Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

armasuisse
Science and Technology

CYD
CYBER DEFENCE CAMPUS

Cyber-Defence Campus

2024 Annual Report

Editorial

Dear readers,

The year 2024 was again marked by a significant surge in cyber incidents. Around 63'000 cyber events were voluntarily reported in Switzerland to the National Cybersecurity Centre (NCSC), highlighting the pressing need to address the growing threats in the digital domain. These cyber threats reinforce the vital role of the Cyber Defence Campus (CYD Campus) in strengthening the nation's cybersecurity and shaping its ongoing digital transformation. Challenged with staying ahead of technological developments and threats, the CYD Campus remains committed to enhancing Switzerland's cyber resilience in an increasingly complex and digital world.

To address the growing challenge of cyber defence, the CYD Campus was tasked this year with leading the Cyber Training @ Cyber-Defence Campus pilot project, a strategic initiative under the umbrella of the Federal Council's National Cyber Strategy (NCS). Developed in collaboration with the Federal Office for Cyber Security (FOCS), this program brings together key stakeholders from across the nation, including cantonal and federal authorities, police forces, and critical infrastructure operators. The training program is designed to foster a unified approach to cybersecurity, leveraging partnerships with industry experts and the Swiss Armed Forces cyber training range. Through this initiative, participants receive tailored training to enhance their technical and operational readiness, ensuring a coordinated response to evolving threats.

Innovation is a cornerstone of the CYD Campus' mission to secure Switzerland's cyberspace. In 2024, the CYD Campus hosted its first Innovation Day, which attracted more than 100 participants from various sectors. The event showcased the latest advances in cyber defence technologies, underscoring the CYD Campus' commitment to fostering innovation and collaboration. This spirit of innovation extends to its engagement with Switzerland's vibrant start-up ecosystem and academic institutions. The 2024 Cyber Start-up Challenge, which focused on the security of AI, provided a platform for emerging companies to present groundbreaking solutions. Patronus AI triumphed in this competition, demonstrating its potential to address critical cybersecurity challenges.

The CYD Campus also actively nurtures young talent by offering opportunities for students to gain practical experience in cybersecurity. In 2024, over 65 students participated in internships and research projects at the CYD Campus, working on real-world problems and contributing to urgently needed advancements in the field. These initiatives not only strengthen the CYD Campus workforce, but also lead to a larger Swiss cyber community of alumnis that have created this year the CYD Alumni Association to stay in contact after their active engagement at the CYD Campus.

Marking its fifth anniversary in 2024, the CYD Campus reflected on a period of significant growth and achievements. Founded in January 2019 by armasuisse Science and Technology, the CYD Campus has evolved into a hub of expertise and collaboration. Over the years, it has forged impactful partnerships with federal, cantonal, and industry stakeholders, delivering valuable research outcomes and strengthening the nation's cyber resilience. Its anniversary has been celebrated through a range of events, including the CYD Campus conference held on October 30 in Bern and the 5 year celebration on December 4 in Zurich. The CYD Campus conference welcomed more than 300 participants from academia, government, industry, and the military to discuss "Emerging and Disruptive Cyber Technologies". Topics such as quantum computing, next-generation networks, and artificial intelligence (AI) were at the forefront of discussions, fostering an exchange of ideas critical to addressing future challenges.

A highlight this year were also our hackathons in the autumn, focusing on contemporary issues like satellite detection, security tracking, and data science. Participants gained hands-on experience in tackling pressing issues, enriching their skills and fostering collaboration across organisations and sectors.

Research continues to be a central pillar of the CYD Campus' mission. In 2024, its research programs, conducted in partnership with academia and industry, identified emerging cyber threats and developed innovative solutions to mitigate them. These efforts resulted in the publication of over 90 scientific papers, covering disruptive technology areas such as artificial intelligence, generative large language models (LLMs), 5G security, quantum computing, space technology cybersecurity, and future network security. The CYD Campus also played a crucial role in identifying and reporting numerous vulnerabilities in software and devices, further securing Switzerland's digital infrastructure.

I'm excited to provide you with a closer look at our projects and daily efforts, and I hope you enjoy uncovering more about the Cyber-Defence Campus.

Thun, December 2024

Dr. Vincent Lenders
Head of Cyber-Defence Campus

Table of Contents

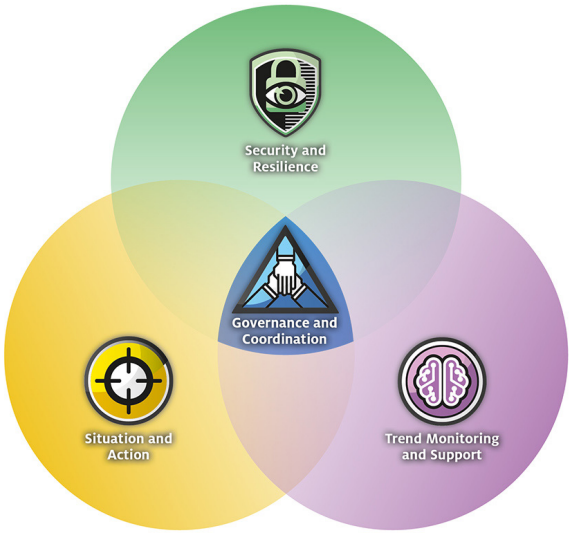
1. About the Cyber-Defence Campus

Strategy and Mission

The Swiss government has recognised cyber security as a critical national security issue due to the expanding digital landscape and the growing risk of cyber attacks across all sectors. In response, the Federal Department of Defence, Civil Protection and Sport (DDPS) has prioritised cyber defence as a strategic and operational focus and has allocated more resources to address this challenge. In 2016, the department introduced the first Action Plan for Cyber Defence (APCD) to strengthen its efforts. Given the escalating cyber threat environment over the past five years, the DDPS has developed a follow-up Cyber Strategy for the period 2021-2024, building on the foundation of the APCD. Both initiatives are closely aligned with Switzerland's overarching National Cyber Strategy (NCS).

The Cyber-Defence Campus (CYD Campus) has been an integral part of the efforts of the DDPS since its establishment in 2019 and operates under the auspices of the Federal Office for Defence Procurement (armasuisse Science and Technology). As a platform for anticipation and knowledge, the CYD Campus enables the DDPS to identify and evaluate emerging technological, scientific and societal cyber trends. To foster close collaboration with universities, industry partners and the DDPS, the CYD Campus operates in three strategic locations: its main hub in Thun (armasuisse Science and Technology), the Innovation Park at the EPFL in Lausanne and a site near the ETH in Zurich. This multi-location setup allows the CYD Campus to efficiently develop expertise across Switzerland and provide tailored cyber knowledge to meet the needs of the Swiss Confederation.

The CYD Campus acts as a bridge between industry, public administration and academia. As part of the "DDPS Cyber Strategy", Federal Councillor Viola Amherd, Head of the DDPS, outlines the focus areas and assigns the corresponding responsibilities.



DDPS Cyber Strategy 2021- 2024.

The CYD Campus focuses on three primary responsibilities:

Early Identification of Cyber Trends: This involves extensive technology and market monitoring, scouting international start-ups, and fostering a robust cooperation network to stay ahead of developments in the cyber domain.

Research and Innovation in Cyber Technologies: By collaborating with universities and industry partners, the CYD Campus identifies emerging cyber risks and develops innovative solutions to address them. It also aims to enhance the security and resilience of existing cyber systems.

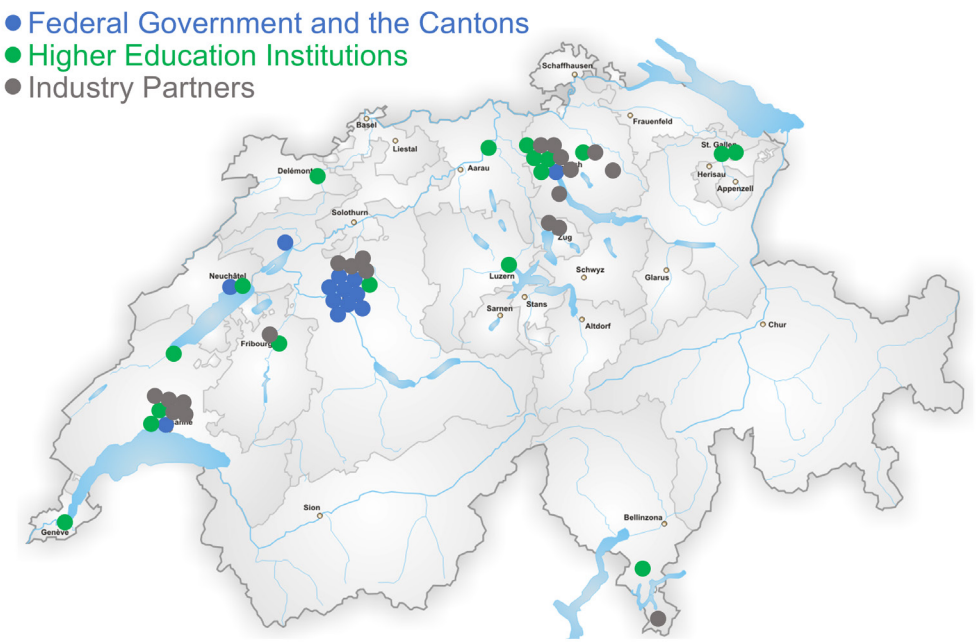
Training Cyber Specialists: The CYD Campus nurtures talent at various academic levels, including master's, doctoral, and postdoctoral programs, while also training interns for future challenges. It organizes joint training activities, such as hackathons, to further develop cyber expertise.

This annual report provides a detailed review at how these tasks were implemented in 2024. It includes an overview of the CYD Campus team, highlights from the year, and a summary of public-facing activities like research projects, customer engagements, and technology demonstrators. The report also covers insights into technology and market monitoring activities, and concludes with an overview of events, presentations and publications.

Core competences of the Cyber-Defence Campus.

Our Partners

National		
Federal Government and the Cantons	Higher Education Institutions	Industry Partners
Cantonal Police Zurich Federal Police fedpol Federal Statistical Office Federal Office of Civil Aviation FOCA Federal Office of Sport FOSPO Federal Department of Foreign Affairs FDFA Federal Intelligence Service FIS National Cyber Security Centre NCSC Swiss Armed Forces Swisstopo Swissnex Trust Valley	Bern University of Applied Sciences (BFH) Paul Scherrer Institute PSI Swiss Federal Institute of Technology in Lausanne (EPFL) • Center for Digital Trust (C4DT) Swiss Federal Institute of Technology in Zurich (ETHZ) • Militärakademie at ETH Zurich (MILAK) • Zurich Information Security and Privacy Center (ZISC) University of Applied Sciences of North-Western Switzerland (FHNW) University of Applied Sciences and Arts of Western Switzerland (HES-SO) University of Applied Sciences and Arts (HSLU) School of Business and Engineering Vaud (HEIG-VD) Eastern Switzerland University of Applied Sciences (OST) University of Applied Sciences and Arts of Southern Switzerland (SUPSI) University of Freiburg University of Geneva University of Lausanne University of Neuchâtel University of St. Gallen University of Zurich Zurich University of Applied Sciences (ZHAW)	Adnovum Anapaya Astrocast Brunner Elektronik CYSEC Decentriq Effixis FLARM Technology IBM Research InfoSec Global Kudelski Security Modulos Nationales Testzentrum für Cybersicherheit Noser Engineering Nozomi Networks RUAG SBB Softcom Technologies Swisscom Tune Insight



International		
Public Organisations	Higher Education Institutions	Industry Partners
Federal Office for Information Security (BSI), GER European Defence Agency EDA KRITIS Luxembourg Army, LUX NATO CCDCOE US Department of Defense, USA	IMDEA Networks, ESP KTH Royal Institute of Technology, SWE KU Leuven, BEL Northeastern University, USA Portland State University, USA Ruhr University of Bochum, GER RPTU Kaiserslautern-Landau, GER University of Murcia, ESP University Rey Juan Carlos, ESP University of Genua, ITA University of Luxembourg, LUX University of Oxford, UK University of Southern California (USC), USA	Countercraft, USA, ENG, ESP CybExer Technologies, EST ONEKEY, GER Osterlab, USA Patronus AI, USA Plug and Play, FRA Quarkslab, FRA SeRo Systems, GER

Faces behind the CYD Campus

CYD Campus Management

Daniel Dorigatti
Head of International Relations and Technology Scouting

Dr. Colin Barschel
Head of Innovation and Industry Collaborations

Stefan Engel
Head of Business Developement and Debuty Head of the CYD Campus

Dr. Vincent Lenders
Executive Director of CYD Campus

Dr. Bernhard Tellenbach
Head of Cyber Security

Dr. Alain Mermoud
Head of Technology Monitoring

Dr. Gérôme Bovet
Head of Cyber Data Technologies

Project Managers and Experts

Cédric Aeschlimann
Cyber Training

Dr. Albert Blarer
Cyber Data Technologies

William Blonay
Cyber Security and International Relations

Dr. Martin Burkhart
Cyber Security

Lucas Crijns
Innovation

Dr. Ljiljana Dolamic
Cyber Data Technologies

Perceval Faramaz
Technology Scouting and International Relations

Peter Hladký
Cyber Security and International Relations

Daniel Hulliger
Cyber Security

Dr. Julian Jang-Jaccard
Technology Monitoring

Dr. Miguel Keer
Cyber Security

Dr. Yago Lizarribar
Cyber Data Technologies

Dr. Raphael Meier
Cyber Data Technologies

Dr. Roland Meier
Cyber Security

Dr. Daniel Moser
Cyber Security

Valentin Mulder
Technology Monitoring

Nicolas Oberli
Cyber Security

Damian Pfammatter
Cyber Security

Llorenç Roma
Cyber Security

Ivo Stragiotti
Cyber Data Technologies

Dr. Martin Strohmeier
Cyber Security

Dr. Etienne Voutaz
Cyber Data Technologies

Support Team

Yasemin Akin
Assistance Zurich

Monia Gieriet
Assistance Thun

Amina Kabashi
Assistance Lausanne

Andrea Alexis Thäler
Communication

Priska Weber
Assistance Thun

2. Highlights

5th Anniversary CYD Campus

The year-end event celebrating the 5th anniversary of the Cyber-Defence Campus honored the best works and projects of recent years. The event highlighted innovative research and technologies that have strengthened cyber security.
Since its establishment in 2019, the CYD Campus has fostered collaboration between academia, industry, and government, serving as an important platform for innovation and practical research. It plays a pivotal role in identifying and countering cyber threats while supporting the development of future cybersecurity experts.
Dr. Vincent Lenders, founder and director of the CYD Campus, reflected on five successful years and outlined future challenges. This was complemented by contributions from Dr. David Gugelmann (Exeon Analytics), Prof. Dr. Shweta Shinde (ETH Zurich) and Prof. Dr. Mathias Payer (EPFL), who discussed current and emerging cyber threats, and how to address them.

At the end of the event, CYD awards were given for the best works and projects of the last five years:

CYD Awards

- **Vladyslav Zubkov (ETH Zurich)** for his master's thesis on "Cross-sectional Analysis of the Bluetooth Stack of Modern Cars."
- **Dr. Dina Mahmoud (EPFL)** for her doctoral dissertation on "Electrical-Level Fault-Injection Attacks on FPGA-based Systems."
- **Dr. Andrei Kucharavy (EPFL)** for his postdoctoral research on "Evolutionary Dynamics for Improved GAN Detection."
- **Ines Arous, Dr. Ljiljana Dolamic, Dr. Jie Yang, Dr. Akansha Bhardwaj, Dr. Giuseppe Cuccu** and **Prof. Dr. Philippe Cudré-Mauroux** for their publication at the AAAI Conference on Artificial Intelligence, titled "Marta: Leveraging Human Rationales for Explainable Text Classification."
- **Dr. Albert Gran Alcoz, Dr. Martin Strohmeier, Dr. Vincent Lenders** and **Prof. Dr. Laurent Vanbever** for their publication at ACM SIGCOMM on "Aggregate-based Congestion Control for Pulse-Wave DDoS Defense."
- **Dr. Sebastian Köhler, Dr. Richard Baker, Dr. Martin Strohmeier** and **Prof. Dr. Ivan Martinovic** for their publication at NDSS on "Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging."
- **Prof. Dr. Dimitri Percia David (HES-SO Valais)** for his contributions in the field of technology monitoring.
- **Melanie Mathys, Marco Willi** and **Prof. Michael Graber (FHNW)** for their contributions to the development of the emerging AI technology "Structured Analysis of AI-generated Images."
- **Prof. Dr. Adrian Perrig, Prof. Dr. David Basin** and **Prof. Dr. Peter Müller (ETH Zurich)** for their contributions to the development of the emerging security technology SCION

- **Friederike Groschupp, Mark Kuhne, Dr. Moritz Schneider, Dr. Ivan Puddu, Prof. Dr. Shweta Shinde** and **Prof. Dr. Srdjan Capkun (ETH Zurich)** for their contribution to cybersecurity with +Phone.

- **Christoph Zubler and Patrick Heeb (Noser Engineering)** for their innovation in "Smartphone as a Sensor and Secure Operations."

- **Dr. David Gugelmann (Exeon Analytics)** for his contributions to the Swiss Armed Forces in combating cyber threats with "ExeonTrace."

Dr. David Gugelmann (Exeon Analytics) during his presentation at the 5th anniversary CYD Campus.

