CYBERCAMPUS SWEDEN

Annual Report 2025

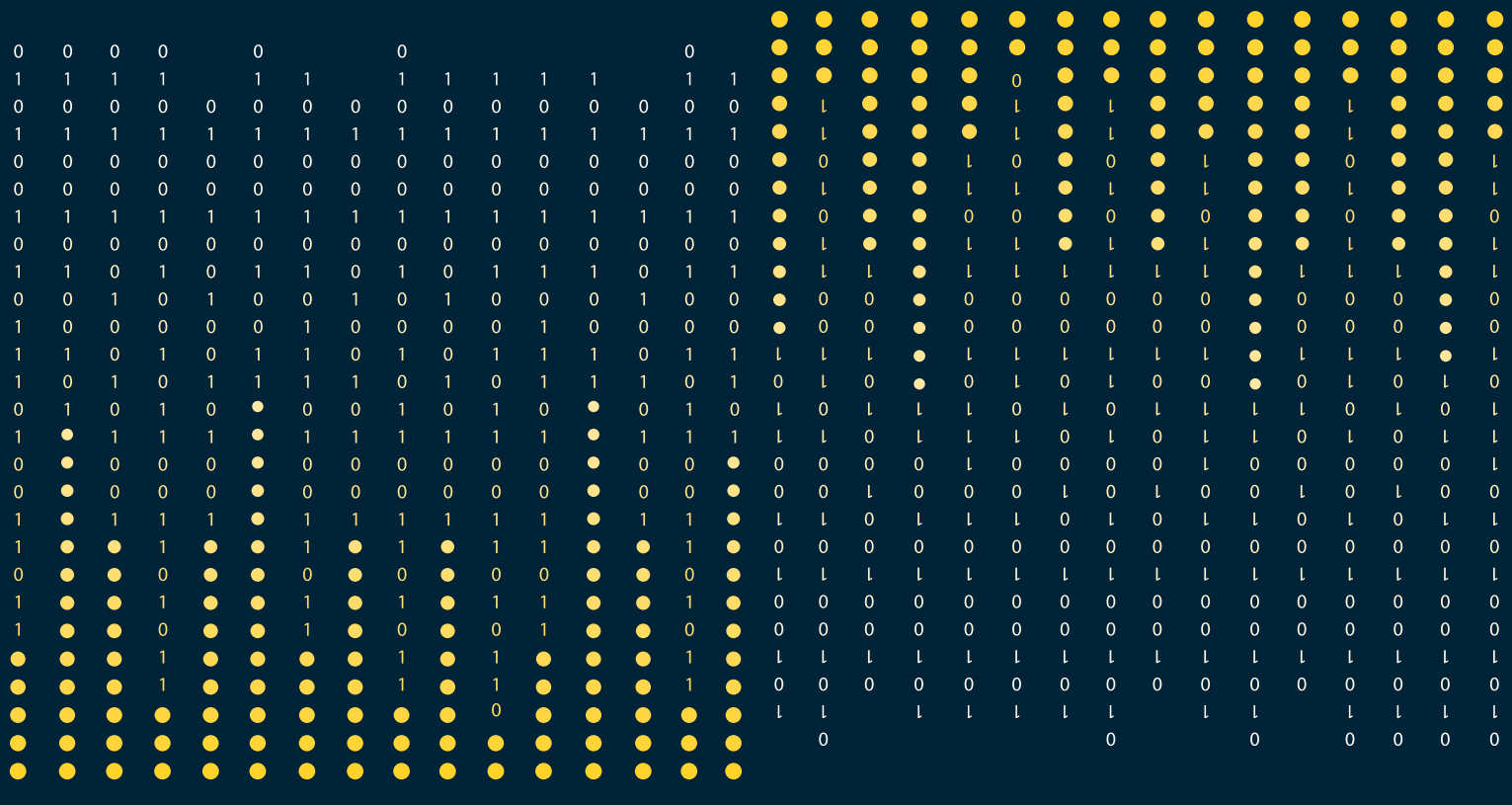


Photo: Gonzalo Irigoyen

Photo: Cybercampus

Photo: Cybercampus

Table of contents

Introduction

2025 was Cybercampus Sweden's second year of operations. Looking back, I can proudly state that we have taken major steps. Our operations have expanded, and we have developed our ways of working. But most importantly, the number of partners and members has grown. It is through joint efforts that opportunities arise, and we can achieve outcomes beyond what is possible for a single university, institute, government agency or company. This year, we also completed and published the first version of Cybercampus Sweden's strategy, which outlines the education, research, and innovation areas. In a world that is constantly changing, these are good conditions for contributing to a more cybersecure and resilient Sweden.

