across technical domains and disciplines will contribute to this end. Therefore, collaboration between cybersecurity researchers across Swedish universities and organisations is essential and envisioned for providing a high-quality cybersecurity PhD education. The National Swedish Graduate School has the following goals and planned activities:

To achieve this vision, Cybercampus builds on the well-established Swedish IT-Security Network SWITS for PhD students and researchers, founded in 2001 and coordinated by Karlstad University (KAU) and collaboration with the Knowledge Foundation (KKS) funded graduate school Swedish Industrial Graduate School on Cybersecurity (SIGS-CyberSec).

Excellence in cooperation through

- Co-funded PhD projects, co-supervised by Cybercampus partners
- Cooperation on prioritised research themes
- Hybrid setup and joint working and meeting space at Cybercampus premises
- Primary placement at Cybercampus or home institution
- Mobility grants and supported secondments at academic or industry partners
- Joint study trips and social activities

Cross-domain and interdisciplinary education through

- Joint broadening and deepening cybersecurity PhD student courses, open to eligible students
- Regular, open research seminars and annual SWITS seminar

Internationalisation through

- International cooperation, visits, and exchange programs with international partner excellence centres

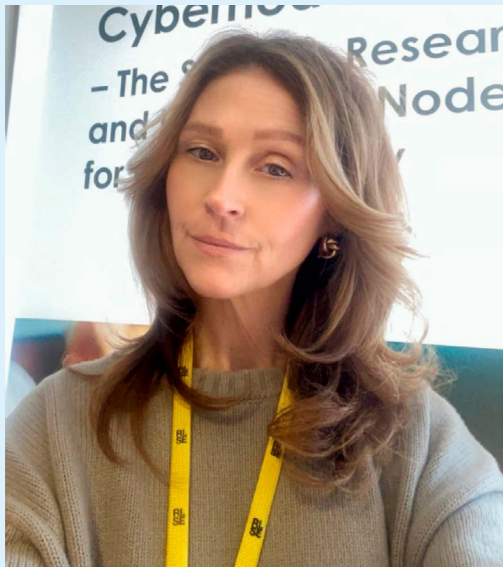
Innovation

Innovation is one of Cybercampus’ core pillars. We create the conditions to drive innovation both within Sweden’s cybersecurity ecosystem and in collaboration with international initiatives.

By bringing together players from the public and private sectors, we pave the way for new partnerships through hackathons, innovation challenges, and networking events. These activities nurture new companies, spin-offs, and other innovative ventures and outcomes in the field of cybersecurity. In December, we held our first partnership development event, with about 50

participants focusing on secure cloud solutions and AI as tools for cybersecurity. The insights from these events are used to refine our offerings in research, education, and innovation. Cybercampus will continue to catalyse innovation by connecting researchers, students, and startups, and by providing mentorship and networking opportunities for early-stage investors.





Petra Fröderberg is Deputy Coordinator at Cybernode, with many years of experience in marketing and communication – two areas that are vital to the cybersecurity domain today.

How do you view the collaboration between Cybernode and Cybercampus?

To the Cybernode, the collaborative effort with Cybercampus is of high importance. We have many common interests and target groups, but we also have separate goals and methods. To collaborate, support and help each other reach out is invaluable. Our ambition is to keep collaborating on as many areas as possible.

What are your expectations on Cybercampus?

Since Sweden has many challenges in cybersecurity, and the competence gap is large and growing, we hope that Cybercampus can provide a large increase of active professionals and general competence of cybersecurity in society, so that we can increase our resilience against any threat targeted against us. I also expect inspiring and instructive events and seminars, both in person and online, from Cybercampus. Our hope is that Cybercampus will be well enough funded to create and stimulate innovative education and solutions.



Anne-Marie Eklund Löwinder is one of Sweden's leading experts in information and IT security. 2010 – 2023 Anne-Marie served as Trusted Community Representative for ICANN, in the role of Crypto Officer, where she participated in DNSSEC key generation for the internet root zone. Anne-Marie is the only Swedish inductee into the Internet Hall of Fame. She is the founder and CEO of Amelsec.

“I expect Cybercampus to create a platform for excellence in cybersecurity.”

What can everyone do to improve their own cybersecurity?

Take the issue seriously, learn more, and view cybersecurity as an investment, not as a cost. Implement the measures that should have been addressed long ago and engage in systematic security work.

What do you expect from Cybercampus?