Prof. Dr. Adrian Perrig, Prof. Dr. David Basin and Prof. Dr. Peter Müller (ETH Zurich) for their contributions to the development of the emerging security technology SCION.

CYD Campus Conference at the Kursaal in Bern with over 300 participants.

CYD Campus Conference

This year's Cyber-Defence Campus Conference focused on pioneering advancements in cyber technologies. The event at the Kursaal Bern attracted over 300 participants from government, industry and academia and provided a platform to explore the opportunities and challenges of quantum computing, next-generation networks and artificial intelligence (AI). The conference featured thought-provoking keynotes, expert-led presentations, and an engaging panel discussion, establishing it as an exceptional gathering for the cyber community.

Dr. Vincent Lenders, Director of the Cyber-Defence Campus, and Dr. Julian Jang-Jaccard, the Program Chair, opened the conference with speeches that outlined the thematic focus of the event. The first keynote, delivered by Florian Schütz, Director of the National Cyber Security Centre (NCSC), highlighted the transformative impact of artificial intelligence on cyber security. Dr. Heike Riel, an IBM Fellow, introduced participants to the advancements in quantum computing. Her presentation, entitled Quantum Computing – The Path to Quantum Advantage, detailed both the progress made and the challenges ahead in achieving quantum supremacy, while also celebrating the establishment of the first European IBM Quantum Data Centre. Another highlight came from Dominique Gruhl-Bégin, CEO of Innosuisse, who showcased Switzerland's innovative strength in disruptive technologies, highlighting the contributions of Swiss start-ups. Prof. Dr. Torsten Hoefler of ETH Zurich provided a fascinating perspective on the growing importance of scalable systems and the transition to the computer age.

The afternoon sessions continued with Dr. Mart Noorma, Director of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), who led a compelling discussion on emerging disruptive technologies (EDTs) in defence. His emphasis on international cooperation in cyber security resonated strongly with the audience. Prof. Dr. Anne-Marie Kermarrec of EPFL then explored the complex challenges posed by distributed AI systems, while Major General Simon Müller of the Swiss Army addressed the practical application of disruptive technologies in military operations. The day culminated in a fascinating panel discussion on quantum technologies in Switzerland, featuring renowned experts. At the end of the event, the winner of the Cyber Startup Challenge was announced. Patronus AI will have the opportunity to develop a proof of concept by 2025, with a focus on AI security.

The day ended with participants enriched with fresh perspectives, innovative concepts and ample networking opportunities. The Cyber-Defence Campus would like to thank all participants and looks forward to the next edition.

Florian Schütz, Director of the National Cyber Security Centre (NCSC), highlights the transformative impact of artificial intelligence on cyber security at the CYD Campus Conference.

Major General Simon Müller of the Swiss Armed Forces presents the practical application of disruptive technologies in military operations.

3. Students & Fellows

CYD Fellows

The CYD Campus, in partnership with EPFL, launched the CYD Fellowship Programme in 2020 to enable students to delve deeper into cyber defence topics and strengthen Switzerland's expertise in this critical area. This initiative enables students to actively contribute to the country's cyber defence efforts through research during their academic studies.
Since its inception, the programme has grown steadily and was this year in its ninth and tenth call for applications. A competitive talent initiative, the CYD Fellowship provides students with mentorship from a CYD expert who will supervise their research. CYD Fellows are enrolled at Swiss universities but carry out their work at one of the CYD Campus offices: the EPFL Innovation Park in Lausanne, in Zurich or the headquarters in Thun.
CYD Fellowships are awarded several times a year to master's students, doctoral candidates and postdoctoral researchers, as well as a CYD Proof of Concept Fellowship.

Master Thesis	Doctoral	Postdoctoral	Proof of Concept
6 months	4 years	2 years	1 year
Living allowance	Salary	Salary	Personnel costs
Research & conference funds	Research & conference funds	Research & conference funds	Development costs

Fellows in 2024:

Patrick Louis Aldover
CYD Master Fellow
October 2024 – March 2025
Project title: Creating a Secure WAN Using Cloud Service Provider Networks

Maxime Bourassa
CYD Master Fellow
March 2024 – August 2024
Project title: Development of a WAN traffic obfuscation system on programmable network switches

Dr. Ana-Maria Cretu
CYD Postdoctoral Fellow
November 2023 – October 2025
Project title: Methods for the Evaluation of Technologies that Promise Privacy

Edoardo Debenedetti
CYD Doctoral Fellow
June 2023 – May 2027
Project title: Real-world Machine Learning Security and Privacy

Daniele Del Giudice
CYD Master Fellow
September 2024 – March 2025
Project title: Security Analysis of KERI

Dr. Francesca Falzon
CYD Postdoctoral Fellow
July 2023 – June 2025
Project title: Towards More Practical Encrypted Databases with Expressive Queries

Benoit Figuet
CYD PoC Fellow
November 2024 – October 2025
Project title: Real-time GPS interference detection based on broadcasted traffic data

Valentin Huber
CYD Master Fellow
September 2024 – February 2025
Project title: Fuzzing Zephyr with LibAFL

Janina Inauen
CYD Master Fellow
October 2024 – March 2025
Project title: Prediction and Analysis of Crowdsourced Network Dynamics

Dr. Lucianna Kiffer
CYD Postdoctoral Fellow
September 2022 – August 2024
Project title: Security and Usability of Blockchain Networks

Christoph Landolt
CYD Master Fellow
October 2024 – March 2025
Project title: Training of offensive penetration testing agents with Multi-Agent Reinforcement Learning (MARL) on Graphs

Andrea Lepori
CYD Master Fellow
November 2024 – April 2025
Project title: Automated Code Obfuscation through Mutation to Bypass Endpoint Detection and Response (EDR) Systems

Dr. Dina Mahmoud
CYD Doctoral Fellow
September 2020 – August 2024
Project title: Attacks and Defenses on FPGA-CPU Heterogeneous Systems

Louis-Henri Merino
CYD Doctoral Fellow
June 2022 – May 2024
Project title: Coercion-Resistant Remote E-Voting Systems with Everlasting Privacy

Shailesh Mishra
CYD Doctoral Fellow
January 2024 – December 2027
Project title: Privacy-Preserving Self-Sovereign Identity Systems with Key Recovery

Raphael Monstein
CYD PoC Fellow
November 2024 – October 2025
Project title: Real-time GPS interference detection based on broadcasted traffic data

Dhruv Nevatia
CYD Doctoral Fellow
June 2024 – May 2028
Project title: A Framework for the Analysis of DNS and other Timed Network Protocols

Basil Ottinger
CYD Master Fellow
November 2023 – April 2024
Project title: Towards Comprehensive Measurement of Global DNS Amplification Threats

Dominique Portenier
CYD Master Fellow
April 2024 – September 2024
Project title: Security Analysis of the SCION Internet Architecture

Marco Seewer
CYD Master Fellow
March 2024 – August 2024
Project title: Security Analysis of the SCION Internet Architecture

Simon Sommerhalder
CYD Master Fellow
November 2023 – April 2024
Project title: Challenges in Robust Detection of Attack Traffic

Alessandro Stolfo
CYD Doctoral Fellow
January 2022 – December 2025
Project title: Privacy-Preserving Learning of Neural Language Models

Filippo Visconti
CYD Master Fellow
April 2024 – September 2024
Project title: Securing Satellite Receivers Firmware Upgrades

Academic Interns

To build cyber expertise among students and enhance Switzerland's long-term resilience to cyber threats, the Cyber-Defence Campus offers academic internships at its three locations. In 2024, a total of 20 students from various universities completed internships, gaining hands-on experience in the field of cyber defence.

Samuel Albrecht

Camille Arruat

Evan Blezinger

Cristian Botocan

Victor Carles

Alessandro Colombo

Henrique Da Silva Gameiro

Cesar Descalzo

Dimitri Francolla

Ana-Maria Indreias

Inan Kadioglu

Grégoire Messmer

Nathan Monnet

Iana Peix

Evgueni Rousselot

Martin Sand

Joshua Smailes

Alexander Sternfeld

Igor Szymanowski

Naima Zingg

Students

CYD Campus members propose and oversee student research projects at the bachelor's, master's, and PhD levels. These projects are carried out at CYD Campus facilities in Lausanne (EPFL), Zurich (near ETHZ), and Thun. In 2024, the CYD Campus supported 22 students in completing their academic projects, contributing to the development of future cyber-defence professionals.

Sami Abuzakuk

Dominique Alguacil

Silvan Bitterli

Isis Daudé

Thomas Ecabert

Simon Englert

Lucas Falardi

Robin Goumaz

Piotr Kulpiński

Marvin Leuenberger

Hain Luud

Damiano Mombelli

Sarina Müller

Joshua Ruoss

Kolja Schön

Mihhail Sokolov

Cédric Solenthaler

Adrian Zanga

Yufei Zhang

Qianjun Zheng

Mehdi Ziazi

Vladyslav Zubkov

4. Talent Promotion

Alessandro Stolfo – Doctoral Fellow at the CYD Campus and at ETH Zurich

Why did you decide to do your Doctoral thesis at CYD Campus?

My interest in interpreting and understanding AI systems to improve their reliability and robustness aligned well with the CYD Campus' focus on security. It also seemed like an excellent opportunity to gain insight into the workings of a governmental institution addressing one of today's most critical challenges.

How do you find working with your mentor?

It's been a positive experience. We meet monthly to discuss my research progress, and her input is consistently valuable in refining my work and navigating challenges.

Where do you see your greatest potential for development during the CYD Fellowship?

The opportunity to exchange ideas with other fellows and CYD Campus researchers is where I see the greatest potential for development. These interactions provide fresh perspectives and foster collaborations that enrich my research.

What contribution does your work make to the CYD Campus?

My publications help give visibility to the CYD Campus within the machine learning interpretability community. Additionally, by presenting my work and sharing the knowledge I've accumulated, I actively contribute to the collaborative and innovative environment at the CYD Campus.

Would you recommend the CYD Fellowship to other students and would you apply again as a CYD Doctoral Fellow?

Yes, I would recommend the CYD Fellowship to other students and would gladly apply again as a CYD Doctoral Fellow.

Dr. Ljiljana Dolamic – Mentor of Alessandro at the CYD Campus

What topic from your time as a mentor at CYD Campus stands out in your mind and why?

Since the CYD fellowship program started, I have had the opportunity and, I have to add, the pleasure to be the mentor for one PostDoc project and one ongoing PhD thesis. From December 2020 until December 2022, I have collaborated with Prof. Dr. Andrei Kucharavy during his post doc fellowship. We have continued the collaboration once his fellowship ended. Currently, I am the CYD Campus mentor for the PhD thesis of Alessandro Stolfo. To be honest, it is impossible for me to choose one of these projects and say it stands out.

Where do you see the greatest potential for development in the CYD Fellows when they start at CYD Campus?

The CYD Fellowship has gained the prestige over the years. Future fellows need to undergo very tough selection procedure to be awarded the fellowship. Once they start working with us, they have the opportunity to meet and to exchange with our collaborators, other fellows or interns all originating from various scientific fields.

What do you like about working with the CYD Fellows?

For me personally, it was and still is a very enriching experience. It gave me the opportunity to work with highly motivated researchers on the cutting-edge technology. Over the past couple of years, I was in the position to learn a lot from my fellows.

Have you had to adapt your mentoring style over the years?

I do not believe in "mentoring style", be it with the CYD Fellows or in generally mentoring any research. The approach itself depends highly on the person one needs to mentor. One needs to adapt this approach for each single fellow. I do follow closely the development itself, trying to be available as much as possible in case of need, but without imposing my personal preferences.

How does the work of the CYD Fellows influence the CYD Campus?

The work done by the CYD Fellows as well as the findings and technologies of the various projects are transferred to the CYD Campus by the mentors, which allows for the potential follow-up research, development or direct implementation, depending on the maturity of the given technology.

Christoph Landolt – Master Fellow at the CYD Campus and at OST

How did you find out about CYD Campus?

I first learned about the Cyber-Defence Campus during my military service in 2023, when I participated in fascinating training on cybersecurity in aviation. I was inspired by the presentation on CYD Campus' projects and the innovative ways they approach cybersecurity challenges. Their work aligned with my interest in combining machine learning and cybersecurity, leading me to attend their conference later that year. There, I got to know the CYD Fellowship programs and then applied with a project proposal, which was fortunately accepted.

Which area of the cyber sector interests you the most?

I am particularly interested in the intersection of machine learning and cybersecurity. The vast amount of data generated by computer networks and the complex interactions between users make this a compelling area for developing and applying advanced machine-learning models to address emerging challenges and detect sophisticated attacks. Since cyber security is not just a technical problem but also has implications in areas such as computer science, artificial intelligence, policing, law and law enforcement, national security, business, and research, the CYD Campus community offers an extremely exciting network of people, which makes collaboration both stimulating and educational.

What did you get out of your poster pitch at this year's CYD Campus Conference at the Kursaal Bern?

The CYD Campus conference took place three weeks after the start of my fellowship, and I had the opportunity to present the project proposal. This poster pitch allowed me to receive constructive feedback and insights from specialists across various fields, enhancing the practical relevance of my project. Additionally, it enabled me to build a strong network of professionals from both industry and academia, offering access to expertise and support in areas where I may need guidance throughout my project.

What are your professional goals after your master's degree?

I truly enjoy working in research, especially in collaborative environments where ideas can be shared and refined with others, such as in the CYD Campus community. What I find particularly cool is the opportunity to contribute to technical development in a multi-disciplined team of peers and mentors and to test new concepts.

Dr. Julian Jang-Jaccard – Mentor of Christoph at the CYD Campus

How long have you been a mentor for CYD Campus?

Though it has been only two months since I was formally nominated as a mentor to a Master's fellowship student at CYD Campus, I bring over 10 years of experience supervising postgraduate students, including master, doctoral, and postdoctoral levels, from my time as a professor before I joined the CYD Campus slightly more than a year ago.

What advice would you give the CYD Fellows?

I always emphasize the importance of time management, as it is a critical factor for success in any research endeavor—or in life in general. Alongside time management, staying organized is equally important (e.g., keeping detailed records of experiments, results, and ideas) to maintain clarity and track progress. I also strongly recommend starting to write at an early stage of research. Writing is the primary communication medium in the scientific community, and engaging in it early can help refine research ideas and effectively communicate findings to others.

What are your responsibilities as a CYD Fellow mentor?

I think there are several key responsibilities. The first is to provide guidance on aspects related to the fellow's research topic, such as methodologies, experimental design, and data analysis. Another critical responsibility is to assist with academic writing, helping the fellow develop their skills in effectively communicating their research. Regularly reviewing their progress and providing constructive feedback is equally important to ensure they stay on track and make meaningful improvements.

What can you personally learn from the CYD Fellows or take away with you?

I always find that mentoring postgraduate students provides a valuable opportunity for me to be exposed to fresh ideas, new methodologies, and areas of study that I may not have deeply explored before. I often learn from fellows as they bring innovative perspectives and introduce me to emerging trends, tools, and topics. Additionally, mentorship offers a chance to expand my professional network by connecting with new professors and institutes.

5. Cyber Security

The aim of the research projects in the field of cyber security is to develop and ensure technological expertise for the identification, assessment and reduction of risks in cyberspace. Due to the very short technology cycles and the rapidly changing threat situation, the research priorities are managed in an agile way along the trends and the needs of the DDPS.

Automated Exploit Generation for the Linux Kernel

Today, the Linux kernel serves as the foundation for various operating systems which in turn are used on a wide range of devices, including desktop PCs, servers, mobile or embedded systems. Due to its extensive usage, the Linux kernel has become an interesting target for attackers aiming to compromise a system.
In a multi-year collaboration with IBM Research Zurich, we are researching on methods to automatically determine if a potential bug in the Linux kernel is security-relevant. This question is important since automated bug identification projects like syzkaller find and publish bugs every day. Identifying the ones which allow an attacker to exploit the system would therefore allow for prioritizing the elimination of critical vulnerabilities.
This year's activities have culminated in a research paper that systematically summarizes the knowledge gained in Automated Exploit Generation (AEG) for the Linux kernel. Furthermore, the development of a proof-of-concept (PoC) tool has advanced to the state where it has been validated on initial bugs with resulting PoC exploits. Future work should focus on expanding the tool's applicability to a broader range of bugs and vulnerability classes. Another sub-project of our research activities focuses on developing an automated method to identify data-only targets. Data-only attack techniques have recently gained popularity, as they can bypass modern security mechanisms, such as Control Flow Integrity (CFI). Initial results have already demonstrated the effectiveness of the implemented approach, revealing previously unknown kernel objects that attackers could misuse to extend their capabilities.

Hacking Micro Drones

Unmanned aerial vehicles (UAVs), commonly referred to as drones, are transforming both the security and military fields. Advances in technology, particularly in miniaturization and cost reduction, have led to a surge in the use of mini UAVs within civilian applications. However, these drones can also be weaponized, as has been demonstrated in the ongoing conflict in Ukraine. They represent a significant threat to military and other organisations due to their advanced sensors, which enable them to infiltrate or gather data in restricted areas. Consequently, these organisations are eager to develop strategies to counteract the risks associated with mini UAVs.
This project aims to explore various methods for disrupting and gaining control over mini UAVs to neutralize their threat. It examines the potential of exploiting control and navigation channels through sophisticated techniques like signal jamming, spoofing, and software manipulation. More specifically, this year we concentrated on a comprehensive analysis and the preliminary development of a proof of concept (PoC) for a spoofer that will allow to showcase and to explore the vulnerabilities within ADS-L

(ADS-B "light"). While not broadly implemented in commercial drones, this is a concept introduced by the European Aviation Safety Agency (EASA) in 2022, originally designed for the surveillance of manned aircraft in U-Space airspace.