Cybercampus Sweden has initiated several important collaborations. We have been invited to present our mission and activities at conferences and seminars, and welcomed many visitors, including the Swedish royal couple during an Icelandic state visit, and the Deputy Chief Information Officer of NATO. We have reached out to different target groups, including young cyber soldiers who participated in events and cybersecurity competitions, teenage girls through the initiative Introduce a Girl to Engineering Day, and board leaders from the business and public sectors. We hosted a panel discussion during the Politicians' Week in Almedalen, talked on podcasts, and gave interviews. In June, we welcomed more than 100 PhD students and researchers from Swedish universities and research centres to Cybercampus, and in September we welcomed a delegation with staff members from the U.S. Senate. We have been engaged in interesting European collaborations, not least within the field of education. The span of target groups, stakeholders and contexts reflects the breadth of perspectives that need to be addressed in the strengthening of Sweden's cyber resilience and cybersecurity.

Furthermore, we have made important progress in both research and education. The high number of expressions of interest for the Cybercampus Graduate School is a clear sign of strong engagement. We also enabled five research projects and initiated CyberSweden, our annual research-centred conference. An educational offer – for public and private organisations – was presented on Cybercampus' website, and we were involved in developing a training programme tailored for diplomatic students.

Looking forward, I expect nothing less than equally eventful years. Some highlights ahead of us include kicking off the Cybercampus Startup Program to foster co-creation activities among inventors, researchers, entrepreneurs and stakeholders, and the first steps of Sweden's first national graduate school dedicated to interdisciplinary cybersecurity. We will have a constantly growing educational offering, including our own programs within cybersecurity.

I hope you share my excitement and look forward to exploring the 2025 annual report. Enjoy!

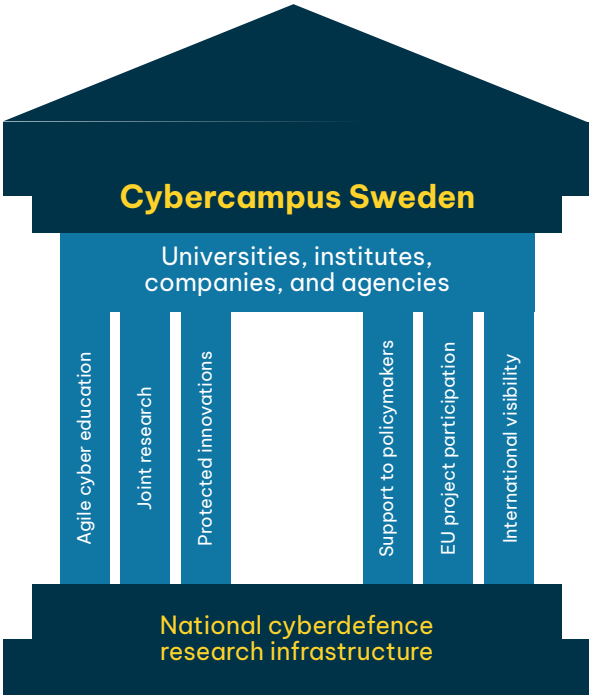
David Olgart
Director, Cybercampus Sverige
December 2025

Photo: Cybercampus

This is Cybercampus Sweden

Cybercampus Sweden is a national collaboration among universities, research institutes, government agencies, and industry.

Cybercampus Sweden is a strong triple helix collaboration that unites expertise across Sweden in an interdisciplinary effort to address gaps no single actor can fill – enhancing cybersecurity, strengthening defence, and reinforcing competitiveness.



Partnership

Cybercampus Sweden's role is to bridge academic research, innovation, and continuous learning. Our partnership offering is co-created with stakeholders across the cybersecurity ecosystem and aims to strengthen Sweden's resilience and competitiveness by meeting national skills needs and creating new opportunities for collaboration.

Partners are invited to take an active role in shaping future offerings. This includes contributing to new educational formats, engaging in roadmap development, influencing academic curricula, supporting startups, strengthening SME networks, and initiating co-creation activities. The final form of Cybercampus Sweden's initiatives will be developed in close collaboration with our partners.

Partners gain access to a broad range of opportunities, including access to our co-working and meeting spaces, workshops, round-table discussions, pitching sessions, interest groups, co-funding arrangements, and access to research expertise and results. Partners may also engage in joint projects, contribute to research publications, participate in contract training or online courses, and take part in Cybercampus Graduate School activities.