I expect Cybercampus to create a platform for excellence in cybersecurity, where research, innovation, and collaboration among experts from different sectors lead to concrete solutions that strengthen both mine and Sweden's digital security.

Partnership Offer

In the first half of 2025, we will launch our partnership offering. It is structured around Cybercampus' three pillars – research, education, and innovation – and is designed to enhance Sweden's resilience and competitiveness by meeting the nation's skills needs.

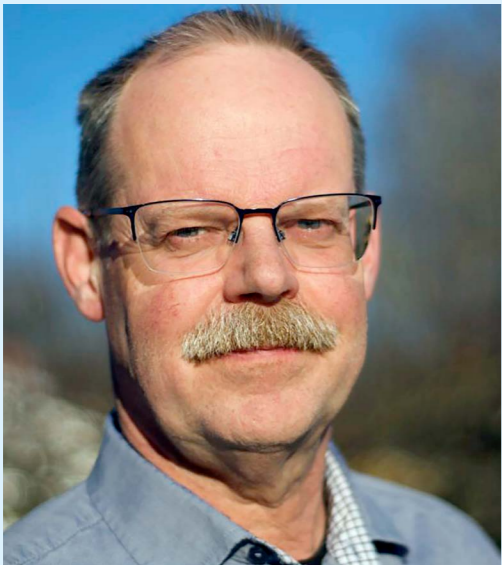
- **Private Sector:** Provides valuable insights on innovation opportunities, challenges, and how to strengthen the ecosystem.
- **Public Sector:** Contributes guidance on how we can offer up-to-date, well-founded, and impartial expertise to decision-makers in cybersecurity and defence.
- **Academia:** Addresses organizational needs through joint research and education, helping to bridge the gap between required competencies and existing curricula.

Within our research framework, our partners will help identify relevant projects supporting Sweden's secure digital transformation, utilising shared infrastructure and co-supervising doctoral students. In **education**, we invite our partners to help shape future competence offerings. In January 2025, the EU project CYCERONE will kick off, aiming to share, define, and develop new educational

“Cybercampus bridges academic research, protected innovation, and continuing education.”

content. For more details, please visit cybercampus.se, where our brochure *Agile Education Imagined* illustrates how we are broadening cybersecurity expertise in society.

Our **innovation** offerings include networking, events, access to students and researchers, and opportunities to pitch ideas and learn from each other. Cybercampus bridges academic research, protected innovation, and continuing education for both the private and public sectors. We serve as a national infrastructure that complements existing resources, with the goal of creating a comprehensive cybersecurity ecosystem.



Thomas Svensson has actively contributed to the planning and execution of cyber security exercises both on national and international level and is the deputy White Team leader for international live-fire cyber defence exercise Locked Shields. He is also a co-author of the handbook for planning, running and evaluating information technology and cyber security exercises published by the Swedish National Defence University.

Why is cybersecurity important right now?

Cybersecurity has always been important but given the increasing digitalisation of society, almost nothing can be done without having to connect to the internet, which in turn means that the attack surface has grown.

What do you expect from Cybercampus Sweden?

A natural hub for spreading information about cybersecurity. A forum where confidence can be built between people who can lead fruitful cooperation. All cooperation is built of confidence between people, and that applies to both public and private operations.

“All cooperation is built of confidence between people, and that applies to both public and private operations.”



Vincent Lenders is the founding Director of the Cyber-Defence Campus in Switzerland and the Head of the Cyber Security and Data Science Business Unit at Armasuisse Science and Technology.

In your opinion, which is currently the most important topic within cybersecurity to focus on, and why?

I believe that the most important topic within cybersecurity to focus on is Artificial Intelligence (AI). AI has transformative potential to revolutionise how we detect, analyse, and respond to cyber threats. With AI, we can identify malicious activity faster and more accurately than ever before. However, AI is a double-edged sword. While it enhances our defences, it also offers new tools to malicious actors who may use AI to create more sophisticated and evasive attacks. As defenders, we must stay one step ahead, understanding how AI can be both a solution and a potential threat in the hands of adversaries.

How can Sweden and Switzerland co-operate within the cybersecurity domain?

Switzerland and Sweden could co-operate within the cybersecurity domain through their respective cybercampus. Both countries have established a successful cybercampus model that focuses on research, innovation and cyber training. International collaboration in these three domains could boost the cybersecurity developments of both countries.