Cyber Scurity in the Domotics and Building Automation Domain

As buildings become smart, the connectivity needs for devices that help control heating, ventilation, air conditioning, lighting, shading, energy production or other building-related functions, for example access control, also increases. As these devices have mostly been designed for industrial use, their security posture is often quite weak but slowly increasing with the introduction of cybersecurity standards and norms along with new and more secure communication protocols.
To evaluate and test those new features, several testbenches are built in partnership with universities and manufacturers. These testbenches mimic Building Automation and Control Systems that could be found in the federal administration and will allow for performing more accurate cyber security evaluations. These testbenches have the form of racks that simulate an individual building system. Those racks can be linked together to form a wider network of centrally managed buildings.
A Building Automation and Control System focused hackathon will happen next year and will showcase these racks along with standalone devices that can be used for testing their cyber security exposure and evaluate potential migration plans for older buildings.

Self-Sovereign Identity (SSI) as a Basis for National Digital Identities

The E-ID, Switzerland's new digital identity, is expected to be available as early as 2026. After the rejection of the 2021 E-ID concept by the Swiss population, the federal government had to revise the bill. One important reason for the rejection at the ballot was the inadequate protection of users' privacy. This point is now explicitly addressed, and users largely retain control over their data. The new paradigm is called Self-Sovereign Identity (SSI) and is also being used in the EU along with eIDAS 2.0. With SSI, central infrastructure elements that control, correlate and monitor the actions of individuals are avoided.
SSI is a young technology, and the international standardization of various components is still ongoing. For SSI to become a solid technological basis, various aspects such as security, scalability, user-friendliness and data protection need to be considered. This year, the CYD Campus has been advising FEDPOL and FOITT by researching several topics.
Encryption keys are the foundation of SSI. Hence, we assessed a potential solution for distributed management of these encryption keys in a Swiss E-ID scenario. The main challenge was how to build up trust between the different participants. Also, a solution for backing up secret keys with the help of social peers was developed by one of our PhD fellows. When it comes to protection of user privacy, two things are important: Selectively disclosing information and not leaking information accidentally, e.g., by using static technical IDs in revocation services. For selective disclosure, the use of cryptographic zero-knowledge-proof (ZKP) frameworks has been studied. While still a bit impractical, this technology is very promising for future use. Moreover, we designed a practical privacy-preserving revocation solution that refrains from using any static elements that could be correlated.

Securing "Infrastructure as Code"

Infrastructure as Code (IaC) has become widely adopted for automating cloud infrastructure management and provisioning. Ensuring accurate cloud configurations is crucial because minimal errors can lead to complete outages of the hosted services or to security issues. Unfortunately, traditional verification methods require deploying the infrastructure before checking its correctness, which greatly delays feedback – hindering common CI/CD approaches – and increases costs.
In this project, we collaborate with the University of St. Gallen to explore the possibilities of verifying the infrastructural code before deployment, offering cloud administrators early insights into issues like network reachability and access control without any cloud interaction. The key insight is that executing IaC in a controlled environment (preview mode) instead of the cloud still enables a verification procedure that covers a large majority of the interesting properties of the final system. We focus on mainstream management tools, specifically Terraform. However, the approach is largely applicable to other tools, as the mock representation of cloud entities that we develop for a local execution can be adopted in different frameworks.
In 2024, we laid the foundations for automated testing and verification: We developed a methodology for automated configuration testing and we collected large datasets of publicly available IaC programs, which will be needed to evaluate the methodology later.

Automating Cyber Defence

In today's rapidly evolving cyber threat landscape, automating cyber defence systems has become essential to keeping pace with sophisticated and relentless attacks. Traditional, manual defenses are often too slow, reactive, and resource-intensive to effectively counter modern threats. By automating key aspects of cyber defence, we aim at detecting, responding to, and mitigating attacks faster and more efficiently, ultimately enhancing resilience and freeing up human experts to focus on higher-level strategy and complex decision-making.
Part of our vision is to create a fully automated cyber defence team capable of participating in exercises such as Locked Shields, with minimal human intervention. Locked Shields, the world's largest cyber defense exercise, represents an ideal proving ground for our research. This vision is a multi-year initiative together with an international team of researchers and students and in collaboration with the NATO CCDCoE.
In 2024, we took part in the Locked Shields to evaluate previously developed tools. Additionally, we collected and published a labeled network traffic dataset, which now serves as a valuable resource for us and other researchers. We also surveyed existing literature on the use of AI in Security Operations Centers (SOCs), analyzing current trends, challenges, and opportunities in automated cyber defense.

Securing Wide-Area Networks

Many public and private organisations use Wide-Area Networks (WANs) to connect their geographically distributed sites. Given that these WANs are often critical for the organisation's operations, their security with respect to confidentiality, integrity, and availability is crucial. A high level of security can be reached if the WAN is built with a dedicated network infrastructure, with the organisation operating its own layer-2/3 routing, for example, multiprotocol label

switching on top of dedicated fibers or leased lines. Unfortunately, this approach is often slow to deploy, requires high operational effort, and is too expensive for many use cases. A cheaper alternative is to construct the WAN as an overlay network on the infrastructure of public Internet service providers (ISPs). Unfortunately, the security of such a WAN is suboptimal. For instance, traffic analysis attacks (on encrypted traffic) can reveal sensitive information transmitted over these public networks, compromised routers between the sites can alter packets, and network-layer distributed denial-of-service (DDoS) attacks can disrupt connectivity.
In this project, we developed a novel inter-ISP network architecture that provides the desired level of control and security for WAN operators, achieving the best of the two above approaches: strong security properties on a cost-efficient public Internet fabric. Our architecture builds on the SCION next-generation Internet architecture and adds extensions for fine-grained path control, connectivity guarantees in the presence of DDoS attacks, and traffic analysis prevention. With this architecture, WAN operators can build on public layer-3 network connectivity services to deploy secure WANs.
In 2024, we first developed the architecture, and we worked on the research and implementation of its individual components. In collaboration with researchers and students from ETH Zurich and EPFL, we increase the technology readiness level of several components (e.g., traffic obfuscation, flexible routing, and bandwidth reservation) and we analyzed the security of today's SCION appliances and deployments.

Vulnerability Research

The vulnerability research program focused on achieving three main objectives. First, it aimed to analyze both hardware and software to identify vulnerabilities that could directly impact IT systems of the Swiss Government. Second, it sought to validate and refine the tools and techniques used to maximize the program's effectiveness. Lastly, the program aimed to demonstrate the real-world impacts of attacks to a wider audience, raising awareness of critical security risks.

TCAS avionics lab at the CYD Campus in Thun.

Consequently, we were able to release an open-source tool, called Morion, which is a proof-of-concept tool for symbolic execution. This tool is designed to assist in the identification and assessment of potential software bugs with regard to their exploitability. In addition, a static analysis tool was developed which employs backward slicing to identify risky code paths, particularly in instances where untrusted data could potentially impact sensitive operations.
The systematic fuzzing of multiple anti-virus engines led to the discovery of multiple memory corruption vulnerabilities with a direct impact on internal systems.
In order to rise awareness of the simplicity and security impact of the Trusted Platform Module (TPM) sniffing attack, a demonstrator was constructed. This demonstrator enables to show the ease with which the attack can be executed and the immediate security impact on Bitlocker-encrypted devices.

Secure, Robust and Resilient Space Systems

This project addresses the critical cyber security challenges in space infrastructure, where many outdated technologies remain in use, often unchanged for decades. Wireless communication systems in these infrastructures frequently lack both encryption and authentication, creating fundamental security risks. Even when encryption is applied, it often relies on weak, proprietary systems instead of secure, open standards, contradicting Kerckhoffs's principle for secure cryptosystems. Newer satellite technologies, such as CubeSats, are also often inadequately tested for security vulnerabilities and lack a primary focus on cyber security in their design.
The project's key research areas include a comprehensive security analysis of modern Low Earth Orbit (LEO) satellite systems, identifying specific vulnerabilities and privacy risks, and developing more robust satellite communication protocols to withstand security threats. Additional research investigates the impact of interference on global navigation satellite systems (GNSS), especially from aircraft communications, and explores vulnerabilities in Very Small Aperture Terminal (VSAT) systems, examining potential exploitation methods via wireless interfaces.
In 2024, we explored a range of security challenges in satellite communications and infrastructure. Our work emphasizes robust satellite fingerprinting against jamming attacks, secure public key infrastructure for interplanetary networks, and inherent security issues in current VSAT configurations. Other studies focus on new techniques for identifying the location of LEO satellite users within defined reception-only areas, effective reconnaissance strategies for satellite cyber security, vulnerabilities in VSAT satellite modems through wireless signal injection, and remote exploitation of VSAT modems from the ground. Through these efforts, the project aims to enhance the resilience and security of space-based systems, establishing a foundation for secure communication in aerospace.

Protection of Unsafe Avionics Systems

This research project focuses on analyzing vulnerabilities in avionics hardware and the associated protocols. In recent years, researchers at CYD Campus have used the avionics lab in Thun to explore attacks on ADS-B (Automatic Dependent Surveillance–Broadcast , CPDLC (Controller-Pilot Data Link Communications), Multilateration, and FLARM technologies, both theoretically and practically.

FLARM is a collision avoidance system for light aircraft and drones, developed in Switzerland, that has gained widespread recognition and adoption globally and has informed the new European protocol ADS-L.
In 2024, the researchers publicly demonstrated the first practical attacks on TCAS (Traffic Collision Avoidance System), which is used in larger aircraft. Beyond this, attacks on the Global Positioning System (GPS), have received even more attention globally, particularly in light of the geopolitical tensions following the outbreak of the Ukraine conflict. Hence, the CYD Campus and partners have been developing monitoring systems that can help detect such jamming and spoofing attacks on commercial and military aircraft.

Human Factors in Security and Safety

Phishing attacks are becoming increasingly sophisticated, targeting individuals directly and exploiting cognitive biases, such as the appearance of authority or urgency. Earlier approaches to user training focused on URL warnings, text-based, or click-based training, with mixed results. To develop more interactive training that is not limited to users' screens, we are exploring the potential of augmented reality (AR) technologies to enhance phishing detection. By using visual representations of biases that attackers commonly exploit and engaging users in haptic interactions, this training aims to help users counteract cognitive biases through heightened awareness and caution.
In a lab study with 100 participants, we evaluated phishing detection rates, user interaction, and feedback on the AR-based training compared to a click-based version and a control condition. Our results show that interactive phishing training that accounts for cognitive biases can increase detection rates by 33%, with interactive elements being well-received. In 2024, we further explored how to personalize phishing training based on different user characteristics and have started testing this in a large-scale, multi-year field study.

Securing Future Electric Vehicles and their Charging Infrastructure

As part of the transition to electric vehicles within the DDPS, the security of existing charging infrastructure must also be reviewed. Preliminary work had already shown that in some Power Line Communication (PLC) systems, data transmissions can be wirelessly intercepted from a distance. This could have various implications for the security and privacy of vehicles and infrastructure. During the CYD Campus Car Hackathon in Thun in October 2021, an active attack on a charging system was developed, where a Denial-of-Service (DoS) attack could wirelessly interrupt and terminate the charging process with minimal effort. This attack, named "Brokenwire," was reported to the National Cyber Security Centre (NCSC), and the researchers involved are in contact with vehicle and charger manufacturers to mitigate it. The analysis of such attacks and possible countermeasures was conducted throughout 2022 and expanded in another hackathon in 2023.
This year, our research focused on the security of Bluetooth systems in civilian vehicles. To support this, a new tool called Bluetoolkit was developed, which can almost fully automate the detection of known security vulnerabilities, potentially useful for procurement processes. A study of 22 vehicles demonstrated that even modern cars have critical Bluetooth security vulnerabilities. Further research on battery management systems and electric charging security is ongoing in various collaborations with academia and industry.

Dr. Bernhard Tellenbach at the Cyber Alp Retreat leading the cyber security session.

6. Cyber Data Technologies

In 2024, the former Data Science Group redefined its focus with the aim of sharpen its position in a rapidly evolving technological world. The experience gained from previous years revealed that the field of data science is too large to deal with all kinds of data science projects. While working with data, having a sound domain knowledge in connection with the problem which needs to be solved is paramount. It is only by having a deep understanding of the challenge, the context, and the data itself that a superior solution can be elaborated. As it is challenging to cover all kinds of data science domains, the group therefore focuses now on specific data domains.

Our new focus is at the intersection between data technologies and the cyberspace. This new strategic orientation also led to a new group name, which is now Cyber Data Technologies (CDT). We will now move our efforts towards a more secure cyberspace by relying on data technologies and more broadly Artificial Intelligence (AI).

Towards AI-Augmented Cyber Security

CyberMind

The main objective of the CyberMind project is to research, design, and implement a cybersecurity framework providing various measures that can be taken to protect AI-based systems and models, and keep them secure from a range of emerging attacks. We put our focus on conducting a thorough analysis of existing techniques and methodologiesutilized for adversarial attacks in Distributed Federated Learning (DFL) frameworks. Innovative approaches for poisoning and inference attacks on DFL were developed, implemented, and evaluated by identifying and exploiting vulnerabilities in DFL. We also put emphasis on enhancing the resiliency of DFL systems to cyberattacks by designing and implementing a multilayer defence framework that leverages novel cybersecurity mechanisms. To identify and mitigate vulnerabilities, defensive strategies such as Anomaly Detection systems (AD), supervised Machine Learning (ML) techniques, and Moving Target Defence (MTD) mechanisms have been explored, designed, and implemented to counter cyberattacks targeting DFL systems across diverse layers. Finally, we were able to increase the trustworthiness of ML/DL/FL models by designing and implementing a framework in charge of computing the reputation of participants training FL models and assessing the quality of datasets used to train ML/DL models. To accomplish that objective, we defined a taxonomy of dimensions relevant to computing the reputation of participants in centralized and decentralized FL.
We thus designed and implemented a preliminary decentralized framework to compute the reputation score of each participant and validated the correct functioning and performance of the framework with several decentralized FL models. Furthermore, we assessed data quality while computing the trustworthiness of ML/DL models. To accomplish that objective, we defined a taxonomy with dimensions relevant to data quality assessment, such as data accuracy, completeness, uniqueness, validity, or timeless,

and finally designed and implemented a preliminary framework to calculate the quality of data used to train heterogeneous ML and DL models.

IoT Smart Guardian

The integration of Internet of Things (IoT) devices in smart homes has vastly improved convenience and efficiency in our daily lives. However, this technological advancement has also increased the vulnerability of these systems to cyberattacks and malfunctions. In this project, we aimed at developing robust methods for detecting anomalies and potential attacks in smart home systems, focusing exclusively on sensor data analysis. By not relying on physical layer or protocol-specific information, the proposed approach ensures compatibility across various sensor technologies, including WiFi, RF, ZigBee, Matter, etc. The key objective was to design and implement causal discovery algorithms that can, in an unsupervised manner, identify causal relationships in sensor data to detect effectively malfunctions or security breaches. For this purpose, we started with the collection of data from a real smart home. This data was in a second step used to train various unsupervised algorithms taking causal aspects between several timeseries into consideration. From our experiments, we can state that such causal algorithms can indeed be used under certain conditions to detect misbehaving IoT devices. For this purpose, the algorithms take into account the interdependency of timeseries across IoT sensors. As an example, we could detect that the heating system might have been hijacked in case it starts heating during the summer while the temperature sensors report a high value, and with no presence in the house being detected.

Improving the Cyber Security of Energy Networks by Analysing Operational Data

The aim of this research is to detect on-off (man in the middle) attacks on an electrical network. An approach based on machine learning has shown encouraging results. However, the lack of operational data means that this approach cannot be validated. As a first step, an algorithm generating synthetic data was developed and validated using real data. The machine learning methods were then validated using this data: The type of attacks considered can be reliably detected. The fact that unsupervised algorithms have proved particularly effective for this task is interesting because it frees the ground truth from the arbitrariness of specific anomaly shapes when training algorithms. An interactive tool was then developed to visualize the impact of cyber anomalies on network operations.

The screens on the right represent the real state of the network (top) and as seen by an operator who is the victim of a data anomaly (bottom). The screen on the left shows the menu for selecting the dispatch, target control units (in this case the hydraulic control units of Pradella and Sils) and detection algorithms (NBC and MLPR). The operator's biased view can lead him to make poor decisions that have a negative impact on network operations.

Anticipation of Cyberattacks

Cyber attacks, data breaches, and vulnerabilities have become a mainstream problem. It would be quite attractive to anticipate attacks before they happen. Predictions could allow to move from purely reactive responses towards proactive defences, saving costly expenses and reputation repair campaigns. In the world of non-cyber warfare (e.g. criminality, social conflicts or activism) the predictive qualities and technologies have reached a high sophistication. Social unrest in different countries, for example, can be predicted accurately from social media activities. Comparable to this, cyberattacks are never isolated. They are motivated by end goals that can inform analysis and they happen in cycles and patterns. In this research, we conduct a correlation analysis over time of cyber-related news articles obtained from the Global Data on Events, Location, and Tone (GDELT - an open data source). We apply both supervised and unsupervised text analysis techniques to understand spatial, temporal and distributional topic patterns. Experimental results show interesting trends, cycles and patterns with respect to cyberattacks such as ransomware, data breach and denial of service attacks. To understand the increasingly evolving spectrum of cyber events, the correlation approach will be extended by a causality approach. Since cause and effect always show a temporal order, the predictive character of this relationship is also given. Elections, geopolitical events or new developments in technology, for instance, may trigger cyberattacks. Here, causal models such as Convergent Cross Mapping (CCM) are used to identify the causal nature of such triggering events.