At the end of 2025, we had 22 partners and members. Many of them have already been involved in collaborative initiatives, such as research workshops, co-creation events, providing access to courses and shared materials on Cybercampus Sweden's website.

Most of the first cohort of partners come from academia and the public sector. This is important for addressing needs related to joint research and education, bridging the gap between required competencies and existing curricula, and gaining insights into the expertise we can offer to decision-makers in cybersecurity and cyber defence. This strong foundation between academia and the public sector supports the development of a triple helix model, fostering conditions for engaging partners from industry.

The ambition for 2026 is to engage in continuous dialogue with both affiliated and potential future partners, with a particular focus on private-sector actors. The industry's perspective is essential for identifying innovation opportunities, understanding challenges, and strengthening the national cybersecurity ecosystem. A diverse partnership network will strengthen collective competence and value—both for Cybercampus as a whole and for each partner. The partnership model will continue to be refined in dialogue with all partners.

Photo: Cybercampus

Senja Nordström is Cybercampus' partnership coordinator since 2025.

Olga Torstensson, lecturer at the School of Information Technology, Halmstad University

“In Ukraine, many universities offer courses in cybersecurity and AI, and the network is very strong. This benefits both Ukrainian and Swedish interests.”

In 2025, we expressed interest in becoming a Cybercampus partner. It is crucial to bring together different competences and perspectives to make Sweden more secure. Together, we can educate more people, carry out joint initiatives, pool expertise, and learn from each other. As a smaller institution, we also see how collaboration provides “muscles”.

Our university has strong expertise in cybersecurity and active research, including two Swedish Institute-funded projects on AI-generated cyber threats and AI-driven cybersecurity. We also have an AI-specialist professor and a doctoral student focused on cybersecurity.

We have launched a new course package in digital forensics called Cyber Security Analyst. The need for this competence is substantial, which is why we have made the course package highly hands-on.

We collaborate with universities in Ukraine and Poland and see strong potential for cooperation in the Baltic region. In Ukraine, many universities offer courses in cybersecurity and AI, and the network is very strong. This benefits both Ukrainian and Swedish interests. The Ukrainian people really continue to fight.

You have a degree programme called IT Forensics and Information Security. Tell us about it!
It is a broad and interdisciplinary bachelor’s programme. After graduating, students can work with the police or other authorities, or as IT security consultants. Former students work with ethical hacking, penetration testing, monitoring attacks in real time, or with legal and policy related aspects.

The master’s programme offers in-depth studies and is also interdisciplinary, with teachers from Law, Political Science, and other fields. It includes components related to social sustainability, definitions of cybercrime, and applications of data mining and machine learning results. There are excellent job opportunities across many sectors.

Karl Andersson, professor, dean of the Faculty of engineering, Luleå University of Technology.

One concrete achievement for us in 2025 was launching a new master's program in cybersecurity. We hope this initiative will strengthen the talent pipeline for Sweden and Europe. Interest has been high. Looking ahead, we plan to offer short introductory courses at the basic level, particularly aimed at professionals. These could be foundational or more specialised, but always accessible.

In addition, our ongoing work in cybersecurity continued to expand. We are leading a regional initiative, Cybersecurity Node North, which gained real momentum in 2025. The participants include twenty companies, two regions, two municipalities, and one government authority. Our work focuses on applied, needs-driven research carried out in close collaboration with companies, municipalities, authorities, and regional actors.

“Our work focuses on applied, needs-driven research carried out in close collaboration with companies, municipalities, authorities, and regional actors.”

How can partnerships within Cybercampus contribute to strengthened cybersecurity and cyber defence?
I strongly believe in collaborative projects. Working through shared platforms is essential, and being relevant to society is central to us - every research project we run includes external partners. For example, we are part of a project supporting the ambulance helicopter operations in Norrbotten, in which the Armed Forces are also involved: *“Future-proof bearer-agnostic overlay networks.”* We are also active in Campus Total Defence, where we see clear synergies.

We decided early on to join Cybercampus. The model and its collaborative approach are a natural fit for our way of working. We share the vision that academia, industry, and the public sector must work closely together to address societal challenges. No single actor can solve these problems alone.

It will be exciting to see how Cybercampus evolves. We are curious about new partners who may become strong candidates for closer collaboration and would be happy to offer more commissioned training if specific needs arise.

Highlights 2025

Photo: Cybercampus

Visit from a delegation with representatives from the Danish Security Tech Space, the Alexandra Institute, Aarhus University, and its innovation office Kitchen. In search of a model to strengthen Denmark's cybersecurity ecosystem, Cybercampus national mission and operations were presented and discussed.

January – Visit from a Danish delegation

January – Start of the EU project CYCERONE

March – Introduce a Girl to Engineering Day

April – FRO event (CTF) at Cybercampus

April – Training in cybersecurity for the Ministry of Foreign Affairs' Diplomatic Programme

April – National Strategy of Cybersecurity presented

May – Icelandic state visit

June – 25th Seminar of the Swedish IT Security Network (SWITS)

June – Panel discussion during the Almedalen Week

Photo: Sanna Johannesson, Blackbox Videoproduktion AB

In May, The Icelandic presidential couple, the Swedish royal couple, Icelandic Foreign Minister Þorgerður Katrín Gunnarsdóttir and Minister of Health Alma Möller, and Swedish Minister of Civil Defence Carl-Oskar Bohlin were part of the delegation that visited Cybercampus during the Icelandic state visit. The program included a panel discussion on digital resilience with participants from business, academia, government and civil society, as well as an exhibition with demonstrations of examples of results from work carried out in the Hacking Lab, academic work by Icelandic academics on site in Sweden, and local startups in the cybersecurity field.

Photo: Carina Jonsson, NCSC

The launch of the national strategy for cybersecurity at the Swedish Defence University in April 2025. The picture shows Carl-Oskar Bohlin, Minister for Civil Defence, Charlotte Lindgren, acting director of the Swedish National Cyber Security Centre (NCSC-SE), David Olgart, director of Cybercampus Sweden, and Malena Britz, pro-vice-chancellor at the Swedish Defence University. The strategy (2025–2029) describes the Swedish government's direction for work on issues of importance to Sweden's cybersecurity.

Photo: Cybercampus

In November, The conference Security Divas aims at strengthening and inspiring women to work with security. Both speakers and target groups are broad, including different aspects of societal, information and digital security, like police, researchers, those already working with tech but maybe not cybersecurity, and others. Cybercampus co-arranged this year's conference, held in Karlstad. The picture shows Ingrid Ivars, innovation manager at Compare, Annika Andreasson, researcher at the Stockholm School of Economics, Katarina Boustedt, research coordinator at Cybercampus, and Simone Fischer-Hübner, director of post-graduate education at Cybercampus.

September – Cyber Sweden

September – Visit from US delegation

November – Security Divas

December – 22 official partners members!

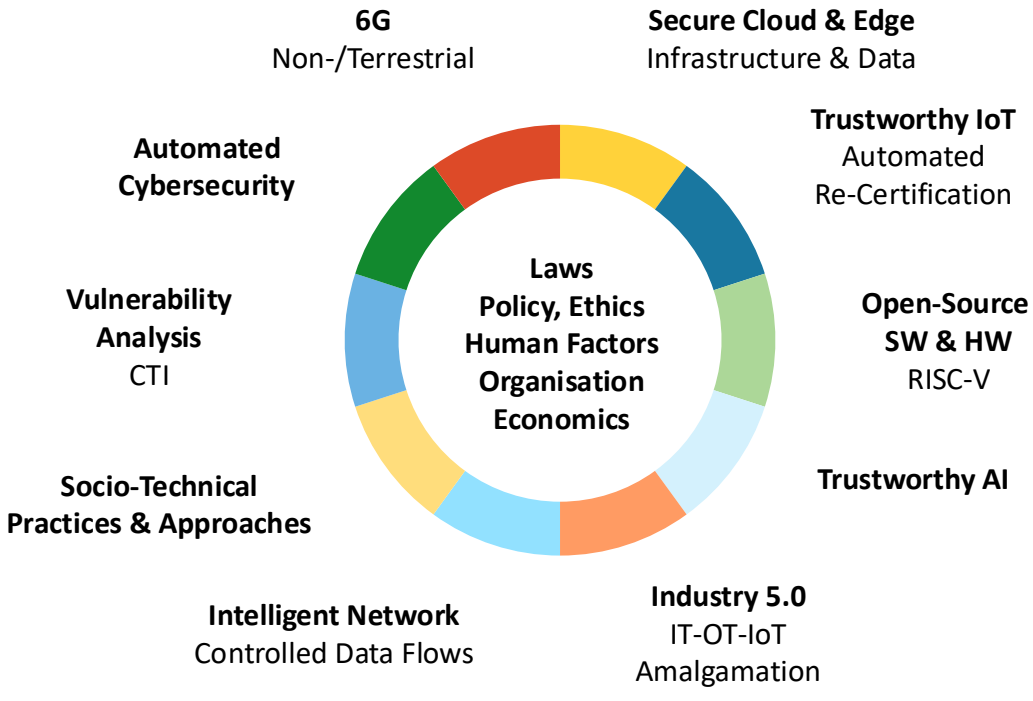
Research

Within the field of research, Cybercampus focuses on mission-oriented, interdisciplinary collaboration designed to deliver concrete, implementable solutions for Sweden's cybersecurity, digital sovereignty and defence posture.