Making AI Systems more Secure

Forensic Analysis of Diffusion Models for Image Generation

Text-to-image models, such as Stable Diffusion, are increasingly used by threat actors to conduct cyber influence activities. The span of actors and threats is large and ranges from individual scammers stealing money to state or state-sponsored actors conducting cyber influence operations. In particular, the generation of photorealistic images is being used to deceive, manipulate or subvert target audiences. Countering this threat usually starts with a basic analytical question: is the photograph real or synthetic (i.e., AI-generated)? Consequently, this project proposed a set of robust methods to differentiate real from synthetic photographs. It developed a comprehensive taxonomy of visually perceivable artifacts of synthetic images which are tell-tale signs that a photograph is indeed synthetic (e.g. artifacts in human anatomy such as e.g. deformed fingers or wrong number of fingers, see figure below). This taxonomy was integrated in a structured analytic technique (SAT) to provide an effective tool to intelligence analysts to judge authenticity of photographs. Furthermore, Machine Learning methods were trained to automatically differentiate synthetic from real photographs and new ways to combined automatic and manual verification of image authenticity based on the developed SAT were investigated.

Example of artifacts in human anatomy which are a clear sign that the image is AI-generated.

Characterizing and Mitigating Attacks on Large Language Models in Code Generation and Privacy

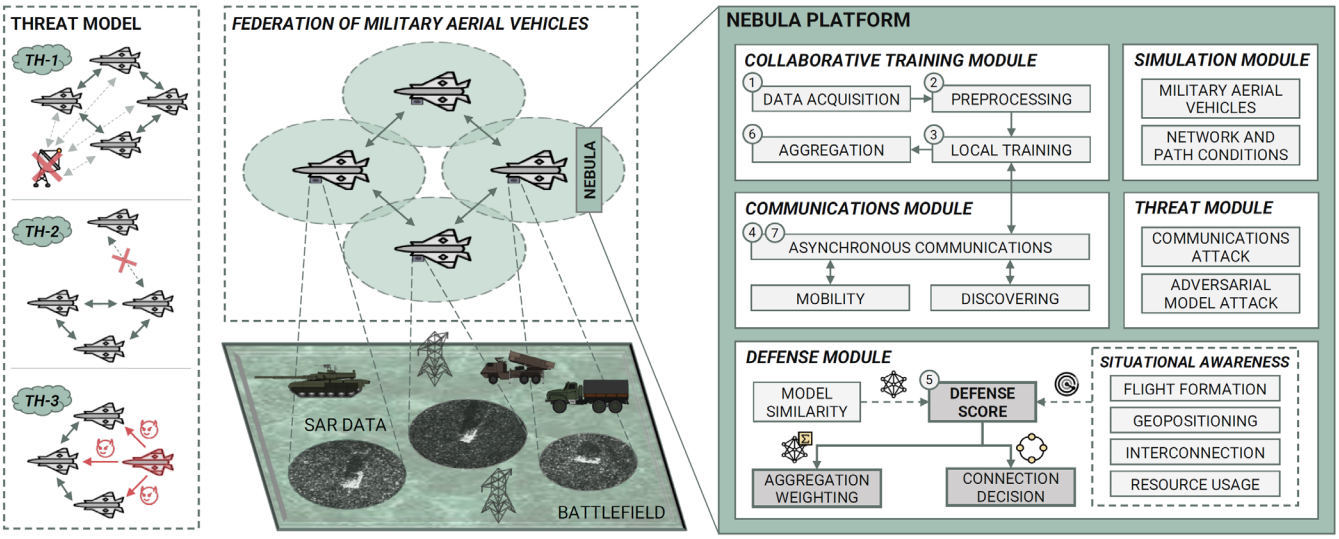
The rapid adoption of coding assistants such as GitHub Copilot or ChatGPT demonstrates the success of LLMs at generating code snippets from surrounding code or explanations in natural language. However, they are trained with enormous quantities of public data, including code containing insecure coding patterns, deprecated functionalities, and libraries that are not considered robust anymore. even if the model outputs a snippet which may appear correct to the user at first sight, it could conceal critical vulnerabilities such as improper input validation (leading to possible injections), missing file I/O closing, missing boundary checking, etc. While dataset curators are increasingly filtering for substandard coding patterns or malicious content, they cannot remove mostly benign patterns with misuse potential in uncommon contexts. Within this project, we created a public database of vulnerability-inducing prompts, based on a new severity metric reflecting both the vulnerability severity and an estimation of how likely it is to affect software in production. We also propose a method to rate models instead of prompts.

ANEMONE: Analysis and Improvement of LLM Robustness

Large Language Models (LLMs) have gained widespread adoption for their ability to generate coherent text and perform complex linguistic tasks. However, concerns around their safety have emerged, particularly related to biases, misinformation, and user data privacy. Using LLMs to automatically generate attacks has become a growing area of research. These attacks often involve generating adversarial inputs designed to exploit weaknesses in target models, such as inducing biased or harmful outputs, or prompting the model to leak sensitive information. Techniques like prompt engineering or adversarial paraphrasing have shown that even minor changes in inputs can lead to drastically different, often undesirable responses. In this project, we propose a new attack framework against LLMs by using another LLM as the attacker. The experiments demonstrate that we can prompt LLMs to generate natural adversarial examples efficiently.

DATRIS: Decentralized AI for Trustworthy and Resource-Efficient Intelligent Systems

This project aims to create an innovative framework for optimizing and securing Federated Learning (FL) environments, particularly focusing on Decentralized Federated Learning (DFL), Trustworthy Artificial Intelligence (AI), and the integration of Large Language Models (LLMs) within Sequential and Hierarchical Federated Learning systems. The goal is to enhance the capabilities and trustworthiness of FL systems, making them more efficient, reliable, and ethically sound. FL systems can be particularly useful for tactical defence applications when the knowledge must be distributed across several nodes. We can consider for example embedded systems with limited computing capabilities that will work together to achieve a goal. The detection of cyberattacks or malwares on IoT devices is a typical scenario where FL techniques come at hand. With this project we intend to understand how ML models can be trained in a distributed manner while considering that the nodes follow a common objective. The NEBULA platform developed as part of this project allows to experiment with real datasets and to apply various federation algorithms while considering robustness aspects. Different scenarios can be emulated with different topologies between the nodes involved in the joint training of ML models.



The NEBULA platform enables testing federation algorithms with real data.

RAEL: Robustness Analysis of Foundation Models

State-of-the-art architectures in many software applications and critical infrastructures are based on deep learning models. These models have been shown to be quite vulnerable to very small and carefully crafted perturbations, which pose fundamental questions in terms of safety, security, or performance guarantees at large. Several defence mechanisms have been developed in the last years to make models more robust against data perturbations or targeted attacks, with the best one being adversarial training, in which the model is fine-tuned by adding properly modified samples in the training set. Yet even the best defence mechanisms are not perfect, and the problem of robustness stays fundamentally unsolved. Even more, with the recent emergence of the new AI paradigm based on large foundation models such as GPT, DALL-E and CLIP, novel robustness challenges have been identified due to the lack of control on the data used for training such models, on top of the lack of guarantees about the models themselves. In the context of this project, we developed a comprehensive understanding of the main fundamental differences between the robustness properties of classical deep learning models and those of recent large models. We also reviewed the new attack scenarios that have been identified in the new foundation model paradigm. We finally reviewed and benchmarked the state-of-the-art defence mechanisms in realistic settings for vision and at a certain extend NLP applications. These activities allowed us to find out that some backdoors in foundation models are still present after the fine-tuning process.

Supporting threat analysis activities

ADAN: Anomaly Detection in Dynamic Networks

Detecting anomalies in time series is an area that has been widely explored, and machine learning has proven very effective for this task. The aim of this work is to detect anomalies in graph time series (non-attributed dynamic networks). This scenario is for example interesting for the study of dynamic communication networks where it can be assumed that the content of communications is encrypted and inaccessible. This work was performed using exclusively surrogate/synthetic data. A review of the existing metrics for comparing network structures and capturing local, as well as global deviations was performed. The methods proposed in this work are based on a geometric notion of graph trajectories. A sequence deviating from geodesics is considered abnormal. The abnormality may well become a new normality and, in this case, we observe a regime change. The algorithms are designed with specific considerations towards computational efficiency and scalability.

Deep Canary Trap: Efficient Photo-robust Screen Watermarks to Trace Data Leaks

Leaking of confidential data has been a major threat to governments worldwide. In particular, the intentional leaking of confidential data has more recently been tied to influence activities to undermine trust in government entities and shape online narratives. Figures and images containing confidential information are commonly leaked in such a scenario due to their visual appeal and ability to attract attention. This project set out to develop a new method to embed invisible watermarks in figures and images of classified documents. The watermarks were required to be robust against all transformations that may occur during the process of leakage (e.g. resizing when uploading to a social media platform, .jpeg compression, etc.). In addition, robustness to photographing was an additional requirement as intentional screen capture of classified content by smartphones is a particularly challenging exfiltration channel. As a result, a method based on an encoder-decoder deep learning architecture was developed and evaluated which can embed invisible photo-robust watermarks in figures and images containing information on user, workstation and time to be able to identify the original data leak.

Applications of Large Language Models

Investigating Hallucinations on Retrieval Augmented Generation Systems (IH-RAG)

In the context of Retrieval Augmented Generation, this project is studying LLM generated text with respect to hallucinations and misinterpretation of information. Hallucinations are understood as factually incorrect or unverifiable statements given external world knowledge. In analysing the properties of RAG based systems we can distinguish two aspects. The most obvious aspect is the distinction between information coming from the pre-trained component (e.g. model's internal knowledge) and the retrieved information. The other aspect is the distinction between the actual retrieved information. This project assessing whether it is the retrieved knowledge that takes predominance in generating the LLM answer or, on the contrary, it is more grounded on the intrinsic knowledge acquired by LLMs during pretraining (and fine-tuning), especially in the case where this two information contradict each other. In addition, the existence of the contradiction within various retrieved documents is also covered. As a special case, it investigates the linguistic preferences of the model with regards to the contradictory information being presented to the models in various languages.

Dialect Identifications with Large Language Models: Analysis, Comparisons & Use Cases (DILLMA)

Language identification is a task of classifying utterances into languages, where languages are regarded as discrete classes (one language, one class). Dialects of a language can be overlapping, sharing linguistic similarities, which make the problem more challenging to tackle, where even the existing LLMs struggle on. The main goal of this project is the verification of the performance of LLMs on the task of dialect identification on a range of dialects, comparison of performances with fine-tuned pre-trained model on different language dialects. Given the recent trends of exploiting the capabilities of LLMs for a range of NLP applications, we explore and analyse the capabilities of the available LLMs for language and dialect identifications and classifications, with the focus on utilizing different prompting techniques – such as hard prompting, chain of thought prompting, and soft prompting approaches such as prompt-tuning, prefix-tuning and p-tuning.

Utilisation of LLMs in a Parliamentary Context

Recent studies have shown that bigger LLMs (Large Language Models) tend to yield better results in general. However, open-source albeit slightly smaller models can yield competitive results in many cases, for instance when fine-tuned on a vertical task or on a dedicated domain. The first task in the context of this project was to experimentally

evaluate the performance of various fine-tuned LLMs on specific tasks in a parliamentary intervention context. In particular, we analysed into the use of fine-tuned LLMs to fix data that can be leveraged for generating responses (with a focus on Swiss laws that are often instrumental in contextualizing a parliamentary question and generating a response) as well as their capability to (partially) generate answers given additional context. The results showed that LLMs are not yet suitable for such tasks as they were not able to formulate satisfying answers. In concrete terms, they were not able to identify the correct legal texts related to the question asked. In the second task we were trying to understand how LLMs reason and if this reasoning is biased at its origin with the data which was used for training. By asking LLMs to provide answer to repeatable experimental questions, we were able to find out that they do not have a physical understanding of our physical world, and that their answers are biased due to the data used during training.

Making Edge Devices more Intelligent

Edge-AI-Based early Warning System for Biomedical Data and Central Hub Device for Data Offloading

The goal for this project was to build an edge device logger and a central hub software for efficient data collection of physiological data from soldiers, as well as to assessing the computation capabilities of the edge device. Every year, soldiers suffer from various health incidents during sport activities. We intend to predict such incidents even before they happen by exploiting such physiological data. From the hardware side, all goals have been achieved: the proof-of-concept logger was built and thoroughly tested. The first batch of 5 devices was extended by another contract from the end-user and was powering the data collection campaign for the year 2024. The central hub software was also built, and it is correctly reporting data from both stations of the study. For the edge device software, currently a new dataset was collected to analyse the accuracy of the sensors when doing similar activities at different movement levels. Then, the goal was to develop a version of the Wobble Index used by the US armed forces, adapted to be used with sensors located on the upper arm. These algorithms are going later to be tested on the edge device to test their computation capabilities.

Evaluation of Real-world High-Altitude RF Signal Measurements for Ground Transmitter Localization

We worked on an approach that describes the operation of RF signal localization with High Altitude Balloons (HABs). It has become nowadays very straightforward to jam or spoof various signals. In order to avoid interferences, it is therefore primordial to localize rogue transmitters. While this task has usually be done in the past with ground sensors, they do not offer a wide coverage. This explains our focus on HABs, as like our simulations showed, we could reach a coverage of more than 1000 km for even low power jammers. When it comes the processing of the data collected by the probe located on the HAB, it can happen following two different approaches. With the first one, the signal is processed locally and transmissions identified and tagged with a timestamp, whereas the second one is a more classical approach and stores data until retrieval for a later processing. While the latter has already been battle tested, it has its obvious drawbacks. The first approach, however, could be an interesting innovation. To assess its feasibility, a method to utilize different signal statistics has been proposed. To validate this hypothesis, a dataset containing signals from 1030 and 1090 MHz bands was collected. This data served as reference for our simulations, as we decided to focus in a first step on the localization of secondary radars.

CARING: Compressed Aerial Radio INtelliGence

With Stratosense, we aim at collecting and processing RF data by relying on a High Altitude Balloon (HAB). The Stratosense probe payload software has been redefined to work with the USRP E310 series, because we realized that the previously used Software Defined Radios (SDRs) did not provide a satisfying enough data quality. The first part of the work has been to define the blocks that could run on the SDR board up to the signal storage state. A large change was also to adapt these blocks to work on the RFNoC that some Ettus boards have. These blocks can be programmed through GNURadio and then directly compiled to the RFNoC, thus being vastly more efficient in terms of compute power and energy usage. In the context of a hackathon we focused towards finalising the receiver and integrated the real-time compression work from the project on RF localization. Another important point that was addressed this year is the power supply of the SDR. The current device and battery would exceed the 2 kg limit of the HAB payload. An analysis was made to verify that it could be powered through the current power system and the battery could be removed.

RF signal localization using High Altitude Balloons (HABs).

7. Technology Monitoring

Advancing Technology Intelligence for Cyber Defence

Over the past year, the Technology Monitoring (TM) team has continued to enhance its operational framework through strategic collaborations with academic and industry partners. The aim is to address the rapidly growing need to monitor and anticipate technology trends that could impact national cyber defense capabilities, as outlined in the Swiss National Cyber Strategy (NCS) and the Cyber DDPS Strategy.
The team operates with a dual focus: advancing the scientific development of robust methodologies and ensuring effective project implementation and data delivery. This approach supports critical stakeholders, including national cyber defense organizations, by providing insights into emerging technology trends to inform strategic decision-making.

Ongoing Development of the Technology Market Monitoring (TMM 2.0) Platform

Building on prior advancements, significant progress has been achieved in extending the in-house big data Technology Market Monitoring (TMM 2.0) platform that combines several open and pay-per-use databases and a specialized analytics platform.
A key milestone in 2024 was the integration of patent data as a resource for technology intelligence. By integrating this resource with existing sources, the CYD Campus can now more accurately identify and analyze trends in technology development. This enhancement further enhances the value of our analyses, which already incorporate insights from scientific articles, company data, and the labor market. Scientific advances are analyzed using OpenAlex and the European Patent Database, while market-related information is obtained through platforms such as Crunchbase and Zefix.

Technology Monitoring of Current Advancement of Quantum Technologies

Quantum technologies have been a key focus area given their transformative potential and implications for national security. Monitoring this area has been crucial, as quantum technologies are poised to revolutionize fields essential for safeguarding national security. A significant potential threat lies in the capacity of quantum technology to compromise traditional encryption methods, potentially leaving critical infrastructure vulnerable. By staying informed on the latest progress, the goal is to anticipate shifts in the cyber landscape, assess emerging threats, and strategically guide cyber defense initiatives.

First Quantum Track at Cyber Alp Retreat

The annual Cyber Alp Retreat featured a dedicated quantum track, leveraging contributions from a network of experts across Switzerland. Participants included representatives from the PSI Quantum Center, IBM Quantum, the quantum centers of EPFL and ETH Zurich, as well as industry leaders from IBM, Rigetti, and the head of the Swiss Quantum Commission.

Quantum Topic at the CYD Campus Conference

Experts in quantum technologies were invited to the CYD Conference, where they participated in panel discussions on topics such as the maturity of quantum technologies, Quantum Key Distribution (QKD), and Post-Quantum Cryptography (PQC). These discussions facilitated direct interaction between defense stakeholders and experts, providing clarity on the implications of quantum advancements.

Open Access Study on Quantum Technologies

An open-access study titled "Quantum Technologies: Trends and Implications for Cyberdefence" has been conducted. This study aims to provide a global overview of quantum technology trends within the context of cyber defense and is scheduled for release in the summer of 2025. Through these initiatives, the project is significantly enhancing both the knowledge base and strategic awareness of quantum advancements, ensuring that the defense sector remains informed and prepared for the rapidly evolving technological landscape.

Executing Shor's Algorithm on Existing Quantum Platforms

Quantum computers represent the forefront of technological innovation, yet their practical realization remains uncertain. Currently, most of these machines are experimental prototypes, lacking the full computational power needed to achieve truly groundbreaking capabilities. In the cybersecurity world, the concept of "Q-Day" is anticipated, marking the day when someone builds a quantum computer capable of completely breaking the encryption protocols that underpin the Internet.
The Technology Monitoring team conducted assessments of quantum computing progress by implementing Shor's algorithm through open-source code. This algorithm was tested on state-of-the-art quantum platforms provided by IBM, IonQ, Quantinuum, and Rigetti, all of which offer cloud-based access to their systems. Findings indicate that the development of Shor's algorithm implementation is still in its early stages. Current quantum machines can only factor very small numbers (such as N=15 and 21), and even this is achieved with significant constraints. We concluded that factoring 2048-bit numbers remains a distant goal.

Quantum-Certified Random Number Generation Testbed Exploration

Quantum Random Number Generators (QRNGs) are essential for modern cybersecurity because they provide a level of randomness that is fundamentally unpredictable, utilizing the principles of quantum mechanics. Traditional random number generators, even cryptographically secure ones, rely on algorithms or physical processes that can, in theory, be predicted or reverse-engineered with sufficient computational power. QRNGs, however, harness the inherently random nature of quantum phenomena, making the numbers they generate truly unpredictable. This high-quality randomness is crucial for creating robust encryption keys and securing sensitive communications, especially as cyber threats and computational power increase. As we approach the age of quantum computing, QRNGs are becoming a vital component of cybersecurity infrastructure, helping protect data against increasingly sophisticated attacks.
In collaboration with the Quantum Computing Lab at the Paul Scherrer Institute (PSI), we are exploring a quantum testbed for quantum-certified, device-independent random number generation for encryption purposes. This project leverages one of PSI's in-house quantum systems to investigate new methods of routinely producing randomness through a verifiable quantum source, utilizing system calibration and maintenance data as a by-product.

Attendees of the technology monitoring tracks at the Cyber Alp Retreat 2024.

AI Trend Monitoring

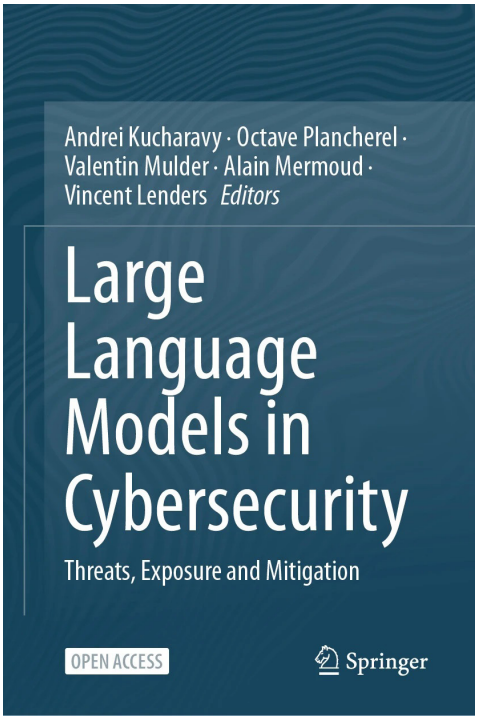
Analyzing trends among AI-focused startups and assessing their cybersecurity readiness is essential for identifying vulnerabilities in emerging technologies at an early stage. This approach enables the cybersecurity community to address potential risks proactively, mitigating threats before they become widespread. Additionally, as AI continues to drive innovation across sectors, ensuring that these startups adopt robust security measures is critical for building public trust and fostering responsible AI deployment. By staying informed about the cybersecurity practices within these rapidly evolving companies, we can support safer technological advancement and promote collaborations that reinforce security across the broader AI ecosystem.
This research project, in partnership with the AI & Digital Economy Lab at the University of Lausanne, provides a combination of state-of-the-art reviews and data on the AI intensity of U.S. firms, focusing on the types of technologies they develop. This exploratory project categorizes AI firms based on their level of AI adoption and examines the technologies they develop, as reflected in patent data. We report on how these AI-intensive firms respond to increased cyber risk given their heightened exposure, and evaluate the measures they employ to protect against cyber threats.

Study on Threats and Impacts of Generative Artificial Intelligence

The development and spread of artificial intelligence present significant challenges for cybersecurity. In particular, machine learning models that generate text, images, and videos – commonly known as generative artificial intelligence (AI) – are becoming increasingly powerful and widely accessible. While generative AI has substantial potential for misuse, including deep fakes, fake news, and fraud attempts, it can also offer positive outcomes when used responsibly.
In collaboration with the University of Applied Sciences and Arts of Western Switzerland Valais, an open-access study titled "Threats and Impacts of Generative Artificial Intelligence on Cybersecurity" was published.

The key findings of the study include:

- Generative artificial intelligence, particularly Large Language Models (LLMs), presents substantial new threats to cybersecurity.
- The use of generative AI within government, industry, and society requires caution to mitigate associated risks.
- Safety checks must be integrated into the data processing chain to ensure secure development and usage of generative AI.



The study highlights the risks and challenges associated with generative AI in cybersecurity, offering valuable insights to experts and decision-makers in public administration and industry for assessing risks and developing appropriate security measures.

Estimating the Cost of Cyber Attacks and Insurances

Since cybersecurity insurance prices are not publicly observable, few firms purchase these contracts, which are typically not public. In collaboration with researchers from the University of Lausanne, this study estimates latent insurance premiums by analyzing firms' stock price reactions to cybersecurity breach events. By leveraging new data from social media, newswires, and stock prices sourced from WRDS, CRSP, and Refinitiv, combined with advanced empirical asset pricing methods, this study provides an innovative approach to uncover historical and current cybersecurity insurance pricing. These insights can support armasuisse in optimizing its procurement strategy within the cybersecurity insurance sector.

Automated Identification of Emerging Technologies

Identifying emerging technologies and forecasting their trends is pivotal for stakeholders and decision-makers across academia, industry, and government agencies. The current strategies employed to track technology trends often rely on proprietary closed datasets and often rely on the insights of human domain experts. Not only are these approaches expensive and manual, but they are also time-consuming.
In this study, we introduce an automated method for identifying emerging trends through a quantitative approach that utilizes extensive publicly available data, including patents, publications, and Wikipedia Pageview statistics. Our method proposes four criteria – novelty, growth, impact, and coherence – to automatically score technologies, based on a mathematical foundation.
This approach enables the monitoring of tech trends across various sectors in an automated manner, without the need for domain experts. The results obtained through rigorous evaluation, benchmarked against similar reports from leading market research firms, illustrate a low recall rate paired with high precision, affirming the reliability of our proposed method. Furthermore, our method identifies emerging technologies not present in similar market reports, highlighting its unique capabilities.

GitHub as a Technology Monitoring Tool: Case with Quantum Technologies

GitHub offers valuable insights into emerging technologies by providing real-time access to code repositories, trends, and collaborative projects. This study examines GitHub's potential as a monitoring tool, with a focus on quantum technologies relevant to cybersecurity.
By analyzing GitHub projects related to quantum computing and quantum communication, insights were obtained using natural language processing (NLP) techniques.
Community engagement, indicated by "stars" on repositories, suggests that quantum technologies are in an early adoption phase, with a primary focus on quantum learning materials. There is also notable interest in quantum algorithms and circuit development to unlock the technology's full potential. Keyword-based analysis on README files attached to each GitHub project highlights the need for transparent guidelines given the complexity of quantum technology. Python plays a central role in quantum development. Time-series-based trend analysis indicates growing projects addressing various aspects, such as integrating classical and quantum computing, post-quantum cryptography solutions, and improving quantum simulation capabilitiesguidelines given the complexity of quantum technology.

Quantum Insights in Finance: Analyzing Trends via Newspaper Headlines

Financial news sources often act as early indicators of emerging technologies with the potential to disrupt markets and industries. By analyzing headlines related to quantum technologies in financial newspapers, one can gain valuable insights into the perceived interest, impact, and market sentiments surrounding these innovations. This approach not only reveals how quantum technology is viewed within the financial market but also sheds light on broader market expectations, extending to sectors like defense. As such, financial newspaper headlines are a valuable resource for staying informed about trends in quantum technology.
We utilized the financial information platform Refinitiv Eikon to gather news headlines from January 2017 to October 2023, focusing on items related to quantum topics. Our analysis showed a strong and growing interest in quantum technologies, with an average growth rate of 250% every two years since 2017. Each major quantum milestone was accompanied by a noticeable surge in interest. Quantum communication topics were the most frequently mentioned in headlines, reflecting a strong focus on securing financial transactions in the near term. Additionally, there was rising interest in futuristic communication technologies like quantum entanglement and quantum internet. Quantum algorithms and machine learning also gained traction, offering promising applications for financial risk management and the development of innovative products.

8. Innovation

Innovation Day

On May 15, 2024, the Cyber-Defence Campus hosted its inaugural Innovation Day in Bern, attracting over 100 participants, including representatives from the Department of Defense, Civil Protection and Sport (DDPS), academia, and industry. This event showcased key innovations in cyber defense, focusing on supporting federal and cantonal stakeholders through emerging technologies.
Highlights included presentations on confidential computing, IoT security, and secure communication via Threema with SCION, led by experts from various government and private organizations. The event emphasized the role of the CYD Campus in developing proof of concepts and expertise in advanced cyber technologies. Attendees appreciated the insights into cutting-edge defense technologies, reinforcing our commitment to fostering innovation for the Swiss defense sector.
The high level of participation of the event underscores the need to supporting defense and cybersecurity advancements in Switzerland through future innovation-focused events.

Cyber Startup Challenges

Smartphone Application Security

We worked with the winner of the 2023 Cyber Startup Challenge, Ostorlab, to test and integrate their technology. The company enables the testing and monitoring of smartphone applications, scanning them for security and privacy issues or listing their components and APIs. It uses advanced analysis capabilities to find vulnerabilities in dependencies, list hard-coded secrets, detect insecure programming patterns, find privacy leaks and intercept back-end communications to identify server-side vulnerabilities. The system dynamically tests applications by interacting with them on real devices running Android and IOS.
While Ostorlab offers a SaaS platform, we were able to install the backend logic on our premises to increase the speed of analysis. The company is building a security scanning orchestrator to automate scans and analyse results. In addition, this system is a first milestone towards a full on-premises solution, which will be important for classified analysis.

Security of AI

The Cyber Start-Up Challenge was held for the fifth time this year. In June 2024, the CYD Campus launched its call for innovative solutions in the field of "Security of Artificial Intelligence". Thirty-eight start-ups responded to the call and presented their solutions to a jury of cyber experts from the DDPS.
Three startups convinced the jury and presented their innovative methods for the security of AI at the CYD Campus Conference on 30 October 2024. The American start-up Patronus AI won the challenge. The company specialises in automated LLM evaluation and provides protection and security measures. Its technology is used to evaluate and compare the performance of LLMs in real-world scenarios, generate large-scale test cases, monitor hallucinations and prevent other unexpected and unsafe behaviours.

IoT Firmware Security Analysis

This year we continue to work with ONEKEY, winner of the Startup Challenge 2022, to analyse more sensitive devices.

About 150 firmwares have been analysed so far. One major vulnerability was discovered and reported to the manufacturer. The vulnerability has now been fixed and new versions of the firmware have been released. In addition, customer-specific analyses have been carried out using ONEKEY. These results are important for procurement projects.

Innovation projects

Smartphone as Sensor

Noser Engineering, winner of the Swiss Society of Defence Technology Challenge 2023, collaborated with CYD Campus on a defense technology project. The CYD Campus contributed expertise in AI, smartphone-based solutions, and infrastructure to develop an AI-driven object recognition platform aligned with the Swiss Army's goals for a comprehensive sensor and intelligence network.
In field trials, soldiers used smartphones to collect and transmit data, which the AI platform analyzed for military relevance. The CYD Campus played a key role in validating AI models, developing the message receiver object detection platform, and ensuring data authenticity with Threema ID verification. This secure, real-time data flow enhanced the Swiss Army's decision-making and digital capabilities, highlighting CYD Campus' vital role in advancing operational intelligence through industry collaboration.

GPU-Based Encrypted Network Traffic Inspection

With most Internet traffic being encrypted and the speeds of network traffic ever increasing, newer, faster ways to inspect such traffic are essential in intrusion detection systems. Analysing encrypted traffic and extracting the certificates or domain names involved is a tedious process that requires massive parallelisation. CPUs are fast but are not well-suited to such highly parallel workloads. This is where GPUs come in: GPUs are optimised for highly parallelised work, which is why they are the cornerstone of modern machine learning. We have shown that high-speed encrypted traffic can be efficiently inspected, and useful data can be extracted on a GPU.

Needle in Haystack at High Speed with an FPGA

Filtering network traffic and determining what is relevant is an essential part of an intrusion detection system. To filter based on content or metadata embedded deeply within a packet at high speed, one needs powerful hardware that can process network traffic in parallel. FPGAs are known for their parallel processing potential, but more importantly, they can be completely fine-tuned for a specific task. We have shown that with an FPGA we can filter network traffic at speeds of more than 100 Gb/s based on reconfigurable rules. To put that into perspective, 100 Gb/s of traffic is more than 15 million packets to search through every second. With this FPGA filter we can literally find a single needle in a haystack of 15 million, every second.

Traffic Caching at High Speed

Networks are becoming faster, but often, the average throughput is not so high. It is the peaks in network traffic that require better links. With existing systems, it becomes increasingly difficult and expensive to accommodate these peaks in throughput. Therefore, we need a system that can absorb these peaks and cache network traffic. We have shown that caching traffic at 100 Gb/s is possible with off-the-shelf hardware.

Ana Maria Montero and Dr. Colin Barschel (CYD Campus) congratulate Michael Westra (Patronus AI) on winning the Cyber Startup Challenge 2024.

9. International Scouting & Cooperations

Scouting

In 2024, the CYD Campus start-up scouting focus was on Switzerland, the United States, the United Kingdom and France, although start-ups from other countries were also considered. The aim of the scouting was to identify new technologies in the areas of cyber security and artificial intelligence to identify important trends and players at an early stage. To do this, interviews were conducted with start-ups and companies, and the insights gained were passed on in a structured way to potential interested parties in the public administration. To gain access to the most promising start-ups and to identify companies in their early stages, the CYD Campus draws on a broad network of venture capitalists, accelerators, ambassadors and business development organisations. Its most important partners include Swisscom's branch in Silicon Valley and the Swissnex network. Another important scouting tool is participation in leading global conferences such as the RSA Conference in San Francisco, Black Hat, Defcon and USENIX Security. These events make it possible to meet many companies and potential partners in a short period of time. The start-ups identified in the scouting process led to several proof-of-concept projects. In addition, the information gathered was used to support the procurement process and to better understand the cyber market.

Research Partnerships

The CYD Campus conducts research projects in collaboration with scientists from leading universities around the world, including the University of Oxford, the University of Genova, or the Ruhr University Bochum.

International Cooperation

CYD Campus also works with international organisations and represents Switzerland in the CapTechs Cyber and Information of the European Defence Agency. When necessary, discussions on specific projects are deepened and CYD Campus researchers assess whether a Swiss contribution would be useful. These committees also provide a platform for informal exchanges among experts. This year, the CYD Campus joined the The European Cyber Security Organisation (ECSO). The CYD Campus is leading the Swiss efforts to potentially participate in a future PESCO project around the Cyber Ranges Federation (CRF). The aim of the CRF is to strengthen the capacities of European cyber ranges by connecting national cyber ranges to form a large cluster.
NATO is also an important cooperation partner: The CYD Campus makes important contributions to the activities of the CCDCoE in Tallinn, both through the presence of researchers William Blonay and Peter Hladký and through research contributions to the work programme. In addition, the CYD Campus participates in selected interesting STO working groups of NATO, supported by the armasuisse office in Brussels.

Bilateral Cooperation

Bilateral exchanges with partner organisations of the DDPS in selected countries in Europe, America and Asia are also of great importance. The CYD Campus works with both large countries, to which it provides its specialised expertise, and with smaller, agile partners that face similar challenges. Depending on the country, the aim is to network researchers with similar interests to exchange expertise, methods and data or, in certain cases, to initiate joint research projects. This collaboration encompasses all areas of the CYD Campus, from technology and market monitoring to cyber security, data science and machine learning.
The CYD Campus works closely with the armasuisse office in Washington and with Swiss embassies and defence attachés worldwide to coordinate and manage projects.