Instead of duplicating existing academic projects, the aim is to complement national efforts by uniting experts across domains including human factors, policy, and law to address challenges that no single organisation can solve alone. Key research themes include secure cloud and edge technologies, trustworthy AI, secure open-source infrastructure, IoT assurance, Industry 5.0 cybersecurity, controlled national network flows, vulnerability analysis, and emerging domains such as 6G security.

The long-term goal is to position Sweden as a leader in cybersecurity research by building a shared national research infrastructure, establishing a cybersecurity graduate school, and enabling collaboration across universities, industry, and government agencies. The expected outcome is directly usable technologies, enhanced resilience in critical sectors, and strengthened sovereignty.

In March, we arranged Introduce a Girl to Engineering day (IGEday), with Kodsport, Women4Cyber, FRO, and KTH – where teenage girls and non-binaries learn more about a career as an engineer. The participants visited the Hacking Lab, tried ethical hacking, and listened to inspiring female leaders within engineering and cybersecurity. In June, we hosted the Swedish IT



CyberSweden at Chalmers University of Technology.

Security Seminar, SWITS, where we welcomed more than 100 PhD students and researchers from universities and research centers across Sweden, presenting Cybercampus and the Hacking Lab to them.

In September, we launched our flagship annual research conference, CyberSweden. The inaugural event was hosted by Chalmers University of Technology in Gothenburg. CyberSweden places research at the centre, creating an arena for advancing scientific excellence and fostering dialogue across academia, industry, and the public sector. This will be the platform where we present our own research in the coming years.

The conference had a strong focus on emerging research talent. Twenty-four PhD students from Swedish universities presented posters and one-minute poster pitches. The format was highly appreciated for its clarity and energy. *The Best Poster Award* was presented to Patrick Shirazi from the University of Skövde for his work on human factors in cyber threat intelligence adoption. The conference also emphasised the pathway from research to inno-vation, highlighting how scientific insights can evolve into startups, spin-offs, and real-world products. Speakers shared concrete journeys illustrating how academic work can

“One of the most engaging sessions focused on backdoors in communication apps, including a presentation from Signal on its role in safe-guarding privacy.”

scale into impactful companies—an ambition aligned with Cybercampus Sweden’s mission to ensure soci-etal and economic benefit from cybersecurity research.

One of the most engaging sessions focused on backdoors in communication apps, including a presentation from Signal on its role in safe-guarding privacy. It was followed by a panel discussion exploring the controversy around cryptographic backdoors, the balance between privacy and law enforcement, and the broader implications for democratic societies—under-scoring the need for informed, evidence-based public discussion.

The success of the first conference lays a strong foundation for the years to come, and we look forward to *CyberSweden* 2026.

CyberSweden 2025. Patrick Shirazi from the University of Skövde receives the Best Poster Award from professor Magnus Almgren.

The Cybercampus Graduate School

During 2025, major steps were taken in establishing the Cybercampus Graduate School, which will become the first national graduate school in cybersecurity. Fifteen Swedish universities and research institutes joined as Cybercampus partners and committed to jointly developing a shared academic environment for post-graduate cybersecurity education.

As part of the launch, partners were invited to submit expressions of interest to host a PhD project funded by Cybercampus Sweden, each requiring a supervisor at the host institution and a co-supervisor from another partner. This ensures true joint supervision and strengthens both academic excellence and cross-sector research capacity.

Simone Fischer-Hübner, professor of Computer Science at Karlstad University, and responsible for Cybercampus Graduate School, describes the initiative:

The overall objective of the Cybercampus Graduate School is to establish a cutting-edge PhD education and training in cybersecurity that goes beyond what a single university can offer. This is enabled through the unique collaboration model, in which the fifteen partners jointly build up and offer a new cross-domain and interdisciplinary postgraduate cybersecurity curriculum in Sweden. This cooperation will enhance cybersecurity collaboration between partner institutions and their PhD students, lead to increased cybersecurity competence and boost cybersecurity networks in Sweden. Ultimately, it will strengthen Sweden's cybersecurity and resilience.

The ambition is for the Cybercampus Graduate School to establish itself successfully in the long term and develop many cybersecurity talents who will contribute to cybersecurity research and innovation at Swedish organisations and for Swedish society.

The graduate school is jointly developed by the participating partners and counts on their active engagement. They have all committed to contribute with holding PhD courses and seminars. An operational team is developing a course structure with mandatory broadening courses in different cybersecurity domains during the first two years, creating common foundations before students take elective deepening courses. Moreover, we will offer courses in transferable skills and professional training, including entrepreneurship and cybersecurity innovation.

A topic of particular interest is the intersection of cybersecurity and AI, often called Trustworthy and Robust AI, but also how AI can be used to enhance cybersecurity and privacy. Many of the planned PhD projects will address or touch on these topics.

Photo: Cybercampus

To establish early momentum, Cybercampus co-funded five research projects in 2025

LLM-Powered Vulnerability Discovery and Analysis in Open-Source Software

Is it possible to discover vulnerabilities in open-source software more quickly? Syafiq Al Atiiq and Christian Gehrmann demonstrate AI capabilities in cybersecurity by discovering real vulnerabilities in critical open-source infrastructure. Scanning major open-source projects to identify and responsibly disclose security vulnerabilities.

This project was conducted by Syafiq Al Atiiq and Christian Gehrmann at Vypr AI AB, a startup company from Lund University.

Machine Learning over Encrypted Data

Using homomorphic encryption (FHE), it is possible to perform computations directly on encrypted data. This enables processing and analysis without ever exposing the underlying information. Potentially, this technology can allow researchers to analyse confidential data from non-trusting parties, such as hospitals, without ever sacrificing data ownership. The aim of this project is to improve the scalability and efficiency of multi-party FHE and explore machine learning on encrypted data. This research is conducted by PhD student Anton Israelsson.

When Anonymized Data isn't Private: How Language Models Reveal Emerging Weak Points

How can individual privacy be safeguarded in an era dominated by artificial intelligence? How can LLMs undermine traditional anonymisation techniques? This project aimed to ' raise awareness about the fragility of conventional anonymization methods and to provide concrete, reproducible evidence showing how even non-expert users, equipped with LLMs, can de-anonymize seemingly harmless data.

This project was conducted by Alejandro Russo at Dpella, a startup company from Chalmers University of Technology.

Readiness to teach cyberhygiene – an exploration of the perceptions of primary school teachers (ReaTCH)

As more educational initiatives at different levels of society have been developed, it becomes crucial that we have methods to evaluate their effects. The project aims to initiate the development of methods for evaluation of learning materials for teaching cyberhygiene in primary school by conducting interviews with teachers and other educators.

Cybercampus co-funds this project at Jönköping School of Engineering and Kodcentrum, and it is led by Joakim Kävrestad and Erik Bergström.

Sweden's Cybersecurity at Crossroads

This research provides a long-term, interdisciplinary platform to support strategic policy learning, measure the implementation of the national cybersecurity strategy, and aims to generate actionable insights by combining historical institutionalism, comparative policy analysis, case studies, stakeholder interviews, an international panel of experts, and scenario-based activities/exercises, to shape Sweden's cyber resilience towards 2040.

The project is led by Henrik Glimstedt, includes postdoc Annika Andreasson (PhD from KTH CDIS), and is co-funded by the Stockholm School of Economics.

Education

As digitalisation accelerates and the security environment becomes more complex, the demand for expertise grows faster than the supply. This affects Sweden's resilience, defence capabilities, and industrial competitiveness.

The shortage of cybersecurity professionals remains substantial, both in Sweden and globally. Women also remain underrepresented in the field.

Cybercampus aims to address the needs of professionals across sectors, specialised cybersecurity experts, decision-makers, and the general public. The long-term vision is to create a unified national curriculum that can be scaled up to large groups of participants. Professionals should be able to upskill efficiently, and societal actors should be able to strengthen their resilience. Initial priorities include leadership development and broad workforce awareness, followed by specialised professional training and outreach activities.

We have established our first education strategy, which emphasises national collaboration to strengthen Sweden's overall cybersecurity competence. Its goal is to provide high-quality, research-anchored education that complements existing university programmes and supports continuous learning. The strategy prioritises advanced learning outcomes such as analysis, synthesis, and evaluation. Education is delivered through flexible formats, including commissioned education for organisations, freestanding university courses, and informal learning activities. Cybercampus also acts as a national hub for shared educational resources, student exchanges, infrastructure, and credit transfer.