Overall, the CYD Campus is recognised worldwide as an example of successful cooperation between government, academia and industry. Every year, delegations from various countries visit the CYD Campus to learn about best practices. With the aim of strengthening global cyber resilience, the CYD Campus actively shares its knowledge with partners and peers.

Daniel Dorigatti and Luigi Rebuffi, Secretary General and founder of ECSO, marking Switzerland's ECSO membership.

10. Customer & Portfolio Assessment

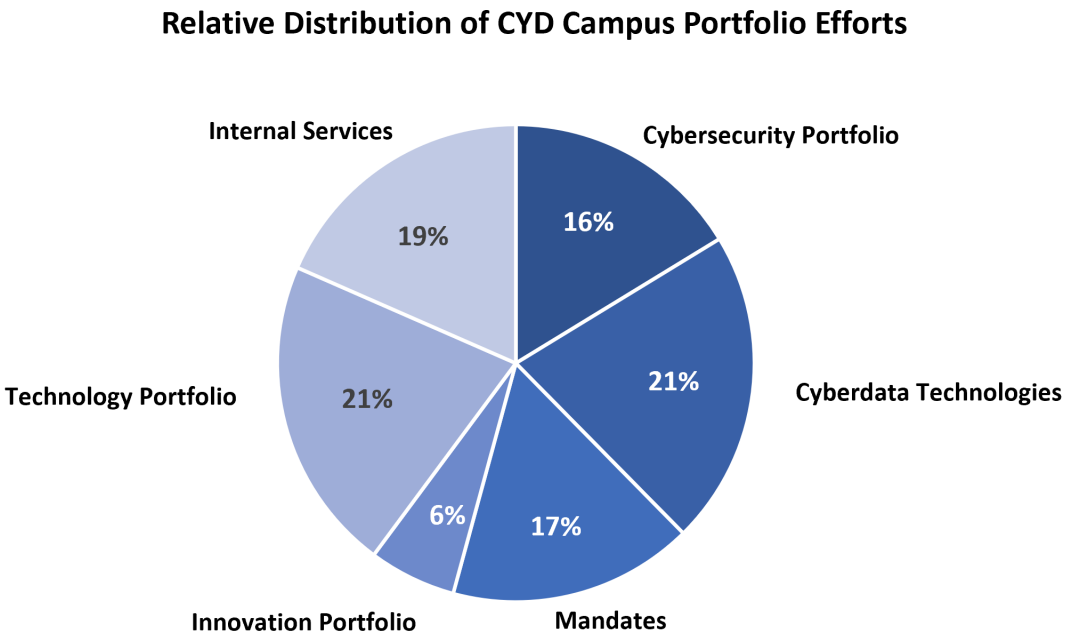
The CYD Campus provides services to various federal offices including armasuisse, the Armed Forces, the Federal Intelligence Service or the Federal Office of Cybersecurity. A common feature of these services is that knowledge generated from the CYD Campus research and innovation is used to provide contributions for basic studies, requirements in the area of procurement, technology transfer concepts and work in the area of cyber security, data science and technology monitoring.

In 2024, the Cyber Command was created within the Armed Forces and the collaboration with this new organization was defined to cover wider spectrum of activities. The CYD Campus conducted studies to increase protection in cyberspace, for security audits and pentesting tests, and for security reviews of secure IT architectures. In this context, CYD Campus members take on various roles in procurement, such as the role of technology or technical responsibility, as well as the role of a penetration tester, a security auditor or a researcher, e.g. when it comes to questions regarding the use of AI technologies.

Various technologies were developed in AI-based speech, image, video and network analysis and classification and provided to the customer as microservices to test the effectiveness of the procedures. Due to data protection and privacy concerns, the application of the procedures in the CYD Campus is not possible, which is why an early technology transformation to the client is necessary. An additional advantage of the procedure is the faster and easier use of new algorithms and a more agile approach to expanding military capabilities for the protection of Switzerland.

In 2024, the CYD Campus supported the following organisations:

- Federal Office for Defence Procurement armasuisse
- Group Defence
- Armed Forces Staff
- Armed Forces Cyber Command
- Joint Operations Command
- Training and Education Command
- Federal Intelligence Service
- DDPS General Secretariat
- Federal Department of Finance
- National Cyber Security Centre NCSC
- Federal Office of Police FEDPOL
- Federal Chancellery


Relative Distribution of CYD Campus Portfolio Efforts
Internal Services
Cybersecurity Portfolio
19%
16%
21%
Technology Portfolio
21%
Cyberdata Technologies
6%
17%
Innovation Portfolio
Mandates

11. Security Services

In 2024, the CYD Campus was again involved in the security testing of military systems and components. These systems were developed as part of the procurement of defense and ICT systems in the DDPS and examined by the CYD Campus as part their security verification. In addition, security components of the new DDPS digital infrastructure were examined. These mandates were commissioned on the direct instructions of the relevant organizational unit. The investigations focused on penetration tests, security advice and security studies.

In 2024, there were approximately 20 investigations, in particular on the following objects:

- Web applications
- Specialist applications
- Middlewares
- Radio Systems
- Various end devices and server systems
- Communication solutions
- Security solutions and architectures
- C2 systems
- Hardware and software crypto systems
- Aviation and satellite communication systems

In order to protect the IT systems of the defense, no detailed information about the vulnerabilities found or the objects under investigation can be provided. However, in addition to the commissioned security tests, the CYD Campus conducts vulnerability research that makes a general contribution to the IT security of the defense and the administration. For the vulnerability research, commercial-of-the-shelf (COTS) products from the administration are selected that can significantly impair security. These vulnerabilities are reported and attributed to the CYD Campus as the discoverer using a standardized process via the CVE number and the advisory, in order to verify and also eliminate them.
Two examples of anonymized investigations are provided to give a more in-depth insight into the activities of CYD Campus in the area of security services. In addition, we provide a list of published vulnerabilities from vulnerability research below.

Pentesting a Web Application Firewall

The objective of this test was to verify the recommended security measures implemented by a web application firewall. The aim of the audit was to examine the extent to which the recommended measures had been implemented and whether new vulnerabilities had been added in the further implementation phase. The pentest was carried out using a white-box procedure. In other words, the source code was available to the auditor for analysis and for the vulnerability search.
From the last audit, critical vulnerabilities were detected in the development environment due to hard-coded RSA private keys, which could also be used to gain elevated privileges in the production environment. It was positively determined in the follow-up audits that no further storage of RSA keys was detected in either a productive or development environment. Now, corresponding keys are stored in a central key management system and are no longer

available to an attacker. Other vulnerabilities, which were reported to the manufacturer in 2023 as part of vulnerability research on COTS products used, have now been properly addressed and no longer pose a threat. However, new vulnerabilities with a high criticality have been identified, since users with elevated rights operate on associated databases, which allow an attacker to perform unauthorized operations at the operating system level.

Security Verifcation of a Hardware Crypto Module

During the security audit of a hardware crypto module, the implementation of IT security at the interfaces and APIs was primarily examined in the CYD Campus. The audit of the crypto part was under the responsibility of the crypto organization of the DDPS.
In detail, the API interfaces were checked for vulnerability by simulating real attacks. In addition, automated means for firmware binary analysis were used for the first time. The advantage of automated firmware analysis lies in the complete examination of all used libraries and sub-components and the detection of proven vulnerabilities in corresponding parts. The investigation was carried out as a black-box audit, i.e. the manufacturer did not provide us with the source code of the components.
Using fuzzing techniques, automated firmware binary analysis and a supplementary manual firmware analysis, vulnerabilities were identified that would have allowed an attacker to gain higher system privileges. Some of the vulnerabilities reported from the automated binary analysis could be classified as false positives. This was not because the vulnerabilities were not inherently present, but because the corresponding code parts are not used and therefore cannot be exploited by an attacker.
The classic firmware analysis in addition to an automated vulnerability assessment at the binary level shows significant advantages for the first time in the completeness of the examination of security-critical components. All the vulnerabilities identified in the study were fixed by the manufacturer in a timely manner and before productive use. The following table lists the vulnerabilities published in 2024.

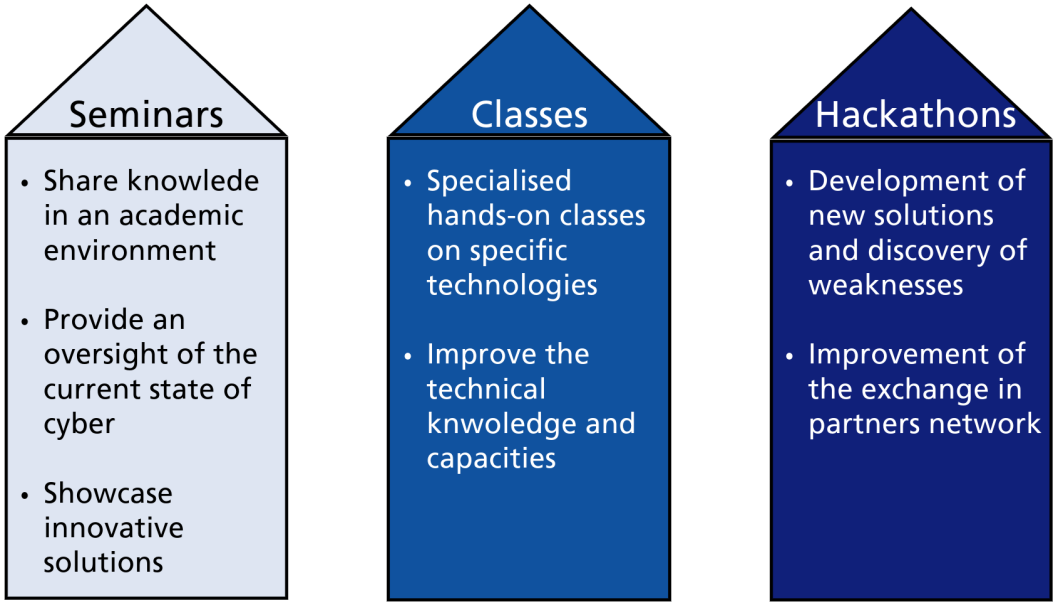
Affected System	Manufacturer	Report	CVSS	Date
Plantronics Hub	Plantronics	CVE-2024-27460	7.8	May 24
DNS	Unbound, PowerDNS, Bind	USENIX Security 2024	5.9	Aug 24
ActaNova	Rubicon	Reported via internal process, fixed	7.4	Aug 24
HaloITSM	Halo Service Solutions	CVE-2024-6200	8	Aug 24
HaloITSM	Halo Service Solutions	CVE-2024-6201	5.3	Aug 24
HaloITSM	Halo Service Solutions	CVE-2024-6202	9.8	Aug 24
HaloITSM	Halo Service Solutions	CVE-2024-6203	8.3	Sep 24
UBR-01 Mk2	MBS Systems	Reported to manufacturer, fixed	5.3	Sep 24
UBR-01 Mk2	MBS Systems	Reported to manufacturer, fixed	9.4	Sep 24
UBR-01 Mk2	MBS Systems	Reported to manufacturer, fixed	7.2	Sep 24
UBR-01 Mk2	MBS Systems	Reported to manufacturer, fixed	6.5	Sep 24
UBR-01 Mk2	MBS Systems	Reported to manufacturer, fixed	6.6	Sep 24

List of the published and reported vulnerabilities of hardware and software components examined in 2024.

12. Cyber Training

In 2024, the Cyber-Defence campus extended its Cyber Training program. Cyber training refers to the set of both technical formation events to learn fundamental skills and exercises designed to train the skills of participants. This program is designed towards technical and strategical experts of the public administration involved in cyber defence, both civilian and military personnel. This approach covers both training dedicated to learning new skills, and exercises designed to foster retention and improve mastery over time.

As part of the national cyber strategy, it has been determined that training and continuous education is a key measure to improve the readiness of Switzerland to face cyber threats. Dedicated training over a lifetime to support specialists is a strategic priority of the country. As part of its duties, the Cyber-Defence Campus has developed a program implementing this approach in its activities, based on the following three core pillars: seminars, hackathons, and classes. Those trainings are made for experts of the federal administration, with support from external actors in sectors of critical infrastructures when their activities overlap with the duties of the federal government.



Seminars

Once a month, the Cyber-Defence Campus invites experts from its staff, from academic institutions, or from its industry partners, in order to give a lecture to members of the DDPS and an overview of a trending topic in cybersecurity research. These regular events are an opportunity for personnel of the department to learn about a new theme and to personally talk and exchange with experts in academia and in the cyber industry. The following list of topics has been covered this year:

- Functional transport privacy with the help of off-the-shelf hardware
- The state of vulnerability in Switzerland and how bug bounties work
- Large language models: breakthroughs, dangers and limitations
- Quantum technologies: trends and implications for cyber defense
- Securing wide-area networks through innovative solutions
- Threats and vulnerabilities in satellite cybersecurity
- Introduction to quantum computing and its possible uses
- Monitoring wireless frequencies for device identification and threat detection
- Manipulate, deceive, subvert: on the role of AI-generated images in cyber influence activities

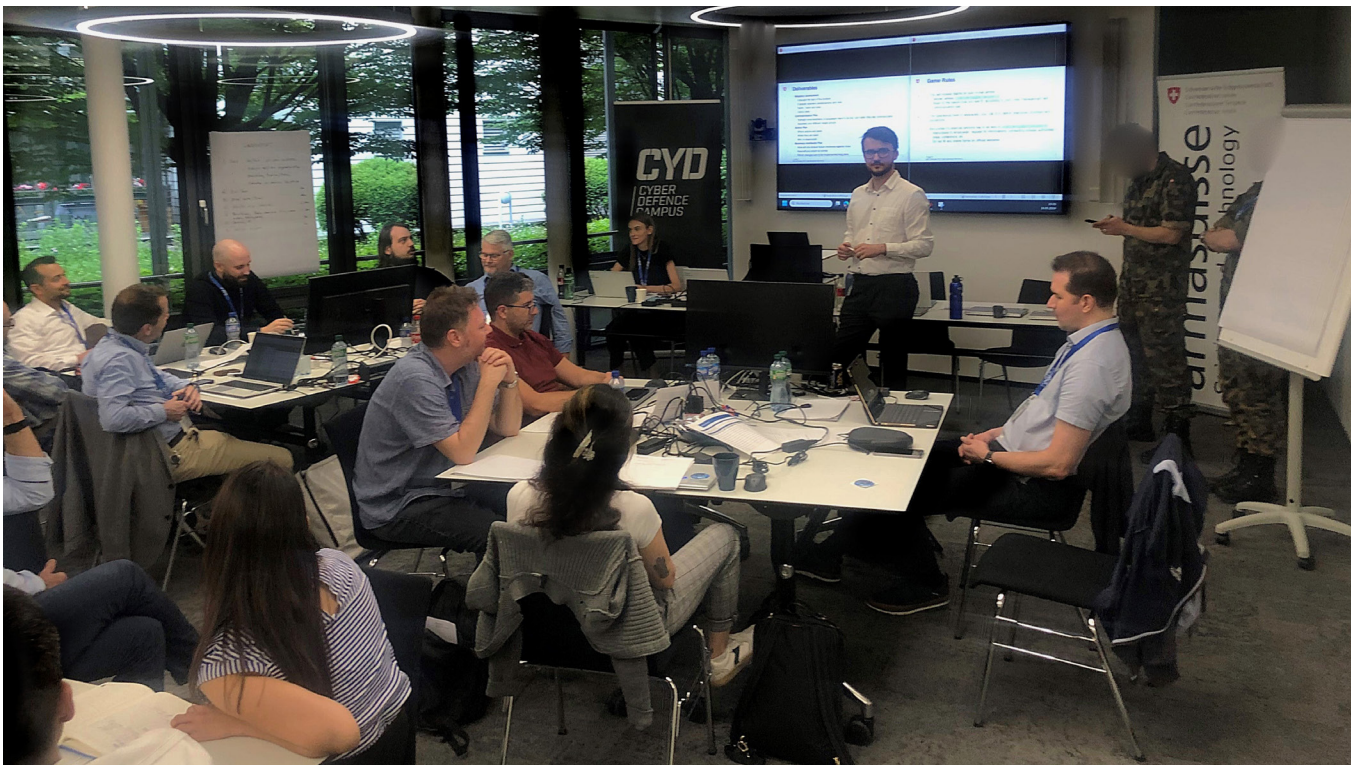
Dr. Martin Strohmeier presents threats and vulnerabilities in satellite cybersecurity.

Classes

Starting from 2023, the Cyber-Defence Campus provides hands-on training on a variety of technical skills, dedicated to providing public servants responsible for cyber defence with the skills required to fill their duties successfully. Throughout the year, multiple days long classes are organised to provide members of the public administration with the opportunity to learn new technical skills and to practice using advanced hardware. Those classes use the partner network of the Cyber-Defence Campus and bring experts from different fields to teach hands-on methods of security, by allowing participants to immediately put into practice what they learn on the hardware provided. Those classes each focus on a concrete technological element and are based on the learning by doing principle.

The classes organized in this area focused on the following topics:

- Forensics of Industrial Control Systems: using a realistic testbed, participants learned how to identify indicators of compromise on the control systems of a power station, and how to solve the identified vulnerabilities.
- Car firmware analysis using fuzzing methods: Using a CAN bus that was provided to them, specialists learned how to implement a variety of fuzzing methods to identify vulnerabilities in the software controlling different functions in modern cars.
- Management skills in a cyber crisis situation: Participants were tasked with playing the role of a crisis board of a fictional energy company, implementing strategical security measures following the method of the armed forces crisis management.