During 2025, we participated in several national and international learning initiatives. One of these was the EU project CYCERONE, which aims to develop and share cybersecurity training for professionals in SMEs and the public sector. The focus is on identifying cybersecurity skills needs, developing targeted educational offers, and distributing training through a shared European platform. Another one is *Cyber Bridge Forum*, a Nordic-Baltic Network with support by the Nordic Council of Ministers, where we among other things work for stronger collaboration with ENISA. We were also engaged in the Vinnova-funded Expert Learning Lab, together with Blekinge Institute of Technology, targeting large enterprises. Both initiatives continue into 2026.

We have provided partners with access to courses and shared materials. The educational offer – structured into the three levels introductory, intermediate, and advanced – is presented on Cybercampus' website. Furthermore, the development of our own educational programmes has progressed significantly. A notable example is CYVAC, a new cyber-vaccination training to be launched in 2026.

"We have established our first education strategy, which emphasises national collaboration to strengthen Sweden's overall cybersecurity competence."

The introductory programme Cyberlyftet, which was launched in partnership with RISE in 2024, continued to generate strong interest and has engaged 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.

Cybersecurity training for future diplomats

Photo: Cybercampus

The diplomat trainees at Cybercampus during the two-day training programme. In the front, Chung-wai Lee from Cisco and Mette Svensson from Cybercampus

In 2025, Cybercampus and Cisco developed a training programme tailored to the Ministry of Foreign Affairs' Diplomatic Program. Diplomat trainees are experts in foreign policy and international relations, and the training complements their expertise with cybersecurity perspectives. In line with our education strategy, we aim to work interdisciplinarily to create a new common area of knowledge.

The two-day training was designed as a seminar-based bootcamp. It introduced key aspects of cybersecurity, AI, and emerging technologies to the participants. The training combined lectures from experts covering a wide range of knowledge in the cybersecurity field, with group discussions and practical elements. The participants also went through the interactive CYVAC training and visited the Hacking Lab.

Thom Thavenius, deputy head of security at KTH, lectured on the geopolitical and security policy situation in the world. He considered this perspective essential for the participants' future roles.

"If you are going to work in a vulnerable position – which diplomats really do – it is important to understand that there are strong interests in learning about Swedish conditions, interests that do not apply to many other countries. Sweden is uniquely interesting to foreign powers! As a diplomat, you carry knowledge that may attract malicious actors. In your job as a stationed officer, you will become a real expert on the local environment, but it may be harder to see the broader geopolitical picture in your daily work. Therefore, it is important to bring this context with you when you go to other regions. With this knowledge, you can better interpret what you observe. Many of the movements we see in security policy manifest differently across regions. It becomes important to decode what you see."

Innovation

Cybercampus works to create the conditions needed to drive innovation in both the public sector and industry, in Sweden and in collaboration with international initiatives. Our role is to enable, support, and accelerate activities that strengthen Sweden's cybersecurity capacity.

We aim to strengthen and support the development of a strong national cybersecurity ecosystem, by offering a shared environment for academia, government agencies, industry, entrepreneurs, and spin-offs – combined with coordinated educational programmes and interdisciplinary research.

Our focus is on the connection between research outputs and practical application. We aim to expand the cybersecurity ecosystem by linking incubators, innovation offices, accelerators, and investors, ensuring that promising teams receive guidance, mentoring, funding opportunities, and technical expertise.

Cybercampus' innovation strategy focuses on enabling partner-driven and research-based innovation and on supporting the development of impactful cybersecurity solutions and startup growth – to complement already existing initiatives.

During 2025, we developed a startup programme together with experts in our network. The programme complements existing innovation environments by offering co-creation opportunities and by providing startups with knowledge that focuses on the unique challenges of cybersecurity markets. We look forward to welcoming the first co-creation cohort.

Looking ahead, we aim to create coordinated arenas for innovation, such as co-creation events, and challenge-driven activities. We also aim to develop innovation matchmaking tools – for example, a challenge portal – while strengthening our network of partners from academia, industry, and the public sector.

"We aim to expand the cybersecurity ecosystem by linking incubators, innovation offices, accelerators, and investors, ensuring that promising teams receive guidance, mentoring, funding opportunities, and technical expertise."

Photo: Carina Schultz

Alejandro Russo from the startup company Dpella and Göran Olofsson, head of innovation at Cybercampus.

Ingrid Ivars, innovation manager at the Compare Foundation

The Compare Foundation works daily with municipalities, companies, and innovators who want to strengthen their cyber and societal security but often lack guidance and the capacity to get started. We see Cybercampus as an important national hub that connects what is happening locally and regionally with national initiatives. We can now help guide these actors to the right expertise, training, and resources within Cybercampus. In this way, the membership helps make cybersecurity more practical, coordinated, and accessible – particularly for smaller municipalities and companies.

What questions and events were particularly important in 2025?
There was a strong focus on digital resilience, preparedness, and societal security. It has become increasingly clear how critical cybersecurity in both the private sector and municipalities is to Sweden's overall resilience. Considering that 240 of Sweden's 290 municipalities have fewer than 20,000 inhabitants – and that 97 percent of Swedish companies are small, with fewer than 10 employees – the need for practical support, capacity building, and coordination has been central. Initiatives such as Cyber Range Light, cybersecurity programs for SMEs, Security Divas, and innovation through Cyber X have all played important roles.

How has your experience as a member been so far?
Together with Karlstad University, Compare has participated in workshops and activities organised by Cybercampus. Among other things, we co-organised Security Divas, a conference that highlights skilled women in cyber and information security. Looking ahead, we hope to develop this together.

We find the dialogue open and constructive, and we see Cybercampus as a unifying platform where regional perspectives are taken into account. We have gained valuable insights into national priorities while also contributing with experiences from regional and cross-border collaboration with Norway. The membership has made it easier to connect our initiatives to a broader national context.

"Among other things, we co-organised Security Divas, a conference that highlights skilled women in cyber and information security. Looking ahead, we hope to develop this together."

Alejandro Russo, researcher, Dpella

“We aim to raise awareness about the evolving risks posed by modern AI-systems and the need for stronger privacy protection.”

You and your team have explored how simple privacy attacks can be amplified by modern AI-tools. Tell us about the results!

A key outcome of the project is a set of concrete prompts that can be used with ChatGPT and other large language models to simulate privacy attacks. These prompts allow anyone to test how easily anonymised or aggregated data can be reconstructed. AI is not only a powerful tool for data analysis but can also significantly lower the barrier for performing de-anonymisation attacks.

We chose a “try it yourself” approach; anyone can visit our project repository, read a blog post explaining the methodology, and experiment with guided examples of the attacks. We released a curated set of prompts that demonstrate how de-anonymisation can be performed in practice.

The examples are designed to be educational and reproducible, allowing readers to understand risks and take inspiration when evaluating the privacy resilience of their own datasets. We aim to raise awareness about the evolving risks posed by modern AI-systems and the need for stronger privacy protection.

What do you see as the most critical factors for ensuring that cybersecurity research leads to practical, real-world solutions?

A key condition for translating research results into practical cybersecurity improvements is sustaining strong foundational research that remains closely connected to real-world applications. Research should both advance theoretical understanding, and generate concrete methods, test cases, and actionable solutions that companies and public institutions can use to strengthen cybersecurity.

Equally important is shortening the time from laboratory results to real-world use. Startups and spin-offs can often play an important role in turning cutting-edge research into operational solutions.

Sustained public project funding is also essential, particularly funding schemes that support collaboration between academia, startups, SMEs, and public institutions. However, high co-financing requirements for startups may unintentionally exclude smaller companies that drive much of the innovation in cybersecurity.

Sofia Wallgren, master's student in Computer Science and event staff at Cybercampus

I've been involved in several activities hosted by Cybercampus and also served as an instructor at FRO's (the Voluntary Radio Organisation) youth events. I have given lectures at Introduce a Girl to Engineering Day, where the goal is to inspire participants by giving them an idea of what you can do within cybersecurity. It's important to encourage young girls to choose – and stay within – the field of technology!

In what ways are activities like these important?
As a teenager, I participated in initiatives like IGEday and FRO courses around Sweden, which I found both fun and inspiring. It's important to encourage young people—especially girls and nonbinary youth—to explore cybersecurity, where more people are urgently needed.

Representation matters and seeing others you can identify with makes a real difference. Bringing more girls and nonbinary individuals into cybersecurity will also help more of them stay in the field.

I think the marketing of activities for young people could be improved. Because they do exist – there are many courses, competitions, and events! But perhaps the organisers aren't reaching everyone who might be interested?

How can Cybercampus contribute to strengthened cybersecurity and cyber defence?
I think the networking opportunities and the mix of perspectives are the most important aspects. Cybercampus is a valuable meeting place for people from different sectors, organisations, and backgrounds, as well as from different age groups.

When people meet at events and are encouraged to talk to one another, they can get inspired to discover their own niche within cybersecurity—whether that's hacking, policy making, teaching, or something else. Cyber defence consists of so many different parts!

"When people meet at events and are encouraged to talk to one another, they can get inspired to discover their own niche within cybersecurity – whether that's hacking, policy making, teaching, or something else. "

CYBERCAMPUS
SWEDEN

www.cybercampus.se

With financial support from Vinnova
and the Swedish Government.

VINNOVA