Cédric Aeschlimann leads the class of the cyber crisis training.

Hackathon

The last part of the training program is our hackathons. This portmanteau term made of “hacking” and “marathon” describes an event where multiple people from diverse backgrounds gather to collaborate on developing software and/or hardware solutions for a specific problem facing their organisation. Every year, one to three hackathons are held in our Thun building or abroad, gathering experts from the CYD Campus, academic and private partners, as well as members of the public administration to experiment using state of the art or new technologies. This approach allows them to perfect their security skills as well as better understand the systems under consideration.

This year, a CYD Campus hackathon took place around the topic of satellite cybersecurity, where experts from around Europe gathered to explore different solutions to improve offensive and defensive capacities in this area. Experts from the ETH Zurich, EPFL, University of Oxford, and the University of Kaiserslautern-Landau collaborated on creating a full-fledged solution to build a system for satellite detection and security tracking. Another hackathon took place in Spain around the topic of data science and novel methods to derive insights from data.

Satellite cybersecurity hackathon at the CYD Campus in Thun.

13. Activities

Visits

- 06.02.2024: National Armaments Director (NAD), Thun
- 13.02.2024: Cyber Bataillon 42 – Cyber Course, Thun
- 26.02.2024: Chief Cyber Command Polish Armed Forces and Chief Cyber Command Swiss Armed Forces, Thun
- 07.03.2024: GCSP: Delegation Military attaché training course
- 20.03.2024: Chief of the DDPS and Members of the SIK-S and SIK-N parliaments
- 28.03.2024: Cyber Bataillon 42 – Cyber Course, Thun
- 17.04.2024: Delegation Cyber Command and German Armed Forces
- 24.04.2024: Delegation Singapore, Lausanne
- 17.05.2024: Deputy National Armaments Director, Lausanne
- 28.05.2024: Deputy National Armaments Director, Zurich
- 27.-28.06.2024: PESCO Cyber Range Federation Meeting, Zurich/Bern
- 28.06.2024: Visit of the 7 General Secretaries of the Federal Departments, Zurich
- 03.07.2024: National Armament Director with Military attachés, Thun
- 11.09.2024: Delegation Cyber Command, Lausanne
- 12.09.2024: Cyber Bataillon 42 - Cyber Course, Thun
- 13.09.2024: Armed Forces Staff, Zurich
- 24.-26.09.2024: NATO SET Meeting, Thun
- 09.10.2024: Armaments Commission, Thun
- 13.12.2024: HSP Connect Day, Zurich

Events

- 29.01.2024: Lunch Seminar, Thun
- 16.03.2024: VIS Contact party, ETH Zurich
- 18.03.2024: Security Challenge, Thun
- 06.05.2024: Lunch Seminar, Thun
- 13.05.2024: Security Challenge, Thun
- 15.05.2024: CYD Innovation Day, Bern
- 16.05.2024: Cyber Training, Zurich
- 27.05.2024: Lunch Seminar, Thun
- 10.06.2024: Lunch Seminar, Thun
- 17. - 21.06.2024: Cyber Alp Retreat, Sachseln
- 26.06.2024: Research report FORA 3a/b, Thun
- 29.07.2024: Security Challenge, Thun
- 14.08.2024: Usenix Security Switzerland Reception, Philadelphia
- 26.08.2024: Lunch Seminar, Bern
- 11.09.2024: ICS2 Chapter Switzerland Event, Zurich
- 23.09.2024: Lunch Seminar, Thun
- 30.09.2024: Security Challenge, Thun
- 14. - 18.10.2024: Satellite Communication Security Hackathon, Thun
- 21.10.2024: Lunch Seminar, Thun
- 23.10.2024: CYD Fellowship Event at ETH Zurich

- 30.10.2024: Cyber-Defence Campus Conference, Bern
- 11.11.2024: Lunch Seminar, Bern
- 11.11.2024: Security Challenge, Thun
- 02.12.2024: Lunch Seminar, Thun
- 04.12.2024: End-of-year event, 5 year celebration CYD Campus, Zurich
- 12.12.2024: Annual technology monitoring event, at EPFL

Visits Abroad

- 25.02. - 26.02.2024: University of Murcia (ESP)
- 26.02. - 01.03.2024: NDSS, San Diego (USA)
- 02.03. - 09.03.2024: IEEE Aerospace Conference, Montana (USA)
- 03. - 09.03.2024: IoT Hacking Training RootedC (ESP)
- 04.03. - 07.03.2024: LockedShields 2024 – Parter Run, Tallinn, Estonia
- 11.03. - 13.03.2024: 11e Eu/EDA CapTech Cyber, Ljubljana (SLO)
- 17.03. - 20.03.2024: University of Oxford, Oxford (GB)
- 21.04. - 26.04.2024: LockedShields 2024 - Exercise, Tallinn, Estonia
- 24.04. - 25.04.2024: CySat, Paris (FRA)
- 04.05. - 10.05.2024: RSA, San Francisco (USA)
- 28.05. - 31.05.2024: Cycon, Estonia
- 18.06. - 20.06.2024: Eurosatory, Paris (FRA)
- 05.08. - 14.08.2024: Technology scouting, San Jose (USA)
- 06.08. - 12.08.2024: Blackhat und DEF CON, Las Vegas (USA)
- 14.08. - 16.08.2024: Usenix Security, Philadelphia (USA)
- 15.09. - 21.09.2024: GTM and SIT Conference 2024, Berlin (GER)
- 19.09.2024: CatB CRF + CapTech Cyber, Bruxelles (BEL)
- 29.09. - 03.10.2024: DASC, San Diego (USA)
- 24.10. - 01.11.2024: ARL + MILCOM, Washington DC (USA)
- 04.11. - 06.11.2024: Global MILSATCOM, London (GB)
- 07.11. - 08.11.2024: OpenSky Symposium, Hamburg (GER)
- 07.11. - 08.11.2024: University of Murcia, Murcia (ESP)
- 11.11. - 16.11.2024: Hackathon, Elche/Alicante (ESP)
- 17.11. - 21.11.2024: European Quantum Technologies Conference 2024, Lissabon (POR)
- 19.11. - 21.11.2024: European Cyber Week, Rennes (FRA)
- 26.11.2024: PESCO CRF, Luxembourg
- 12.12.2024: BlackHat Europe 2024, Arsenal (GB)

Cyber Alp Retreat in Sachseln.

14. Presentations

- 17.01.2024: AI and Desinformation, World Economic Forum, Davos
- 06. - 07.03.2024: Towards a fully automated blue team, Locked Shields Partners' Run, Tallinn (Estonia)
- 24. - 25.04.2024: Towards a fully automated blue team, Locked Shields, Tallinn (Estonia)
- 26.04.2024: IoT Security, Insomniak, Lausanne
- 02.05.2024: Generative Artificial Intelligence, Digital Day armasuisse, Bern
- 27.05.2024: Security of Satellite-Based Air Traffic Control Systems at the European Space Agency in Leiden, (NL)
- 28.05.2024: Leveraging AI for cyber defense, NATO CCDCOE CyCon 2024, Tallinn (Estonia)
- 29.05.2024: On Building Secure Wide Area Networks over Public Internet Service Providers, NATO CCDCOE CyCon 2024, Tallinn (Estonia)
- 06.06.2024: Exploiting Bluetooth: From your Car to the bank account Area 41, Zurich
- 06.06.2024: Keynote on artificial intelligence, Tech4Trust Award Ceremony, Lausanne
- 09.08.2024: Exploiting Bluetooth - from your car to the bank account, DEF CON 32, Las Vegas (USA)
- 10.08.2024: Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface, DEF CON 32, Las Vegas (USA)
- 10.08.2024: RF Attacks on Aviation's Last Line of Defense Against Mid-Air Collisions (TCAS II), DEF CON 32, Las Vegas (USA)
- 10.08.2024: Analyzing the Security of Satellite-Based Air Traffic Control, DEF CON 32, Las Vegas (USA)
- 21.08.2024: Developing cyber resilience – Trends and Perspectives, Helvetia Cyber Symposium, Bern
- 12.09.2024: Quantum Technologies, digitalswitzerland
- 22.10.2024: Building Military-grade WANs with Scion, Scion Day, Zurich
- 31.10.2024: Cyber-STRAT/Federal Public Prosecutor's Office: presentation of CYD Campus (activities, priorities, cooperation with ECSO) in Bern
- 06. - 07.11.2024: Large Language Models and AI at work, Security Academy DDPS
- 15.11.2024: Large Language Models in Cybersecurity, GoHack24, Zurich
- 28.11.2024: AI Cybersecurity CY Bat 42
- 12.12.2024: Morion, BlackHat Europe 2024, Arsenal (GB)
- 17.12.2024: Quantum Technologies, Parliamentary event, Bern

Innovation Day 2024.

Dr. Roland Meier presents at Locked Shields 24.

15. Publications

December

ProFe: Communication-Efficient Decentralized Federated Learning via Distillation and Prototypes
Pedro Miguel Sánchez Sánchez, Enrique Tomás Martínez Beltrán, Miguel Fernández Llamas, Gérôme Bovet, Gregorio Martínez Pérez, Alberto Huertas Celdrán, arXiv.

Secret Collusion among AI Agents: Multi-Agent Deception via Steganography
Sumeet Ramesh Motwani, Mikhail Baranchuk, Martin Strohmeier, Vijay Bolina, Philip Torr, Lewis Hammond, Christian Schroeder de Witt, Conference on Neural Information Processing Systems (NeurIPS 2024), Vancouver, Canada.

Extreme Multi-label Completion for Semantic Document Labelling with Taxonomy-Aware Parallel Learning
Julien Audiffren, Christophe Broillet, Ljiljana Dolamic, Philippe Cudré-Mauroux, arXiv.

November

Corrections to “Dynamic Security Analysis on Android: A Systematic Literature Review”
Thomas Sutter, Timo Kehrer, Marc Rennhard, Bernhard Tellenbach, Jacques Klein, IEEE Access.

Roadmap for a European open science alliance for ATM research
Tatjana Bolic, Andrew Cook, Rainer Koelle, Enrico Spinielli, Quinten Goens, Martin Strohmeier, EJTIR.

The open performance data initiative: a foundation supporting the European open science alliance for ATM research
Goens, Q, Koelle, R, Spinielli, E, Bolic, T., Cook, A.J. and Strohmeier, 14th SESAR Innovation Days, Rome, Italy.

NMT-Obfuscator Attack: Ignore a sentence in translation with only one word
Sahar Sadrizadeh, César Descalzo, Ljiljana Dolamic, Pascal Frossard, arXiv.

October

Can the Variation of Model Weights be used as a Criterion for Self-Paced Multilingual NMT?
Àlex R Atrio, Alexis Allemann, Ljiljana Dolamic, Andrei Popescu-Belis, arXiv.

Fedstellar: A platform for Decentralized Federated Learning
Enrique Tomás Martínez Beltrán et al., Expert Systems with Applications, 242, 122861.

OpenSky Report 2024: Analysis of Global Flight Contrail Formation and Mitigation Potential
Junzi Sun, Xavier Olive, Esther Roosenbrand, Céline Parzani, Martin Strohmeier, 2024 IEEE Access, AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC), San Diego, USA.

You Know What?-Evaluation of a Personalised Phishing Training Based on Users' Phishing Knowledge and Detection Skills
Lorin Schöni, Victor Carles, Martin Strohmeier, Peter Mayer, Verena Zimmermann, Proceedings of the 2024 European Symposium on Usable Security, Karlstad, Sweden.

Let's Take This Upstairs: Localizing Ground Transmitters With High-Altitude Balloons?
Matthias Schäfer, Yago Lizarribar, Gérôme Bovet, Dieter Verbruggen, 2024 IEEE Military Communications Conference (MILCOM), Washington, USA.

Identification of IoT Devices Through Machine Learning and Hardware Fingerprints Based on Clock-Skew
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Sergio Marín Sánchez, Kallol Krishna Karmakar, Gérôme Bovet, Gregorio Martínez Pérez, In: IoT Sensors, ML, AI and XAI: Empowering A Smarter World.

FedEP: Tailoring Attention to Heterogeneous Data Distribution with Entropy Pooling for Decentralized Federated Learning
Chao Feng, Hongjie Guan, Alberto Huertas Celdrán, Jan von der Assen, Gérôme Bovet, Burkhard Stiller, arXiv.

De-VertiFL: A Solution for Decentralized Vertical Federated Learning
Alberto Huertas Celdrán, Chao Feng, Sabyasachi Banik, Gerome Bovet, Gregorio Martinez Perez, Burkhard Stiller, arXiv.

MTFS: a Moving Target Defense-Enabled File System for Malware Mitigation
Jan Von der Assen, Alberto Huertas Celdrán, Rinor Sefa, Burkhard Stiller, Gérôme Bovet, 2024 IEEE 49th Conference on Local Computer Networks (LCN), Normandy, France.

Reputation System based on Distributed Ledge to Secure Decentralized Federated Learning
Jan von der Assen, Sandrin Raphael Hunkeler, Alberto Huertas Celdran, Enrique Tomas Martinez Beltran, Gérôme Bovet, Burkhard Stiller, Research Square.

Bibliometric Network Visualization with OpenAlex: An Analysis of the Quantum Computing Hardware Ecosystem
Martin Sand, Alain Mermoud, Julian Jang-Jaccard, 28th International Conference on Science, Technology and Innovation Indicators (STI2024).

September

LLM Detectors Still Fall Short of Real World: Case of LLM-Generated Short News-Like Posts
Henrique Da Silva Gameiro, Andrei Kucharavy, Ljiljana Dolamic, arXiv.

Leveraging MTD to Mitigate Poisoning Attacks in Decentralized FL with Non-IID Data
Chao Feng, Alberto Huertas Celdrán, Zien Zeng, Zi Ye, Jan von der Assen, Gerome Bovet, Burkhard Stiller, arXiv.

Asset-Centric Threat Modeling for AI-Based Systems
Jan von der Assen, Jamo Sharif, Chao Feng, Christian Killer, Gérôme Bovet, Burkhard Stiller, 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, UK.

Monitoring cybersecurity technology through the years: a technology mining approach through bibliometrics and patent analysis
Tugrul Daim, Haydar Yalcin, Alain Mermoud, Journal of Cyber Security Technology.

Extracting Semantic Entity Triplets by Leveraging LLMs
Alexander Sternfeld, Andrei Kucharavy, Dimitri Percia David, Julian Jang-Jaccard, Alain Mermoud, Joint Workshop of the 5th Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2024) and the 4th AI + Informetrics (AII2024).

LSPR23: A novel IDS dataset from the largest live-fire cybersecurity exercise
Allard Dijk, Emre Halisdemir, Cosimo Melella, Alari Schu, Mauno Pihelgas, Roland Meier, Elsevier Journal of Information Security and Applications, Volume 85, 2024.

August

ThreatFinderAI: Automated Threat Modeling Applied to LLM System Integration
Jan Von der Assen, Alberto Huertas, Jamo Sharif, Chao Feng, Gérôme Bovet, Burkhard Stiller, 2024 IEEE International Conference on Network and Service Management (CNSM), Prague, Czech Republic.

Wireless Signal Injection Attacks on VSAT Satellite Modems
Robin Bisping, Johannes Willbold, Martin Strohmeier, and Vincent Lenders, 33rd USENIX Security Symposium (USENIX Security), Philadelphia, USA.

On a Collision Course: Unveilling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS)
Giacomo Longo, Martin Strohmeier, Enrico Russo, Alessio Merlo, Vincent Lenders, 33rd USENIX Security Symposium, Philadelphia, USA.

Record: A Reception-Only Region Determination Attack on LEO Satellite Users
Eric Jederman, Martin Strohmeier, Vincent Lenders, and Jens B. Schmitt, 33rd USENIX Security Symposium, Philadelphia, USA.

KeySpace: Public Key Infrastructure Considerations in Interplanetary Networks
Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, Ivan Martinovic, arXiv.

Collective Victim Counting in Post-Disaster Response: A Distributed, Power-Efficient Algorithm Via Ble Spontaneous Networks
Giacomo Longo, Alessandro Cantelli-Forti, Enrico Russo, Francesco Lupia, Martin Strohmeier, Andrea Pugliese, Proceedings of The Second Arabic Natural Language Processing Conference, Bangkok, Thailand.

Synthetic Photography Detection: A Visual Guidance for Identifying Synthetic Images Created by AI
Melanie Mathys, Marco Willi, Raphael Meier, Array, 100360.

NLP_DI at NADI 2024 shared task: Multi-label Arabic Dialect Classifications with an Unsupervised Cross-Encoder
Vani Kanjirangat, Tanja Samardzic, Ljiljana Dolamic, Fabio Rinaldi, Future Generation Computer Systems, 157.

DART: A Solution for decentralized federated learning model robustness analysis
Chao Feng, Alberto Huertas Celdrán, Jan Von der Assen, Enrique Tomás Martínez Beltrán, Gérôme Bovet, Burkhard Stiller, Array, 100360.

A Big Data architecture for early identification and categorization of dark web sites
Javier Pastor-Galindo, Hông-Ân Sandlin, Félix Gómez Mármol, Gérôme Bovet, Gregorio Martínez Pérez, Future Generation Computer Systems, 157.

Unmasking SDN flow table saturation: fingerprinting, attacks and defenses
Beytüllah Yiğit, Gürkan Gür, Bernhard Tellenbach, Fatih Alagöz, International Journal of Information Security.

CAMP: Compositional Amplification Attacks against DNS
Huayi Duan, Marco Bearzi, Jodok Vieli, David Basin, Adrian Perrig, Si Liu, Bernhard Tellenbach, 33rd USENIX Security Symposium 24, Philadelphia, USA.

July

Unmasking SDN Flow Table Saturation: Fingerprinting, Attacks and Defenses
Beytüllah Yiğit, Gürkan Gür, Bernhard Tellenbach, Fatih Alagöz, International Journal of Information Security, International Journal of Information Security.

HydroLab: A Versatile Hydroelectric Power Lab for Security Research and Education
Sebastian Obermeier, Giorgio Tresoldi, Bernhard Tellenbach and Vincent Lenders, 21st International Conference on Security and Cryptography (SECRYPT) Journal, Dijon, France.

Air-Bus Hijacking: Silently Taking over Avionics Systems
Daniel Dorigatti, Martin Strohmeier, Stephan Neuhaus, Proceedings of the 10th ACM Cyber-Physical System Security Workshop, Singapore, Singapore.

Sparse vs Contiguous Adversarial Pixel Perturbations in Multimodal Models: An Empirical Analysis
Cristian-Alexandru Botocan, Raphael Meier, Ljiljana Dolamic, arXiv.

June

Do Large Language Models Exhibit Cognitive Dissonance? Studying the Difference Between Revealed Beliefs and Stated Answers
Manuel Mondal, Ljiljana Dolamic, Gérôme Bovet, Philippe Cudré-Mauroux, Julien Audiffren, arXiv.

BUST: Benchmark for the evaluation of detectors of LLM-Generated Text
Joseph Cornelius, Oscar Lithgow-Serrano, Sandra Mitrović, Ljiljana Dolamic, Fabio Rinaldi, Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Mexico City, Mexico.

Exploring cybertechnology standards through bibliometrics: Case of National Institute of Standards and Technology
Tugrul Daim, Haydar Yalcin, Alain Mermoud, Valentin Mulder, World Patent Information, 77, 102278.

Carbon Emissions and Debt Maturity Structure: Do ESG Controversies Matter?
Souad Brinette et al., The Journal of Alternative Investments.

Supercomputers and quantum computing on the axis of cyber security
Haydar Yalcin, Tugrul Daim, Mahdieh Mokhtari Moughari, Alain Mermoud, Technology in Society, 77, 102556.

May

VSAsTer: Uncovering Inherent Security Issues in Current VSAT System Practices Johannes Willbold, Moritz Schloegel, Robin Bisping, Martin Strohmeier, Thorsten Holz, Vincent Lenders, 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Seoul, Republic of Korea.

On Building Secure Wide-Area Networks over Public Internet Service Providers
Marc Wyss, Roland Meier, Llorenç Romá, Cyrill Krähenbühl, Adrian Perrig and Vincent Lenders, 16th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Defeating and Improving Network Flow Classifiers Through Adversarial Machine Learning
Yannick Merkli, Roland Meier, Martin Strohmeier and Vincent Lenders, 16th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

Leveraging Pre-Trained Extreme Multi-Label Classifiers for Zero-Shot Learning
Natalia Ostapuk, Ljiljana Dolamic, Alain Mermoud, Philippe Cudré-Mauroux, 2024 11th IEEE Swiss Conference on Data Science (SDS), Zurich, Switzerland.

Cleaning Semi-Structured Errors in Open Data Using Large Language Models
Manuel Mondal, Julien Audiffren, Ljiljana Dolamic, Gérôme Bovet, Philippe Cudré-Mauroux, 2024 11th IEEE Swiss Conference on Data Science (SDS), Zurich, Switzerland.

Follow the Path: Hierarchy-Aware Extreme Multi-Label Completion for Semantic Text Tagging
Natalia Ostapuk, Julien Audiffren, Ljiljana Dolamic, Alain Mermoud, Philippe Cudré-Mauroux, Proceedings of the ACM on Web Conference 2024, Singapore, Singapore.

SecBox: a Lightweight Data Mining Platform for Dynamic and Reproducible Malware Analysis
Chao Feng, Jan Von Der Assen, Alberto Huertas Celdran, Raffael Mogicato, Adrian Zermin, Vichhay Ok, Gerome Bovet, Burkhard Stiller, 2024 11th IEEE Swiss Conference on Data Science (SDS), Zurich, Switzerland.

Analyzing the robustness of decentralized horizontal and vertical federated learning architectures in a non-IID scenario
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Enrique Tomás Martínez Pérez, Daniel Demeter, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, Applied Intelligence.

ORAN-Sense: Localizing Non-cooperative Transmitters with Spectrum Sensing and 5G O-RAN
Yago Lizarribar, Roberto Calvo-Palomino, Alessio Scalingi, Giuseppe Santaromita, Gérôme Bovet, Domenico Giustiniano, IEEE INFOCOM 2024-IEEE Conference on Computer Communications, Vancouver, Canada.

Rl and fingerprinting to select moving target defense mechanisms for zero-day attacks in iot
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jan Von Der Assen, Timo Schenk, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, IEEE Transactions on Information Forensics and Security.

Transfer Learning in Pre-Trained Large Language Models for Malware Detection Based on System Calls
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez, arXiv.

Voyager: Mtd-based aggregation protocol for mitigating poisoning attacks on dfl
Chao Feng, Alberto Huertas Celdrán, Michael Vuong, Gérôme Bovet, Burkhard Stiller, NOMS 2024-2024 IEEE Network Operations and Management Symposium, Seoul, Republic of Korea.

Impact of Sustainable Energy Policies on European Stock Markets
Vineeta Kumari et al., The Journal of Alternative Investments.

Climate Risk for Coastal Commercial Real Estate in the Language of Modern Portfolio Theory
Emilian Belev et al., The Journal of Alternative Investments.

April

LLM-Aided Social Media Influence Operations
Raphael Meier, In: Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.

E-Vote Your Conscience: Perceptions of Coercion and Vote Buying, and the Usability of Fake Credentials in Online Voting
Louis-Henri Merino, Alaleh Azhir, Haoqian Zhang, Simone Colombo, Bernhard Tellenbach, Vero Estrada-Galiñanes, Bryan Ford, arXiv

The dilemma of neuroprotection trials in times of successful endovascular recanalization
Antje Schmidt-Pogoda, Johannes Kaesmacher, Nadine Bonberg, Nils Werring, Jan-Kolja Strecker, Mailin Hannah Marie Koecke, Carolin Beuker, Jan Gralla, Raphael Meier, Heinz Wiendl, Heike Minnerup, Urs Fischer, Jens Minnerup, Frontiers in neurology, 15, 1383494.

Conversational Agents
Ljiljana Dolamic, In: Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.

FEVER: Intelligent Behavioral Fingerprinting for Anomaly Detection in P4-Based Programmable Networks
Matheus Saueressig, Muriel Figueredo Franco, Eder J Scheid, Alberto Huertas, Gerome Bovet, Burkhard Stiller, Lisandro Z Granville, International Conference on Advanced Information Networking and Applications, Kitakyushu, Japan.

Monitoring Emerging Trends in LLM Research
Maxime Würsch, Dimitri Percia David, Alain Mermoud, In: Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.

LLM-Resilient Bibliometrics: Factual Consistency Through Entity Triplet Extraction
Alexander Sternfeld, Andrei Kucharavy, Dimitri Percia David, Alain Mermoud, Julian Jang-Jaccard, Proceeding of the 5th Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2024).

Automated Identification of Emerging Technologies: Open Data Approach
Ljiljana Dolamic, Julian Jang-Jaccard, Alain Mermoud, Vincent Lenders, Joint Workshop of the 5th Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2024) and the 4th AI + Informetrics (AII2024), Changchun, China.

Dynamic Security Analysis on Android: A Systematic Literature Review
Thomas Sutter, Timo Kehrer, Marc Rennhard, Bernhard Tellenbach, Jacques Klein, IEEE Access.

March

Satellite Cybersecurity Reconnaissance: Strategies and their Real-world Evaluation
Johannes Willbold, Franklyn Sciberras, Martin Strohmeier, Vincent Lenders, IEEE Aerospace Conference (IEEE Aerospace), Big Sky, USA.

On the Security of Satellite-Based Air Traffic Control (ADS-C)
Martin Strohmeier, Tobias Lüscher, Vincent Lenders, 2nd Workshop on the Security of Space and Satellite Systems (SpaceSec 2024), San Diego, USA.

Neural Exec: Learning (and Learning from) Execution Triggers for Prompt Injection Attacks
Dario Pasquini, Martin Strohmeier, Carmela Troncoso, Proceedings of the 2024 Workshop on Artificial Intelligence and Security.

Sticky fingers: resilience of satellite fingerprinting against jamming attacks
Joshua Smailes, Edd Salkield, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, Ivan Martinovic, arXiv.

Synthetic Image Generation in Cyber Influence Operations: An Emergent Threat?
Melanie Mathys, Marco Willi, Michael Graber, Raphael Meier, arXiv.

Channel and hardware impairment data augmentation for robust modulation classification
Erma Perenda, Gerome Bovet, Mariya Zheleva, Sofie Pollin, IEEE Transactions on Cognitive Communications and Networking.

Asset-driven Threat Modeling for AI-based Systems
Jan von der Assen, Jamo Sharif, Chao Feng, Gérôme Bovet, Burkhard Stiller, arXiv.

Federatedtrust: A solution for trustworthy federated learning
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Ning Xie, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, Future Generation Computer Systems, 152.

Adversarial attacks and defenses on ML-and hardware-based IoT device fingerprinting and identification
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez, Future Generation Computer Systems, 152.

Unsmoothing Smoothed Return Series for Risk Management and Asset Allocation
Christian W Frei et al., The Journal of Alternative Investments, 26(4).

Graph Language Model (GLM): A new graph-based approach to detect social instabilities
Lemes de Oliveira Wallyson, Shamsaddini Vahid, Ghofrani Ali, Singh Inda Rahul, Sai Veeramaneni Jithendra, Voutaz Étienne, arXiv.

Trends in Large Language Models: Actors, Applications, and Impact on Cybersecurity
Ciarán Bryce, Alexandros Kalousis, Ilan Leroux, Hélene Madinier, Alain Mermoud, Valentin Mulder, Thomas Pasche, Octave Plancherel, Patrick Ruch, Technology Watch.

Measuring technological convergence in encryption technologies with proximity indices: A text mining and bibliometric analysis using openalex
Alessandro Tavazzi, Dimitri Percia David, Julian Jang-Jaccard, Alain Mermoud, arXiv.

February

Single-board device individual authentication based on hardware performance and autoencoder transformer models
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez, Computers & Security, 137, 103596.

Robust Federated Learning for execution time-based device model identification under label-flipping attack
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdran, José Rafael Buendía Rubio, Gérôme Bovet, Gregorio Martínez Pérez, Cluster Computing, 27(1).

Measuring the performance of investments in information security startups: An empirical analysis by cybersecurity sectors using Crunchbase data
Loïc Maréchal, Alain Mermoud, Dimitri Percia David, Mathias Humbert, arXiv.

Prioritizing Investments in Cybersecurity: Empirical Evidence from an Event Study on the Determinants of Cyberattack Costs
Daniel Celeny, Loïc Maréchal, Evgueni Rousselot, Alain Mermoud, Mathias Humbert, arXiv.

FeedMeter: evaluating the quality of community-driven threat intelligence
Andreas Rüedlinger, Rebecca Klauser, Pavlos Lamprakis, Markus Happe, Bernhard Tellenbach, Onur Veyisoglu, Ariane Trammell, arXiv.

January

X-Attack 2.0: The Risk of Power Wasters and Satisfiability Don't-Care Hardware Trojans to Shared Cloud FPGAs
Dina G. Mahmoud, Beatrice Shokry, Vincent Lenders, Wei Hu, and Mirjana Stojilovic, IEEE Access Journal.

Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.
Andrei Kucharavy, Octave Plancherel, Valentin Mulder, Alain Mermoud, Vincent Lenders, In: Large Language Models in Cybersecurity: Threats, Exposure and Mitigation.

A Cost-Efficient RFI Localization Approach to Detect GNSS Jamming and Spoofing
Michael Felux, Valentin Fischer, Sophie Jochems, Okuary Osechas, Manuel Waltert, Luciano Sarperi, Martin Strohmeier, Proceedings of the 2024 International Technical Meeting of The Institute of Navigation, Long Beach, USA.

GuardFS: A file system for integrated detection and mitigation of linux-based ransomware
Jan von der Assen, Chao Feng, Alberto Huertas Celdrán, Róbert Oleš, Gérôme Bovet, Burkhard Stiller, arXiv.

Mitigating communications threats in decentralized federated learning through moving target defense
Enrique Tomás Martínez Beltrán, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez, Alberto Huertas Celdrán, Wireless Networks.

A Summary of Adversarial Attacks and Defenses on ML-and Hardware-based IoT Device Fingerprinting and Identification
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez, Future Generation Computer Systems, 152.

A Summary of RansomAI: AI-powered Ransomware for Stealthy Encryption
Jan von der Assen, Alberto Huertas Celdrán, Janik Luechinger, Pedro Miguel Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, IX Jornadas Nacionales de Investigación En Ciberseguridad.

Sentinel: An aggregation function to secure decentralized federated learning
Chao Feng, Alberto Huertas Celdrán, Janosch Baltensperger, Enrique Tomás Martínez Beltrán, Pedro Miguel Sánchez Sánchez, Gérôme Bovet, Burkhard Stiller, ECAI 2024.

RL and Fingerprinting to Select Moving Target Defense Mechanisms for Zero-Day Attacks in IoT
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jan von der Assen, Timo Schenk, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, IEEE Transactions on Information Forensics and Security, 19.

TechRank
Anita Mezzetti, Loïc Maréchal, Dimitri Percia David, Thomas Maillart, Alain Mermoud, The Journal of Alternative Investments, 26(3).

16. Communication

Strategic Communication for Cybersecurity

In the past year, the Cyber-Defence Campus has continued to play a vital role in raising awareness about cybersecurity challenges and promoting the Campus's activities nationally and internationally. We aim to effectively enhanced visibility and engagement through strategic communication and innovative content creation.

Growing Digital Presence

The team's efforts have significantly boosted the CYD Campus' online presence. On LinkedIn alone, the channel grew to over 7,600 followers, gaining over 2,700 new followers in 2024 with 240,850 impressions during this period. This growing online presence reflects a commitment to engaging diverse audiences, from cybersecurity professionals to academic and public stakeholders.

Raising Awareness Through Events and Content

The CYD Campus has been instrumental in organising and supporting events designed to foster dialogue and knowledge exchange in the cybersecurity field. Initiatives like the Lunch Seminars, the Cyber Alp Retreat, and Cybersecurity Conferences have been enriched with tailored content, including event flyers, articles, and dynamic social media campaigns. These activities not only promote the Campus's work but also strengthen connections between the federal government, industry, military, and academic institutions.

Proactive Communication in a Rapidly Evolving Field

In the fast-changing landscape of cybersecurity, proactive communication is essential. The rapid rise of technologies such as AI tools, including ChatGPT, underscores the need for continuous public engagement and education. By addressing potential cyber risks and fostering collaboration among experts, the CYD Campus contributes to safeguarding digital spaces while promoting Switzerland as a leader in cyber defense.
Through effective storytelling, strategic outreach, and robust event support, the communications team has successfully strengthened the Campus' role as a national and international hub for cybersecurity innovation and collaboration.

Selection of Public Media and Web Releases

- **04.01.2024** Cyber trend monitoring gains importance at Cyber-Defence Campus
- **14.02.2024** Machine learning enables early-warning signals to be recognised in the event of social instability
- **07.03.2024** First Successful Quantum Computing Experiments at the Cyber-Defence Campus
- **30.04.2024** Insights into security-relevant smartphone innovations at the Cyber Defence Campus
- **08.05.2024** From research at the Cyber-Defence Campus to the capabilities of the Federal Administration's cyber defence
- **31.05.2024** Successful crisis simulation strengthens cybersecurity capabilities in Switzerland
- **11.06.2024** Lucrative Innovation Day of the Cyber-Defence Campus
- **27.06.2024** Swiss Team uses SCION to connect to Estonia during Cyber-Defense Exercise
- **16.07.2024** Study results on threats and impacts of generative artificial intelligence on cyber security
- **22.08.2024** Insights into the work of the Cyber Data Technologies team at the CYD Campus
- **16.09.2024** Consultancy expertise of the Cyber-Defence Campus in the field of smartphone innovations
- **29.10.2024** Introducing the finalists of the Cyber Startup Challenge 2024
- **31.10.2024** The startup «Patronus AI» wins over the DDPS in the Cyber Startup Challenge 2024

CYD Campus Website

LinkedIn

Andrea Thäler of the CYD Campus communication at the 5 year celebration in Zurich.

LEGAL NOTICE

Editor: Cyber-Defence Campus, armasuisse Science and Technology, Feuerwerkerstrasse 39, CH-3602 Thun
Contact: +41 (0)58 480 59 34, cydcampus@armasuisse.ch
Photo credits: Where not otherwise stated: Source VBS/DDPS, Adobe Stock, iStock

Contact

Cyber-Defence Campus
Feuerwerkerstrasse 39
CH-3602 Thun

Zollstrasse 62
CH-8005 Zürich

EPFL Innovation Park, Bâtiment I
CH-1015 Lausanne

cydcampus.admin.ch
cydcampus@armasuisse.ch
+41 58 462 99 00